

BUSINESS CONTINUITY AND DISASTER RECOVERY PLANNING FOR IT PROFESSIONALS

Second Edition



Susan Snedaker
with Chris Rima

Business Continuity and Disaster Recovery Planning for IT Professionals

This page intentionally left blank

Business Continuity and Disaster Recovery Planning for IT Professionals

Second Edition

Susan Snedaker

Chris Rima



ELSEVIER

AMSTERDAM • BOSTON • HEIDELBERG • LONDON
NEW YORK • OXFORD • PARIS • SAN DIEGO
SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO

Syngress is an Imprint of Elsevier

SYNGRESS®

Acquiring Editor: Chris Katsaropoulos
Development Editor: Benjamin Rearick
Project Manager: Malathi Samayan
Designer: Maria Inês Cruz

Syngress is an imprint of Elsevier
225 Wyman Street, Waltham, MA 02451, USA

First edition 2007

© 2014 Elsevier, Inc. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or any information storage and retrieval system, without permission in writing from the publisher. Details on how to seek permission, further information about the Publisher's permissions policies and our arrangements with organizations such as the Copyright Clearance Center and the Copyright Licensing Agency, can be found at our website: www.elsevier.com/permissions.

This book and the individual contributions contained in it are protected under copyright by the Publisher (other than as may be noted herein).

Notices

Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods or professional practices, may become necessary. Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information or methods described herein. In using such information or methods they should be mindful of their own safety and the safety of others, including parties for whom they have a professional responsibility.

To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions, or ideas contained in the material herein.

Library of Congress Cataloging-in-Publication Data

Snedaker, Susan.

Business continuity and disaster recovery planning for IT professionals / Susan Snedaker, Chris Rima. – 2 Edition.

pages cm

Includes bibliographical references and index.

ISBN 978-0-12-410526-3 (pbk.)

1. Business—Data processing—Security measures. 2. Electronic data processing departments—Security measures. 3. Crisis management. 4. Computer networks—Security measures. 5. Management information systems—Security measures. I. Rima, Chris. II. Title.

HF5548.37.S67 2013

658.4'78—dc23

2013025237

British Library Cataloguing-in-Publication Data

A catalogue record for this book is available from the British Library.

For information on all Syngress publications, visit our website store.elsevier.com/Syngress

ISBN: 978-0-12-410526-3

Printed in the United States of America

14 15 16 13 12 11 10 9 8 7 6 5 4 3 2 1



Working together
to grow libraries in
developing countries

www.elsevier.com • www.bookaid.org

Contents

Acknowledgments	xix
About the Authors	xxi
Introduction.....	xxiii
CHAPTER 1 Business Continuity and Disaster Recovery Overview.....	1
Introduction.....	1
Business Continuity and Disaster Recovery Defined	3
Components of Business	4
People in BC/DR Planning	6
Process in BC/DR Planning.....	8
Technology in BC/DR Planning.....	10
The Cost of Planning versus the Cost of Failure.....	11
People	15
Process.....	16
Technology.....	17
Types of Disasters to Consider	18
Business Continuity and Disaster Recovery Planning Basics	19
Project Initiation	21
Risk Assessment	22
Business Impact Analysis	22
Mitigation Strategy Development	22
Plan Development.....	23
Training, Testing, and Auditing	23
Plan Maintenance.....	23
Summary	24
Key Concepts.....	25
BC/DR Defined.....	25
Components of Business.....	26
The Cost of Planning versus the Cost of Failure.....	26
Types of Disasters to Consider.....	27
BC/DR Planning Basics.....	27
References.....	27
CHAPTER 2 Legal and Regulatory Obligations Regarding Data and Information Security.....	29
Introduction.....	29
Impact of Recent History	31

Current Regulatory Environment	33
Source of Legal Obligations	33
Scope of Legal Obligations	35
Information Security Management.....	37
Responsibility Lies at the Top.....	37
Written Information Security Program (WISP)	38
Did You Know?.....	40
Summary	40
Key Concepts.....	41
Impact of Recent History	41
Current Regulatory Environment	41
Information Security Management.....	41
References.....	42
Case Study	
Case Study: Legal Obligations Regarding Data Security	43
Contributor Profile.....	43
Background	44
The Sony PlayStation Incident.....	44
State Laws Regarding Data Security	45
Notice of Security Breach Laws	45
Safeguarding Personal Data State Laws	47
Federal Laws Regarding Data Security	47
U.S. House of Representatives Proposed Bill.....	48
U.S. Senate Response	49
Executive Order-improving Critical Infrastructure	
Cyber Security	49
Conclusion	49
References.....	50
CHAPTER 3 Project Initiation	51
Introduction.....	51
Elements of Project Success.....	52
Executive Support.....	53
User Involvement.....	56
Experienced Project Manager.....	56
Clearly Defined Project Objectives.....	57
Clearly Defined Project Requirements.....	58
Clearly Defined Scope.....	59
Shorter Schedule, Multiple Milestones	61
Clearly Defined Project Management Process.....	61

Project Plan Components	63
Project Initiation or Project Definition.....	64
Forming the Project Team	71
Project Organization	74
Project Objectives	74
Project Stakeholders	77
Project Requirements	78
Project Parameters	80
Project Infrastructure	84
Project Processes.....	85
Project Communication Plan	89
Project Planning.....	91
Work Breakdown Structure	91
Critical Path	91
Project Implementation	92
Managing Progress.....	93
Managing Change	94
Project Tracking	94
Project Close Out.....	95
Key Contributors and Responsibilities.....	96
Information Technology	96
Human Resources	99
Facilities/Security	99
Finance/Legal.....	100
Warehouse/Inventory/Manufacturing/Research	101
Purchasing/Logistics	102
Marketing and Sales	102
Public Relations	103
Operations	105
Project Definition	106
Business Requirements.....	107
Functional Requirements.....	109
Technical Requirements	111
Business Continuity and Disaster Recovery Project Plan	112
Project Definition, Risk Assessment	113
Business Impact Analysis	113
Risk Mitigation Strategies	114
Plan Development.....	114
Emergency Preparation.....	114
Training, Testing, Auditing	114
Plan Maintenance.....	115

Summary	115
Key Concepts.....	117
Elements of Project Success.....	117
Project Plan Components.....	117
Key Contributors and Responsibilities.....	118
Project Definition.....	118
Business Continuity and Disaster Recovery Plan	119
References.....	119

Industry Spotlight #1—Energy/Utilities

Business Continuity and Disaster Recovery in Energy/Utilities	121
Introduction.....	121
Integrating BC/DR Requirements into IT Governance	123
BC/DR Requirements Definition.....	124
IT Service Level Definition.....	125
Application Recovery Procedures	126
Summary of Integrating BC/DR Requirements into IT Governance	127
Improving BC/DR Recovery and Risk Mitigation Strategies ...	128
Ensuring Access to BC/DR Documentation in a Disaster...	128
Change Approval Board and Technical Change Review Committees	130
Security Control Testing.....	131
Separation of Duties	132
Centralized Security Vulnerability Assessment	132
IT Network Vulnerability Assessment	133
Security Control Baselines and Change Detection	134
Data Center and Network	134
Compute and Data	135
Self-service Application Failover and Failback	139
Industrial Control Systems	140
Summary of Improving BC/DR Recovery and Risk Mitigation Strategies.....	142
Improving BC/DR Testing	143
Recovery from Actual Incidents: Postmortems and Documenting Lessons Learned	143
Scheduled BC/DR Tests	144
Summary of Scheduled BC/DR Testing	149
Summary of Best Practices and Key Concepts	150
References.....	150

CHAPTER 4 Risk Assessment	151
Introduction.....	151
Risk Management Basics	153
Risk Management Process.....	155
People, Process, Technology, and Infrastructure in Risk Management.....	159
People	159
Process.....	160
Technology.....	160
Infrastructure	161
IT-Specific Risk Management.....	161
IT Risk Management Objectives.....	162
The System Development Lifecycle Model.....	163
Risk Assessment Components.....	166
Information Gathering Methods	168
Natural and Environmental Threats	169
Human Threats.....	185
Infrastructure Threats.....	195
Threat Checklist.....	199
Threat Assessment Methodology	202
Quantitative Threat Assessment.....	203
Qualitative Threat Assessment	207
Vulnerability Assessment.....	211
People, Process, Technology, and Infrastructure	214
Vulnerability Assessment	216
Summary	219
Key Concepts.....	221
Risk Management Basics.....	221
Risk Assessment Components	222
Threat Assessment Methodology	222
Vulnerability Assessment	223
References.....	223
CHAPTER 5 Business Impact Analysis	225
Introduction.....	225
Business Impact Analysis Overview.....	226
Upstream and Downstream Losses	229
Understanding The Human Impact	230
Understanding Impact Criticality	232
Criticality Categories	232
Recovery Time Requirements	235

Identifying Business Functions	241
Facilities and Security	242
Finance	243
Human Resources	244
Information Technology	245
Legal/Compliance	245
Manufacturing (Assembly)	246
Marketing and Sales	246
Operations	247
Research and Development	247
Warehouse (Inventory, Fulfillment, Shipping, and Receiving)	248
Other Areas	248
Gathering Data for the Business Impact Analysis	249
Data Collection Methodologies	250
Determining the Impact	254
Business Impact Analysis Data Points	256
Understanding IT Impact	260
Preparing the Business Impact Analysis Report	268
Summary	270
Key Concepts	271
BIA Overview	271
Understanding Impact Criticality	271
Identifying Business Functions	272
Gathering Impact Data	272
Determining Impact	273
BIA Data Points	273
References	273

Industry Spotlight #2—Healthcare

Business Continuity and Disaster Recovery in Healthcare	275
Introduction to Healthcare IT	275
Types of Healthcare Organizations	277
The Rising Cost of Healthcare	280
Governmental Incentives and Penalties	281
HIEs and Accountable Care Organizations	283
Integration of Healthcare IT and Medical Equipment	285
Consumer-Driven Healthcare	286
Real-Time Data	287
Summary	288

Regulatory Environment.....	289
Centers for Medicare and Medicaid Services/Joint Commission on Accreditation of Healthcare Organizations ..	289
U.S. Food and Drug Administration	290
Health Insurance Portability and Accountability Act	292
Health Information Technology for Economic and Clinical Health	294
Payment Card Industry	295
State and Local Requirements.....	296
Healthcare IT Risk Management	296
Patient Safety	297
Patient Care.....	298
Organizational Solvency.....	298
Facility Management	299
Technical Needs—Healthcare IT Architecture.....	299
Clinical Systems	300
Business Systems	301
Types of Data.....	302
Types of Systems and Storage	304
Healthcare Operational Needs.....	310
Admitting	310
Insurance Verification and Billing Services	311
Clinical Care	313
Interoperability Among Disparate Systems	315
Electronic Medical Record	315
Diagnostic Imaging.....	316
Medical Equipment.....	316
Food Services.....	316
Environmental Services	316
Billing and Payment Systems.....	317
Payroll	317
Human Resources	318
Current Environment and New Technology	318
Advances in Data Storage and Replication.....	318
Mobile Devices	319
Virtualization and Cloud Computing	320
Communication Systems	322
Current Environment and New Technology Summary	323
Healthcare IT BC/DR Best Practices	323
Security Frameworks	323
Best Practices	326

Summary	328
Overview of Healthcare IT	328
Regulatory Requirements	328
Healthcare IT Risk Management.....	329
Technical Needs—Healthcare IT Architecture	329
Healthcare Operational Needs.....	330
Interoperability Among Disparate Systems—Integration in Healthcare IT	330
Current Environment and New Technology	331
Healthcare IT BC/DR Best Practices	331
Key Concepts.....	332
References.....	335
 CHAPTER 6 Risk Mitigation Strategy Development	337
Introduction.....	337
Types of Risk Mitigation Strategies	339
Risk Acceptance	340
Risk Avoidance.....	340
The Risk Mitigation Process	343
Recovery Requirements.....	343
Recovery Options	343
Recovery Time of Options	346
Cost versus Capability of Recovery Options	347
Recovery Service Level Agreements	347
Review Existing Controls	349
Developing your Risk Mitigation Strategy	350
People, Buildings, and Infrastructure	354
IT Risk Mitigation	355
Critical Data and Records.....	356
Critical Systems and Infrastructure	356
Backup and Recovery Considerations	358
Alternate Business Processes.....	358
IT Recovery Systems.....	359
Documenting Your Risk Mitigation Strategy	364
Summary	365
Key Concepts.....	365
Types of Risk Mitigation Strategies.....	365
Risk Mitigation Process.....	366
IT Risk Mitigation	367
Backup and Recovery Considerations.....	367
References.....	367

CHAPTER 7 Business Continuity/Disaster Recovery Plan Development	369
Introduction.....	369
Implement Risk Mitigation Strategies	371
Phases of Business Continuity and Disaster	375
Activation Phase	375
Recovery Phase	381
Business Continuity Phase.....	382
Maintenance/Review Phase	383
Defining BC/DR Teams and Key Personnel	383
Crisis Management Team	384
Management	385
Damage Assessment Team.....	385
Operations Assessment Team.....	385
IT Team.....	386
Administrative Support Team	386
Transportation and Relocation Team	386
Media Relations Team.....	387
Human Resources Team.....	387
Legal Affairs Team.....	387
Physical/Personnel Security Team	388
Procurement Team (Equipment and Supplies)	388
General Team Guidelines	389
BC/DR Contact Information.....	390
Defining Tasks and Assigning Resources.....	392
Alternate Site	393
Cloud Services	395
Contracts for BC/DR Services.....	397
Communications Plans	400
Internal	400
Employee	400
Customers and Vendors.....	401
Shareholders.....	401
The Community and the Public.....	401
Event Logs, Change Control, and Appendices	402
Event Logs	403
Change Control	404
Distribution	405
Appendices.....	406
Additional Resources	407
What's Next.....	407
Summary	408

Key Concepts.....	409
Phases of Business Continuity and Disaster Recovery.....	409
Defining BC/DR Teams and Key Personnel.....	409
Defining Tasks and Assigning Resources.....	410
Communications Plans	410
Event Logs and Change Control	411
Appendices.....	411
References.....	411
Industry Spotlight #3—Financial	
Business Continuity and Disaster Recovery in Financial Services	413
Overview.....	413
Finance Industry Regulation Overview	413
United States Financial Regulation	414
European Financial Regulation	415
Other Regions' Financial Regulation	415
Finance Industry Requirements for Business Continuity	416
Industry Impact—September 11 Attacks	416
Industry Impact—Hurricane Sandy.....	420
Industry Impact—Cyber Threats.....	422
Looking Forward	424
Summary	425
References.....	425
CHAPTER 8 Emergency Response and Recovery.....	427
Introduction.....	427
Emergency Management Overview	428
Emergency Response Plans.....	428
Emergency Response Teams.....	430
Crisis Management Team.....	432
Emergency Response and Disaster Recovery	433
Alternate Facilities Review and Management	433
Crisis Communications.....	433
Human Resources	435
Legal.....	436
Insurance	436
Finance	436
Disaster Recovery.....	436
Activation and Emergency Response Checklists	437
Recovery Checklists	437
IT Recovery Tasks	438

Business Continuity	444
Summary	446
Key Concepts.....	447
Emergency Management Overview	447
Emergency Response Plans	447
Crisis Management Team	448
Disaster Recovery	448
IT Recovery	448
Business Continuity	449
References.....	449
 Industry Spotlight #4—SMBs	
Business Continuity and Disaster Recovery for Small- and Medium-Sized Businesses	451
Overview of SMB Disaster Recovery.....	451
SMB Disaster Preparedness: Survey Results.....	453
On-Premise Disaster Recovery	453
SMB Case Studies	455
Using a Co-location Data Center for Disaster Recovery	456
The Value of Co-location Data Centers in a Disaster	457
Tips for Selecting a Co-location Provider	457
What Does a Co-location Center Cost?	458
SMB Case Study: Balancing Internal Capability and Cost with Co-location Data Centers for DR	459
Disaster Recovery in the Cloud	460
Disaster Recovery in the Cloud Options.....	462
Protecting Branch Offices with Cloud Disaster Recovery ..	465
SMB Case Studies	469
Summary	474
Key Concepts.....	474
Overview of SMB Disaster Recovery	474
SMB Disaster Preparedness: Survey Results	475
On-premise Disaster Recovery	475
Using a Co-location Data Center for Disaster Recovery....	476
Disaster Recovery in the Cloud.....	476
References.....	477
 CHAPTER 9 Training, Testing, and Auditing 479	
Introduction.....	479
Training for Disaster Recovery and Business Continuity	479

Emergency Response	480
Disaster Recovery and Business Continuity	
Training Overview	481
Training Scope, Objectives, Timelines, and Requirements	481
Performing Training Needs Assessment	482
Developing Training	483
Scheduling and Delivering Training	484
Monitoring and Measuring Training	485
Training and Testing for Your Business Continuity and Disaster Recovery Plan	485
Paper Walk-Through.....	487
Functional Exercises	491
Field Exercises	492
Full Interruption Test.....	492
Training Plan Implementers	493
Testing the BC/DR Plan.....	493
Understanding of Processes.....	494
Validation of Task Integration	495
Confirm Steps	495
Confirm Resources	495
Familiarize with Information Flow	495
Identify Gaps or Weaknesses	496
Determine Cost and Feasibility	496
Test Evaluation Criteria.....	498
Recommendations.....	499
Performing IT Systems and Security Audits	499
IT Systems and Security Audits.....	499
Summary	501
Key Concepts.....	503
Training for Emergency Response, Disaster Recovery, and Business Continuity	503
Testing your Business Continuity and Disaster Recovery Plan.....	503
Performing IT Systems Audits	504
References.....	504
CHAPTER 10 BC/DR Plan Maintenance	505
Introduction.....	505
BC/DR Plan Change Management.....	506
Training, Testing, and Auditing	507

Changes in Information Technologies	507
Changes in Operations.....	508
Corporate Changes.....	509
Legal, Regulatory, or Compliance Changes	510
Strategies for Managing change	510
Monitor Change	511
Evaluate and Incorporate Change.....	512
BC/DR Plan Audit	513
Plan Maintenance Activities.....	514
Project Close Out.....	515
Summary	516
Key Concepts.....	518
BC/DR Plan Change Management.....	518
Strategies for Managing Change	518
BC/DR Plan Audit	519
Plan Maintenance Activities.....	519
Project Close Out.....	519
APPENDIX A Risk Management Checklist.....	521
Risk Assessment	521
Mitigation Strategies.....	524
APPENDIX B Crisis Communications Checklist	527
Communication Checklist	527
Message Content.....	528
APPENDIX C Emergency Response and Recovery Checklists	529
High-Level Checklist.....	529
Activation Checklists.....	530
Emergency Response Checklists.....	531
Recovery Checklists	533
APPENDIX D Business Continuity Checklist	537
Resuming Work	537
Manufacturing, Warehouse, Production, and Operations	539
Resuming Normal Operations	539
Transition to Normalized Activities.....	541
APPENDIX E IT Recovery Checklists	543
IT Recovery Checklist One: Infrastructure	543
Recovery Checklist Three: Office Area and End-User Recovery	544

Recovery Checklist Four: Business Process Recovery.....	545
Recovery Checklist Five: Manufacturing, Production, and Operations Recovery	545
APPENDIX F Training, Testing, and Auditing Checklists	547
Training and Testing	547
IT Auditing	547
APPENDIX G BC/DR Plain Maintenance Checklist	549
Change Management	549
 Glossary of Terms	551
Index	565

Acknowledgments

First, a heartfelt thanks to Chris Rima for agreeing to collaborate on this second edition with me. Chris's real-world expertise combined with his process-oriented approach made him the perfect cohort for this project. He has helped improve upon the first edition in many respects. He's also one of the smartest people I know and our working meetings turned into technology discussions that were engaging and enlightening. Thanks also to my friend and colleague, and brilliant attorney, Deanna Conn, for contributing a piece on legal aspects of data security within the context of business continuity and disaster recovery (BC/DR) planning. Thanks to my colleague Debbie Earnest who shared her expertise and experience (bumps and bruises) garnered from working in the field of BC/DR. Her advice and comments guided me in crafting the first edition of this book and her advice remains relevant today. Her contribution offers time-tested techniques for overcoming some of the common challenges to BC/DR planning. Last, but not least, this book would not have been possible without the support of our family and friends. Thanks to Lisa Mainz for wrangling the dogs and holding down the fort while I was working long hours to complete this project, and thanks to John Nowak for his unwavering support of Chris while we were out on this journey together. And a big shout out to Chris' co-workers: Tony, Stephen, Nevin, Tony, Thomas, and Scott, for without whom Chris would not have been able to help me write this book.

This page intentionally left blank

About the Authors

Susan Snedaker is currently Director of IT and Information Security Officer at a large community hospital in Arizona, which has achieved HIMSS Analytics Stage 7 (EMR) certification and has been voted Most Wired Hospitals 2012 & 2013 years in a row. Susan has over 20 years' experience working in IT in both technical and executive positions including with Microsoft, Honeywell, and VirtualTeam Consulting. Her experience in executive roles has honed her extensive strategic and operational experience in managing data centers, core infrastructure, hardware, software, and IT projects involving both small and large teams. Susan holds a Master's degree in Business Administration (MBA) and a Bachelor's degree in Management from the University of Phoenix. She is a Certified Professional in Healthcare Information Management Systems (CPHIMS), Certified Information Security Manager (CISM), and was previously certified as a Microsoft Certified Systems Engineer (MCSE) and a Microsoft Certified Trainer (MCT). Susan also holds a certificate in Advanced Project Management from Stanford University and an Executive Certificate in International Management from Thunderbird University's Garvin School of International Management. She is the author of six books and numerous chapters on a variety of technical and IT subjects.



Chris Rima is currently Manager of Infrastructure Systems at a large utility in the southwestern U.S. recently named Utility of the Year by the Solar Electric Power Association, and winner of a CIO 100 award for creating business value with technology innovation. Chris has over 15 years' experience in information technology (IT) operations management and has coauthored three books on IT operations and security. Chris holds a Bachelor of Science degree in Aerospace Engineering from the University of Virginia and a Master of Science in Computer Information Systems from the University of Phoenix. Chris taught mathematics and IT courses at both the undergraduate and graduate level from 1999 to 2007 and has previously worked as a Program Analyst for the Department of Defense. Additionally, Chris holds a certificate in ITIL Foundations and was previously certified as a Microsoft



Certified Systems Engineer (MCSE), a Microsoft Certified Trainer (MCT), and a Certified Technical Trainer (CTT). In 2008, Chris garnered a CIO 100 Award and two Storage Networking World award nominations for efforts at his current employer to streamline the management of server and storage operations using virtualization and shared storage technologies in order to reduce operational costs and improve disaster recovery capability.

Introduction

When I wrote the first edition of this book, business continuity and disaster recovery were not topics most companies wanted to focus on. There was a lot of organizational resistance to spending the time and money necessary to develop a thorough and actionable plan. In the intervening years between the first edition and this updated second edition, more companies have come to understand that BC/DR planning is really a business requirement. That said, there still appears to be a huge opportunity for improvement across all businesses and industries.

Clearly, businesses that have been impacted by disasters, whether natural or man-made (terrorism, primarily), have gotten serious about BC/DR. Financial services firms, which are now fully electronic, have fairly robust failover systems, backup scenarios, and the ability to run their business from any one of a number of worldwide locations. This industry pretty much leads the pack when it comes to BC/DR, primarily because of the cost of downtime and the enormous potential financial impact of a disaster.

Many other industries, required by law and regulation to have BC/DR plans in place, are still struggling to meet these requirements. Many meet them “on paper” but would be hard-pressed to actually implement their plans. Some have plans that are now a decade old and obsolete. Others have plans that were never fully formed and are sitting on a file share someplace gathering electronic dust.

The bottom line is that it’s still difficult to get business leaders to willingly spend money and resources on BC/DR planning and implementing the risk-mitigating strategies. It’s gotten easier over the past decade, but challenges remain. The soft global economy of the past five years has had a dramatic impact on companies’ willingness and ability to invest in BC/DR solutions. On the upside, advances in technology, from virtualization to all manner of cloud services, have enabled companies to spend their IT dollars more effectively and build BC/DR into their high availability computing systems. To the extent that BC/DR can be operationalized, companies can leverage scarce IT resources more effectively and still protect the vital electronic assets of the company.

This book is newly updated to include examples of how companies in various industries have approached BC/DR. It contains tips, examples, suggestions, and checklists intended to assist you in creating a fully functional, up-to-date, operational BC/DR plan. Best of luck to you and may you never have to use the plan you create.

This page intentionally left blank

Business Continuity and Disaster Recovery Overview

1

IN THIS CHAPTER

- Business continuity and disaster recovery defined
- Components of business
- The cost of planning versus the cost of failure
- Types of disasters to consider
- Business continuity and disaster recovery planning basics
- Summary
- Key concepts

INTRODUCTION

Massive Tornado Hits Moore, OK. Mercy Hospital Destroyed in Joplin, MO Tornado. Powerful Earthquake Triggers Tsunami in Pacific. Super Storm Sandy Wipes Out New Jersey Boardwalk. Hurricane Katrina Makes Landfall in the Gulf Coast. Avalanche Buries Highway in Denver. These headlines are all too common these days, and it seems storms are getting larger and more destructive. These tragic events impact people's lives forever, and the loss of life and the toll on the families and communities is enormous. In the midst of these tragedies, though, is a resilience of human spirit. We pick ourselves up, assess the situation, and carry on. As an information technology (IT) professional, your job is to provide the technology to enable business to run (or, after a tragedy, to resume). IT is in every corner of just about every organization today. In some small businesses, it is as simple as a few servers and a handful of desktops or laptops. In larger organizations, it is as complex as hundreds of applications running on hundreds of servers across multiple load-balanced locations. Regardless of how simple or complex your IT environment is, you need to plan for business disruptions, which can range from a local power outage to a massive, regional event such as a tornado, hurricane, or earthquake. Some natural disasters can be predicted and even tracked, as was the case with Hurricane Katrina and Super Storm Sandy (among others), but other events are completely unexpected. Business continuity and disaster recovery (BC/DR) plans were certainly put to the test by many financial firms after the terrorist attacks in the United States on September 11, 2001; but more than a decade later, there are still many firms that do not have any meaningful BC/DR plan in place.

While it might seem insane or at least irresponsible not to have such a plan in place, statistics show that many companies don't even have solid data backup plans in place. Given the enormous cost of failure and the massive impact to a business, why are so many companies behind the curve? The answers are surprisingly simple: lack of time and resources, lack of a sense of urgency, and lack of a process for developing and maintaining a plan. This book will help you overcome those challenges and provide you a step-by-step approach to developing your plan.

There is a significant disconnect between IT and business executives when it comes to disaster recovery preparedness, according to the results of a new State of Disaster Recovery survey. While both sets of executives share same views on the importance of information availability to the business, survey data reveal a split in how to achieve the goal of minimizing downtime when an unplanned IT outage occurs.

In the survey commissioned by SunGard Availability Services and conducted by Harris Interactive, both IT and business decision-makers say information availability is important to the success of their business (83% IT, 78% business). However, fewer than half of business executives say BC/DR is important to business success compared with a large majority of IT executives (74% IT, 49% business) ([Harris Interactive, 2009](#)). A previous study by Harris Interactive also indicated that CIOs lacked confidence in their disaster readiness. In the intervening years, CIOs across all industries have gotten more savvy about the need for disaster preparedness, especially in light of the massive storms in the past few years. Yet the fact remains, there are many companies that have BC/DR plans that run the gamut from nonexistent to off-site backups only to a plan that was developed a decade ago and never refreshed. Back in 2000, some companies might have thought a "good" disaster readiness plan was having off-site backups. After the terror attacks, bombings, anthrax incidents, hurricanes, and floods that hit the United States (and other major incidents worldwide) since that time, most IT professionals now understand that off-site backups are just a small part of an overall strategy for disaster recovery.

In today's environment, every company that uses IT must address the need for BC/DR planning, regardless of the company size, revenues, or number of staff. The statistics on the failure rate of companies after a disaster are alarming (discussed later in this chapter) and that alone should serve as a wakeup call for IT professionals and corporate executives. Granted, the cost of planning must be proportionate to the cost of failure, which we'll address throughout this book.

Let's face it—very few of us want to spend the day thinking about all the horrible things that can happen in the world and to our company. It's not an energizing subject and one most of us would rather avoid in favor of deploying the latest technology in our state-of-the-art data center—which also helps explain the glaring lack of BC/DR plans in many companies. Stockholders of publicly held companies are increasingly demanding well thought-out BC/DR plans internally as well as from key vendors, but in the absence of pressure from stockholders or the Board of Directors, many companies expend their time and resources moving the business forward. BC/DR planning projects have to compete with other urgent projects for IT dollars. Unless you

can create a clear, coherent, and compelling business case for BC/DR, you may find strong executive resistance at worst or apathy at best. The good news is that changes in technology architecture over the past decade have made BC/DR solutions easier to architect and deploy, as we'll discuss throughout this book.

You may wonder why you should have to champion this cause on behalf of your entire organization and push for a budget or authorization to create a BC/DR plan. The truth is that you shouldn't, but since a disaster will probably have a disproportionately high impact on the IT department, it's very much in your own self-interest to try to get the OK to move forward with a planning project.

In this chapter, we'll look at some of the impediments to BC/DR planning as well as some of the compelling reasons why spending time, money, and staff hours on this is well worth the expenditure. We'll provide you with specific, actionable data you can use to convince your company's executive or management team to allocate time and resources to this project. We'll also look at the different types of disasters that need to be addressed—they're not all obvious at first glance. Finally, we'll provide a framework for the rest of the book and for your BC/DR planning.

BUSINESS CONTINUITY AND DISASTER RECOVERY DEFINED

Before we go too far, let's take a moment to define BC/DR. These two labels often are used interchangeably, and though there are overlapping elements, they are not one and the same. *Business continuity planning* (BCP) is a methodology used to create and validate a plan for maintaining continuous business operations before, during, and after disasters and disruptive events. In the late 1990s, BCP came to the forefront as businesses tried to assess the likelihood of business systems failure on or after January 1, 2000 (the now infamous "Y2K" issue). BCP has to do with managing the operational elements that allow a business to function normally in order to generate revenues. It is often a concept that is used in evaluating various technology strategies. For example, some companies cannot tolerate any downtime. These include financial institutions, utility companies, healthcare organizations, credit card processing companies, high volume online retailers, and others. They may decide that the cost for fully redundant systems is a worthwhile investment because the cost of downtime for even 5 or 10 minutes could cost millions of dollars or cause irreparable harm to the firm. These companies require their businesses run continuously, and their overall operational plans reflect this priority. Business continuity has to do with keeping the company running, regardless of the potential risk, threat, or cause of an outage.

Continuous availability is a subset of business continuity. It's also known as a zero-downtime requirement and is extremely expensive to plan and implement. For some companies, it may be well worth the investment because the cost of downtime outweighs the cost of implementing continuous availability measures. Other companies have a greater tolerance for business disruption. A brick-and-mortar retailer, for example, doesn't necessarily care if the systems are down overnight

or during nonbusiness hours. Although it may be an inconvenience, a retailer might also be able to tolerate critical system outages during business hours. Granted, every business that relies on technology wants to avoid having to conduct business without that technology. Every business that relies on technology will be inconvenienced and disrupted to some degree to have to conduct business without that technology. The key driver for BCP is how much of a disruption to your business is tolerable and what are you able and willing to spend to avoid disruption. It's always a balance between the two. If money were no issue, every business using technology would probably elect to implement fully redundant, zero-downtime systems. But money *is* an issue. A retailer, a regional parts supplier, or even a large manufacturing firm can ill afford to spend a million dollars on fully redundant systems when their revenue stream for the year is \$5-\$10 million or even \$50 million. The cost of a business disruption for a company of that size might be \$25,000, \$100,000, or even \$1,000,000, and it would not justify a million dollar investment. On the other hand, a million dollar investment in fully redundant systems for a company doing \$5 billion annually might be worth it, especially if the cost of a single disruption would cost more than \$1 million. As previously mentioned, your BC/DR plan must be appropriate to your organization's size, budget, and other constraints. In later chapters, we'll look at how to assess the cost of disruption to your operations so you can determine the optimal mitigation strategies.

Disaster recovery is a part of business continuity and deals with the immediate impact of an event. Recovering from a server outage, security breach, or hurricane, all fall into this category. Disaster recovery usually has several discreet steps in the planning stages, though those steps blur quickly during implementation because the situation during a crisis is almost never exactly to plan. Disaster recovery involves stopping the effects of the disaster as quickly as possible and addressing the immediate aftermath. This might include shutting down systems that have been breached, evaluating which systems are impacted by a flood or earthquake, and determining the best way to proceed. At some point during disaster recovery, business continuity activities begin to overlap, as shown in [Figure 1.1](#). Where to set up temporary systems, how to procure replacement systems or parts, how to set up security in a new location—all are questions that relate both to disaster recovery and business continuity but which are primarily focused on continuing business operations. [Figure 1.1](#) shows the cycle of planning, implementation, and assessment that is part of the ongoing BC/DR maintenance cycle. We'll discuss this in more detail later, but it's important to understand how the various elements fit together at the outset.

COMPONENTS OF BUSINESS

There are many ways to break down the elements of business, but for the purposes of BC/DR planning, we'll use three simple categories: people, process, and technology. As an IT professional, you understand the importance of the interplay among these three elements. Technology is implemented by people using specific processes.



FIGURE 1.1

Business continuity and disaster recovery cycle.

The better defined the processes are, the more reliable the results (typically). Technology is only as good as the people who designed and implemented it, and the processes developed to utilize it. As we discuss BC/DR planning throughout this book, we'll come back to these three elements. When planning for BC/DR, then, we have to look at the people, processes, and technology of the BC/DR planning itself as well as the people, processes, and technology of the plan's implementation (responding to an emergency or disaster). Let's look at each of the three elements in this light. [Figure 1.2](#) depicts the relative relationship of people, process, and technology in most companies. Infrastructure is part of the technology component but is listed separately for clarity.

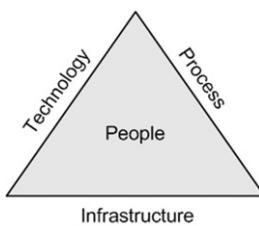


FIGURE 1.2

People, process, technology and infrastructure.

People in BC/DR planning

Clearly, people are the ones who do the actual planning and implementation of a business continuity and disaster plan, but there are many aspects to the *people* element that often are overlooked during the planning process. In this section, we'll look at a few of the commonly missed elements. However, as you read through this, keep your own organization in mind. Every company is different, and therefore, every BC/DR planning process will have to be different. A small retail outlet's IT planning for BC/DR will be very different from a call center, hospital, accounting firm, or a manufacturing facility. There is no "one size fits all" approach, so although we can point out the major elements, you'll need to fill in the specifics for your company.

Let's begin with one very interesting fact. According to a survey completed in 2010, human error is responsible for 40% of all data loss, as compared to just 29% for hardware or system failures. An earlier IBM study determined data loss due to human error was as high as 80%, so we know it's somewhere in that range ([Woodie, 2010](#)). That's the *people* part of the equation. People are responsible for designing, implementing, and monitoring processes intended to safeguard data. However, people make mistakes every single day. As one National Transportation Safety Board official put it when interviewed about a plane crash, there are multiple layers of systems in place to ensure the plane doesn't crash, but sometimes a series of bad choices or errors lead to a critical event. The same is true with your IT infrastructure. Hopefully, there are multiple layers of processes, procedures, and cross-checks in place to prevent human-caused disasters,

but sometimes, these fail. If 40-80% of data loss is attributable to human error, that leaves 20-40% of data loss attributable to other causes such as hardware and systems malfunctions, natural disasters, and terrorism (which is in the same general category of “human-caused” but at a different level altogether).

We’ll discuss the specific steps needed to form your BC/DR plan later in this chapter and in subsequent chapters. Now, though, let’s look at some general guidelines. Your BC/DR plan requires people from across your organization in order to be effective. As an IT professional, you may know who has which laptop and how applications are secured across the network, but you very likely have no idea how things run, on a day-to-day basis, in other parts of the company. You may not know what data, what processes, and what parts of the technology puzzle are critical to various departments. You certainly will not know critical dates, key milestones, or other information that people in other departments know. To create a plan without input from across the company almost guarantees the plan will fail—if not during the planning stage then certainly in the implementation stage. Getting key people in the company to participate in the planning helps you develop a more robust plan and, just as important, helps you identify the key people needed to implement the plan, should that become necessary.

Another key aspect to people in BC/DR planning is that it’s critical to remember that if a disaster hits your company, people will have a wide variety of responses. Some people, especially those with emergency preparedness training, will rise to the occasion and start taking effective action through leadership roles. Others will be completely overwhelmed and unable to act effectively (or at all). As was seen in many natural disaster responses over the years, people are often without food, shelter, power, or cellular service. Regardless of their willingness to respond, they may be unable to give the physical environment that surrounds the disaster. Understanding this is important when creating your BC/DR plan because it will not be “business as usual” when an emergency hits. Emotional and physical stress may reduce effectiveness of even the most prepared individuals, circumstances will force some staff to be unavailable, and worst case, some staff may not survive a disaster, so working with the assumption that addressing issues with people may be your biggest challenge will help ensure a successful plan and, more importantly, a successful outcome when the plan needs to be implemented.

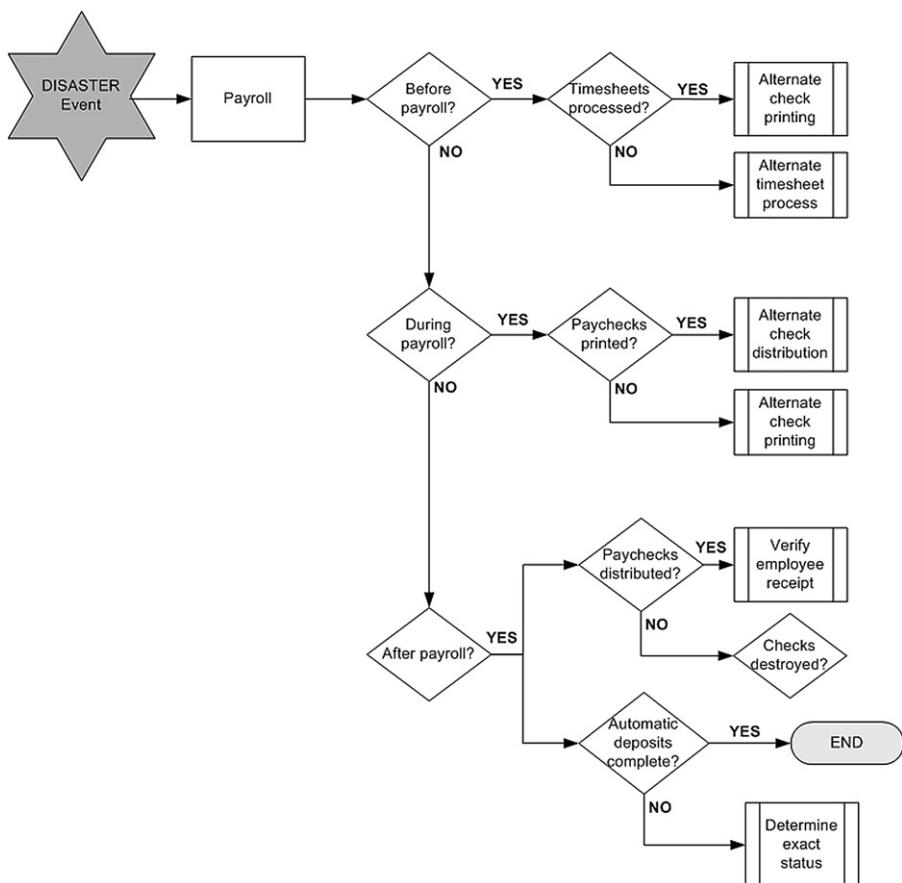
As an IT professional, it may be that you do not have primary responsibility for your company’s BC/DR planning. That said, you may be the only person in the company that recognizes the need for this type of planning. Therefore, you may have to champion the cause and rally resources to get the planning going. If you’re a senior manager in a small- or medium-sized firm, you may, in fact, be the go-to resource for both the planning and implementation of a BC/DR plan. Regardless of your role, we will discuss the broader implications of BC/DR throughout so you can either include them yourself or ensure that others in the organization are including them. Our objective is to help you create a simple, but effective, BC/DR plan for IT, but that cannot be accomplished in a vacuum. It will need to be integrated across the organization in order to be effective when it counts—when things go wrong.

Process in BC/DR planning

Process in BC/DR planning also has two phases: the planning phase and the implementation phase. The processes your company uses to run the day-to-day business are key to the long-term success of the business. These processes were developed (and hopefully documented) in order to manage the recurring business tasks. Things outside the normal recurring tasks typically are handled as exceptions until they recur often enough to create a new process, and the cycle continues. If your business is suddenly hit by a disaster—fire, flood, earthquake, or chemical spill—your processes are immediately interrupted. How quickly you recover from this and either reimplement or reengineer your processes to get the business up and running again relies on the processes delineated in your BC/DR plan. By developing a process for handling various types of emergencies and disasters, you can rely on these when people are stressed and business is interrupted. Trying to develop effective processes in the face of an emergency is usually not at all successful. Having simple, well-tested processes to rely on when disaster strikes is often the difference between eventual recovery and business failure.

As you'll see later in this book, the processes used by the company in day-to-day operations need to be evaluated and prioritized. What processes are critical to the ability of the company to conduct operations? What processes can be put on hold during an emergency? Circumstances surrounding the emergency certainly come into play—time of year, where you are in various business cycles, and so on. When looking at your payroll process during an emergency, for example, you'll also need to understand the normal timing of these processes within the company. A power outage right *after* payroll is processed may be far less critical than a power outage just before payroll is processed. As we look at processes within the company, we'll keep these kinds of timing issues in mind. However, this is another justification for having a wide array of interests represented during the BC/DR planning phases, so you can evaluate these aspects and factor them in appropriately. Let's look at an example from the Human Resources department. In [Figure 1.3](#), you can see a portion of a simple flowchart that HR could construct to assist both IT and HR in the aftermath of a disaster.

As you can see in [Figure 1.3](#), there are defined steps in your company's payroll process. These steps become the framework for a decision flowchart to help HR staff determine what steps need to be taken in the aftermath of a significant event with regard to payroll processing. The first step is to determine the exact status of payroll—did the disaster hit before, during, or after payroll? Then, depending on the status, what would be the appropriate steps to take and how can these steps be taken if key systems are down? Although you might think that payroll should be the least of your company's concerns in the immediate aftermath of a disaster, your company's employees will think otherwise. They may need to seek alternate accommodations such as staying in a nearby hotel or they may need to purchase food, medical supplies, or transportation. They may be relying on that very paycheck in order to provide them adequate funds to pay rent or eat that week. Without addressing

**FIGURE 1.3**

Simple HR/Payroll flowchart.

payroll needs, your company will be unnecessarily increasing the stress levels for all employees, even those who may not be dependent on receiving those funds immediately. Perhaps more importantly, this issue might not matter on the first day or two after an event, but what happens if your company's building was destroyed in a fire and it will be weeks before you resume normal operations?

This procedure clearly helps HR understand the current process they use and what processes may be needed in the event of a minor, major, or catastrophic event. It might also help them see ways to improve processes in their current day-to-day operations since few of us ever take the time to map out key processes. You don't need to use flowcharts, though they do provide a good visual, but you do need to find some standardized method of evaluating processes and creating contingency plans. We'll discuss this later in the book in more detail.

Technology in BC/DR planning

Technology is clearly the piece of the puzzle that you, as an IT professional, will be most familiar with. As you participate in your company's BC/DR planning (or head it up, as previously mentioned), you will be in the best position to understand what happens with various technology components during different types of disasters. Part of the reason for BC/DR planning is to look at your use of technology and understand which elements are vulnerable to which types of disasters. A power outage, for example, impacts all the technology in a building. Suppose you have battery backup or generators for lights and certain computers but no power for air conditioning in Miami in July? Timing and circumstance come into play and working closely with your facilities team, for example, will help you look at the plan in a more holistic (and realistic) manner than you might on your own. Do you know where your building control systems are located? How are they managed and maintained? Do you have backups of that data? Is the system managed by the vendor? Is it hosted in the cloud? These are the kinds of questions you'll be asking and answering throughout this process.

As we look at BC/DR planning, we'll also look at various vulnerabilities of different technologies and discuss, in broad strokes, strategies, tools, and techniques that might be helpful to mitigate or avoid some of these risks. We won't delve into specific technology solutions as those are ever-evolving, but we will look at common methods used today and what needs to be considered as you look at your unique circumstances. In some cases, your BC/DR planning may yield information you can use to make the business case for why the firm should authorize the purchase of a particular technology or service. For example, if you've been trying to get funding approved for co-location services to speed up user access to critical business data across a wide geographic area, you can use the results of your BC/DR planning to add to the business case. Clearly, co-location can be part of a solid business operations management strategy and can also be an integral part of a BC/DR plan. When you can add strength to your business case, you're more likely to find executive support for funding.

As an IT professional, you will need to work closely with members of other departments to understand the technology needs in an emergency—not only what technology is needed to get the business back up and running (business continuity) but also what is needed to manage the crisis. These are two distinct (but overlapping) concerns that should be assessed and addressed by your plan.

LOOKING AHEAD . . .

BC/DR Planning Resources

There are numerous organizations worldwide that focus on BC/DR planning. Many of these organizations provide training, methodologies, and certification tracks. For anyone interested in becoming a focused specialist in one of these areas, you would do well to investigate these various organizations. If you're involved with BC/DR planning and want to stay current on the latest trends from the field, be sure to bookmark a few of these sites. We've listed just a few

Continued

LOOKING AHEAD . . .—cont'd

here, but a quick Internet search will yield more resources. Please keep in mind, as with any URL listed in this book, Web sites and URLs can change.

- The Business Continuity Institute (UK): www.thebci.org (The Business Continuity Institute, 2013)
- DRI International (USA): www.drii.org/DRII/index.htm (DRI International, 2013)
- GlobalContinuity.com (South Africa): www.globalcontinuity.com (Global Continuity, 2011)
- Department of Homeland Security Business Readiness (USA): www.ready.gov/business/index.html (U.S. Federal Emergency Management Agency, 2013)
- Disaster Recovery Journal (USA): www.drj.com (Disaster Recovery Journal, 2013)

THE COST OF PLANNING VERSUS THE COST OF FAILURE

Companies typically look at their “top” line and their “bottom” line. Top line is revenue, and many publicly held companies chase after top-line growth, meaning they want to aggressively increase revenues. This often means they are grabbing a larger share of the market or are pushing the market to expand. It does not, however, account for the cost of doing so. If you pick up another \$100 worth of business but it costs you \$125 to do so, you may have top-line growth, but your bottom line (profitability) will suffer. In some cases, this makes sense in the short term—you can capture market share that becomes profitable at some later point in time. Other companies look just for bottom-line growth—revenues minus expenses (and other things) equals profit—so if a company’s revenues minus expenses are greater than past years, it means that the company has generated a larger profit (generally speaking). However, if your company is losing market share and lays off three-quarters of the workforce and closes four locations, things are not going well, even if you end up with short-term bottom-line growth. Therefore, most companies look for a balance between top and bottom-line growth.

You might be wondering what all this has to do with BC/DR planning, so let's connect the dots. The cost of planning might be significant in terms of staff time, resources, and the like, and might impact your bottom line (depending on many factors). If your company is concerned only with top-line growth, they may not be overly concerned with the cost of a BC/DR project plan. You may also find that key customers desire or demand that your company have such a plan, so you might argue that creating this plan could contribute to top-line growth. If you're able to capture a new customer because you have a BC/DR plan, that's clearly going to help your case. On the other hand, if you work for a company strictly concerned with bottom-line growth, you may have a bigger challenge. You can certainly see if having such a plan would improve operational efficiencies or land you a new client. Short of that, you might have to point out the potential hit to the bottom line if you experienced a disaster without a BC/DR plan in place. However, you can be sure that failure to mitigate the impact of a disaster will absolutely impact both your top

and bottom lines and will likely put your company's very existence in peril. Therefore, when you compare the cost of planning to the cost of failure, there is only one approach that makes business sense—and that is to plan to the extent it makes financial sense to do so.

Disasters can result in enormous business losses—financial, investor confidence, and corporate image. They can also lead to serious legal issues, especially when more and more private data are being captured, stored, and transmitted across the public Internet. These losses and legal challenges can have a small, short-term impact but more often than not, they have a significant, long-term impact, and in some cases imperil the existence of the company. For more information on the legal implications of disasters and data security, be sure to read [Chapter 2](#) as well as the case study by Deanna Conn, a well-respected IT attorney, which follows [Chapter 2](#).

In companies that do have some sort of disaster plan in place, it more than likely resides in or originates from the IT department. IT staff have long understood the business implications of the outage of even one server (Help Desk phones ringing off the hook is one measure of the importance of even a single server or business application). However, it's also clear that IT equipment—routers, servers, switches, hubs, firewalls, and more—is just part of the overall business equation. Certainly, without these technology components in place, business as usual will be limited at best. However, without also considering the way in which your company earns income and the way in which it conducts its business, all the IT planning in the world won't protect a company if a disaster strikes. A holistic approach to the business is needed in order for any BC/DR planning to be realistic and effective. This involves every key area of your business and the various stakeholders that represent those business units. It won't help if you can keep your Web site's e-commerce functions up and running if your warehouse operations have come to a screeching halt. We've included four industry spotlights in this book as a way of engaging you in discussion around various aspects of BC/DR. As you'll see when you read these industry spotlights, the overarching theme is that success starts with a strong understanding of the operations of your company, outside the IT department. This is the foundation of any solid BC/DR plan and you'll see this theme woven throughout this book along with tips on how to gain that understanding as well as real world input from IT professionals who have been through several iterations of BC/DR planning.

Most IT departments have some minor disaster recovery procedures in place. If your firm performs backups of critical data on servers, you have basic disaster recovery capabilities, assuming those backups are taken off-site or are stored (or performed) remotely. Though you might think this is quite obvious, you might be surprised to know how many companies (and IT professionals themselves) either fail to make backups or fail to store them in a safe location. However, many small, medium, and certainly most large companies at least have a reasonable data backup solution in place. This, in and of itself, is a good start but does not constitute a BC/DR plan. For example, if your area was flooded and you were unable to enter your building, could the company continue operations? If this is one location out of many, perhaps. If this is your only location, perhaps not. It depends, of course, on the nature of

your business. If you have a warehouse full of product that is also underwater, you might have contracted with your suppliers to direct ship to customers in the event of a disaster. Did you also develop a plan for how customers would place orders or how you would track and invoice those orders? Clearly, the technological component is a critical link in the chain, but it's not the only link. Throughout the remainder of the book, we'll look not only at the IT components but the other non-IT elements that need to be in place as you develop your BC/DR plan so that you don't overlook any crucial aspects of the business.

Disaster planning is about recovering after an event, but BCP is not just about recovering from outages of key technical components, it is a way of looking at and managing business. BC planning is about looking ahead and seeing what could potentially disrupt your company's operations and then finding ways to mitigate or avoid those events. It really is a coordinated and integrated approach that spans the entire company and all its operations. As in any other area of life, one or two poor decisions can usually be corrected or overcome, but when things get stressful, it's highly likely that a string of poor decisions could literally spell disaster for your company. The point of BC/DR planning is to help avoid those pitfalls that can be avoided and to provide a sane, rational, well thought-out approach to managing the disaster when an event does occur. If the number of poor decisions can be held to a minimum, there is a stronger likelihood that you will avoid compounding the problem and perhaps even be able to come out of it quickly and in relatively good shape.

BCP is something many small companies simply don't think about at all; it's something larger companies can afford to put resources on but often are reluctant to spend more than a small percentage (some estimates put this number at 1% of revenues) on BC/DR. It's astounding that companies spend so little on an activity that literally could mean the difference between remaining in business and closing the doors.

According to the U.S. Small Business Administration, 25% of businesses that experience a data loss never reopen, but, more alarming, 90% of small business struck by disaster close after 2 years. If they survive in the immediate aftermath (only 75% will), those remaining will almost certainly fail sometime within the following 24 months ([U.S. Small Business Administration, 2013](#)). FEMA sees it a bit differently for businesses overall, but no more optimistically—their statistics indicate that 40% of businesses fail after a disaster and another 25% fail within the first year ([U.S. Federal Emergency Management Agency, 2013](#)). Regardless of how you view it, the numbers come out stacked against businesses of any size surviving disasters. Looking specifically at fires, the most common disaster businesses experience, it is estimated that 44% of companies whose premises experience a significant fire do not recover at all, primarily because they have no BC/DR plans in place. The World Trade Center bombing in Manhattan in 1993 resulted in 150 out of the 350 businesses located in the center going out of business—that's about a 42% failure rate. Contrast that with many of the financial firms who had well-developed and tested BC/DR plans that were located in the Twin Towers on September 11, 2001—a majority of them were back up and running within days. More recently, Hurricane Sandy

flooded lower Manhattan and the New York Stock Exchange had to suspend operations because of power loss and flooding, but firms in the area were able to quickly transfer operations to data centers outside of the storm's path and dramatically reduce the impact to their business. The evolution of IT architecture is largely responsible for these improvements in BC/DR functions. As we'll discuss throughout this book, incorporating BC/DR planning in your daily operations can help create an enterprise architecture that is resilient, reliable, and easily managed across two or more data centers.

Small businesses, those most likely to avoid, delay, or short-cut BC/DR planning, are most susceptible to the long-term impact of emergencies and disasters. Yet, these same small companies are the economic engine of many economies around the world. In the United States, small businesses account for 99.7% of all U.S. businesses employing 49.2% of all private sector employees, creating 64% of net new private sector jobs ([U.S. Small Business Administration Advocacy, 2012](#)). Small businesses are critical to the U.S. economy, and yet they are most prone to failure during a disaster. Private insurance and government assistance aside, small businesses have the most to gain by creating a solid BC/DR plan—and the good news is that for small businesses, there are numerous leading edge technologies that can dramatically reduce your risk and increase your resilience. If you work in a small business IT department (or you are the IT department), be sure to read [*Industry Spotlight #4—Small/Medium Businesses*](#) for a focused discussion.

Regardless of the size of your company, the odds are high that if your company experiences any sort of disaster—natural or man-made—it has better than even chance of going out of business as a result. Certainly, the strength of the company, the industry, and other factors come into play when looking at long-term survival of companies hit by disasters, but it's clear that if your company doesn't have a BC/DR plan, it is essentially taking a 50% chance on failing. Without a well-conceived BC/DR plan, that's an enormous gamble to take. It impacts not just the corporate entity itself but the lives of all the employees, the local community, and your suppliers as well.

There are many people who will counter with the argument that a company could spend a lot of money on planning and *never* have to deal with a disastrous event. True. And that is often the argument used by businesses to avoid undertaking the time or expense to create a BC/DR plan. Many people drive their entire lives and never have a single auto accident, but they probably all have auto insurance. Clearly, the question is one of balance. If your company does \$50M in annual revenue, a cost of \$1M for BC/DR planning is very little to pay for that type of insurance. If your company does \$1.25M annually, you probably don't need to (and can't) spend \$1M on BC/DR planning. Obviously, the cost of planning must be balanced with the cost of doing nothing and the risk of going out of business. Like auto insurance, you certainly hope you'll never need to use it, but you don't want to get caught without it either. Ultimately, it's less expensive to expend an appropriate and proportionate amount of time and resources to create and maintain the plan than to face even one disaster without a plan. As we proceed through this book, we'll take this into account. For example, if your company is in the Gulf States region of the United

States, you need to have an emergency plan in place in the event a hurricane hits the area, as has happened repeatedly in the past few years and certainly will again in the future. On the other hand, if your firm is located in the desert southwest of the United States, you don't need to plan for hurricanes, but you will have to plan for power outages, flash floods during storm season, and lightning strikes. Even though this is obvious, it bears mentioning because you don't need to over-engineer your BC/DR plan. You will need to evaluate the potential impact to your company of various types of events and then create a plan for just those events most likely to occur and most likely to have a critical impact on operations. When you do this, you use your planning time effectively, and the cost of planning will certainly be far lower than creating an all-encompassing plan or the cost of facing a disaster empty-handed. This is a key concept you'll see discussed throughout this book as well—the plan must address the most likely threats in a fiscally responsible manner because your company most likely does not have an open checkbook when it comes to IT expenditures for BC/DR.

While we're on this topic, let's take a moment to look at how the cost of planning (investment) and the cost of failure (loss) impact the people, processes, and technology of a company. The impact, though not immediately apparent, is significant and worth exploring briefly.

REAL WORLD

A Bad Plan Versus No Plan . . .

A bad plan or incomplete plan is often worse than no plan at all. An ill-conceived or incomplete plan may lead people to mistakenly assume that emergency and contingency plans are in place when, in fact, they are not. A false sense of security can lead to an even bigger problem than the disaster event itself precipitates. Remember, if a disaster strikes your area, emergency personnel will be going to hospitals, nursing homes, day care centers, and schools to help. Your business, unless one of the aforementioned, will be pretty low on the list of priorities, so you need to be prepared to take matters into your own hands. If employees falsely believe the company is prepared for disaster, you're facing a whole host of problems. A poorly conceived plan may also lead to significant financial penalties and legal liabilities since it might be argued you had the opportunity to plan and failed to do so.

People

Spending time and resources to plan for emergency responses, from an organizational perspective, is an excellent investment for many reasons. One that might not be immediately evident is that when employees understand that the company has contingency plans in place, they tend to feel that the company is organized, positioned for success, and concerned for their safety. It provides an opportunity for the company to demonstrate its commitment to its employees' well-being, which can help retain key employees. Companies that run in a perpetual ad hoc manner are often more at risk of losing key employees for this same reason. Will a solid BC/DR plan keep employees happy? Of course not, but it does contribute to an overall environment that fosters respect and concern for employee well-being.

In addition, a crisis that is well managed by the company is less likely to cause key employees to seek employment elsewhere. A well-managed event also keeps employees calm and focused so business can get back to usual as quickly as possible. A well-managed crisis can also enhance a company’s reputation, leaving it stronger than it was before the incident. One example of excellent crisis management (not IT related) was when the Extra Strength Tylenol pain product was contaminated with cyanide in 1982. The company quickly asked retailers to pull *all* of its products from store shelves until it could understand the nature and extent of the “attack.” The year prior to the incident, Tylenol had about 35% of the billion dollar analgesic market or about \$350 million in annual sales. Immediately afterward, its market share was 0%. However, within 4 years, the company has regained almost all its former market share (98% of precontamination sales revenues). Although this example is outside the domain of IT professionals, it points to the opportunity a company has to manage an emergency. It gets one shot to get it right, and its future reputation rides on the decisions made during the crisis. Today, the “Tylenol incident,” as it is sometimes referred to, is discussed in business school case studies and is held up as an excellent example of how a company can and should respond to a crisis (Harris et al., n.d.).

The effect of stress on people during an emergency cannot be overemphasized. Having a well thought-out and well-rehearsed BC/DR plan will reduce that stress considerably. In turn, people will be able to function again and return to their jobs more quickly. Thus, the very act of planning how to take care of the people in your organization during an emergency can quickly impact the company’s ability to return to normal operations—and revenue generation. BC/DR planning, then, directly impacts the top and bottom line, and the cost of planning will quickly offset the cost of an unmanaged event.

Process

BC/DR planning can provide an opportunity for a company to evaluate and improve its business processes. As your project team (we’ll discuss the team later in the book) evaluates business processes as it relates to BC/DR, it might discover new ways to streamline operations. For example, in planning for a major disruption due to a natural disaster, your team might uncover new methods while determining “bare minimum” requirements. If a process takes 20 steps and four departments now, you might find that the pared-down approach discussed in a postdisaster scenario would actually work well all the time. When you’re forced to look at everything from the ground up, which is what happens when you’re dealing with a disaster, you discover that you don’t need all the bells and whistles. This can sometimes translate into streamlined processes that can be incorporated into the day-to-day operations. If you’re undertaking any sort of Six Sigma, Agile, or Lean initiative, you can certainly incorporate these results of those efforts into your BC/DR planning process. Reducing steps, avoiding waste, and streamlining processes are all good business practice, and they’re especially helpful in a disaster when things are stripped to the bare minimum.

In addition, documenting critical business processes can truly mean the difference between life and death for the corporate entity. If you are unable to resume some

sort of operations in a reasonable time frame after a disaster, your company is not likely to survive. The cost, then, may be the ultimate corporate cost—failure to exist. This is not only unfortunate for the corporate shareholders (whether publicly or privately held), but it impacts the lives of all the company’s employees and their families and takes a toll on the community as well. The ripple effect is enormous and should not be quickly discounted.

Technology

Scrambling to deal with technology issues once a disaster has hit is guaranteed to cost your firm more than if you have a solid plan in place beforehand. For example, if you need temporary computing facilities, it’s less costly to have a contingency contract in place in advance than to desperately call various facilities looking for assistance while the smoke clears. Not only will you be in a better frame of mind emotionally in the planning phase (vs. the reaction phase after a disaster), you’ll be in a much stronger position to negotiate the details of a contingency contract.

In addition, if the disaster impacts other companies, it might also create a competitive situation that drives the price for technology components up. Again, being able to calmly negotiate and procure commitments for emergency services beforehand almost always generates lower costs when those contracts are activated by an emergency. Finally, it is customary for most companies to provide service to contract holders before they provide service to noncontract holders. If you’re currently a customer, you’re going to get service before the person who just called in today looking for assistance. So, prenegotiating anticipated emergency services can generate lower costs and a higher ROI on your BC/DR planning process.

REAL WORLD

Dealing with Optimists and Pessimists

When developing your BC/DR plan, you have to find some balance between the optimists and the pessimists. The optimists will dismiss many potential risks and dangers and will often minimize the potential impact of events. On the other hand, pessimists believe every possible danger is likely to occur and would have a much larger impact than it likely would should it occur. Part of your job is to try to remain balanced and realistic, especially when it comes to developing mitigation strategies, which we’ll discuss later in [Chapter 6](#) of this book. Additionally, many BC/DR planners place a disproportionate amount of time and attention on major catastrophes. As you’ll see, we first look at the most common disaster scenarios like fire and flood and then turn our attention to major events such as hurricanes, tornadoes, and earthquakes. The thinking is this: If you spend time to prepare for the common, smaller events, you can then perform a second round of planning for major catastrophes or create two different planning teams. If you’re ready for the next Category 5 hurricane but you fail to have a solid plan in place for a workplace fire (the most common business emergency), you’ll be doing yourself, your employees, your company, and your community a disservice. So, in the end, you will need to balance the need for disaster planning with the financial and organizational constraints of your company and focus on the smaller, more likely events first. This can best be accomplished by listening to both the optimists and the pessimists and finding acceptable middle ground.

TYPES OF DISASTERS TO CONSIDER

So far, we've spent time talking about *why* it's important to plan for disasters. Now, let's turn our attention to the types of disasters that might occur. The reason for this is that there may be a few you don't think of immediately (or at all) that might potentially impact your company. Although this list is extensive, it is certainly not exhaustive. Throughout this book, we'll give examples of a variety of disasters because we want to make sure you cover all your bases and think through all potential threats to your company. You and your BC/DR planning team should be sure to look at your company's specific location(s), your industry, and your operations to determine exactly what types of disasters and events could have a significant impact on you. This list should be a good starting point and might also spark ideas about other elements that could be essential to include in your company-specific plan. Not only is it important to review the entire list and be sure you've covered your bases, you also have to start with the more likely events and move outward from there. As mentioned, fire is the most common business emergency that most companies face. So, if you don't have an established fire response plan, you're really a sitting duck. As you'll see in [Chapter 4](#), the risk assessment should be holistic and broad in scope, but it should also then narrow down your focus to those risks that are most likely to occur and that will have the biggest impact on your company's operations.

As an IT professional, your job may be limited to dealing with just the technology aspects of the BC/DR plan, but you need to be aware of all the various threats because your company will be relying on you to understand and address the potential impact of threats on the company's technological operations. Technology is so pervasive in most organizations these days that IT will be one of the key drivers in both the planning phase and the implementation/recovery phase. Therefore, it's critical that you and your IT team be well versed in all aspects of BC/DR planning.

Threats or hazards come in three basic categories:

- Natural hazards
- Human-caused hazards
- Accidents and technological hazards

Clearly, natural hazards are the ones that can sometimes be anticipated and the effects mitigated; other times, they come without warning and must be responded to. Human-caused hazards also can sometimes be anticipated and other times come as a surprise. Finally, accidents can happen and accidents span the range from minor to major to catastrophic. Included in this category are what often are termed "technological threats" because they involve the failure of buildings or infrastructure technology. We'll look at these types of threats in more detail later in the book.

The list of disasters within each of these categories is long (refer to [Chapters 4, 5](#), and [Appendix A](#)) and is enough to keep you awake at night. Unfortunately, these are all incidents that can and have occurred, and the best way to deal with these kinds of unimaginable uncertainties is to imagine them and develop a methodical plan for

handling them. To be sure, if one of these more major events occurs and you have to deal with it, it's unlikely you'll follow your plan to the letter. It's impossible to imagine everything you'll be experiencing and have to deal with until you're in the middle of it. Having a solid plan in place that's been tested and practiced will reduce the stress of the situation and increase the likelihood that you've anticipated the major issues you'll need to address. In dire circumstances, that can mean the difference between surviving or not, between recovering or not.

REAL WORLD

Corporate-Wide Participation

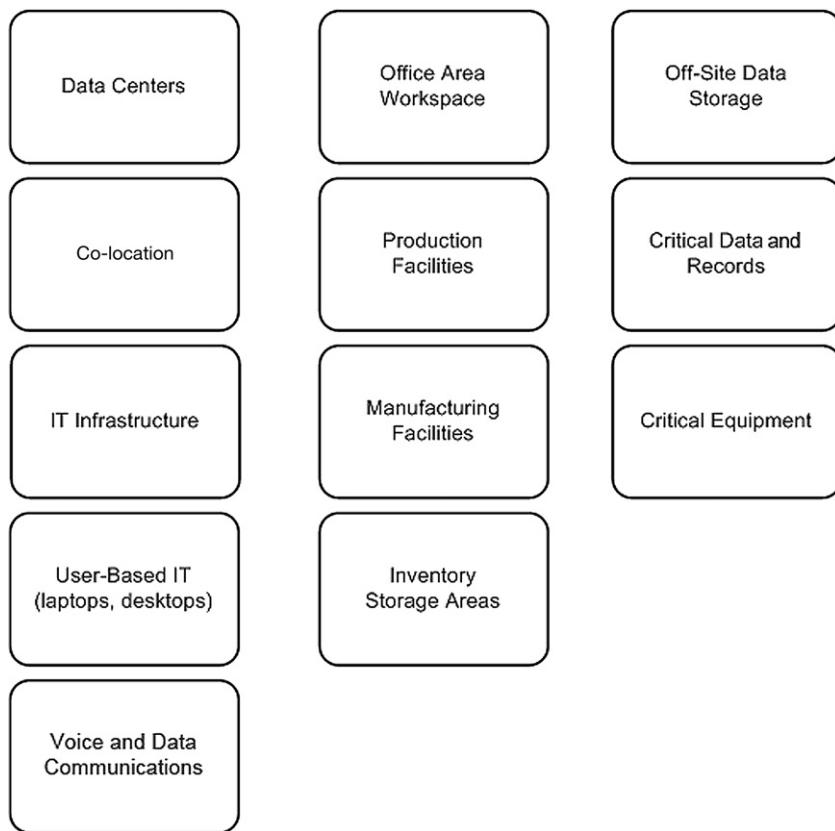
Although your specific role in the company may not bear responsibility for business continuity and disaster planning, you may need to lead the charge. As an IT professional, you understand the immediate implications of a power outage or a cyber-attack or even a building evacuation on your business. If you're leading the BC/DR planning, you'll need to educate yourself to the larger business issues for two reasons. First, you'll need to understand the broader business issues involved with BC/DR, not just the IT issues. Second and perhaps more important, you'll need to gain executive support for your BC/DR planning initiative. Executive support is key to success for any type of project, and this is no exception. If the folks "upstairs" don't support the project, you'll have a hard time gaining the authority, funding, staffing, or resources needed to create a successful BC/DR plan. Going through the motions without creating a workable plan is almost worse than having no plan at all—it may provide a false sense of security to your organization. If or when disaster strikes, your plan has to work, it can't just be words in a document. Gaining executive support, a topic we'll discuss in [Chapter 3](#), is key to success, as is participation across the organization.

BUSINESS CONTINUITY AND DISASTER RECOVERY PLANNING BASICS

Your role as an IT professional is unique in BC/DR because on one hand, you are not necessarily responsible for the company's comprehensive BC/DR planning, but on the other hand, technology is so integral to most corporate operations, IT can't be completely separated out as a stand-alone issue. As a result, we will continually address BC/DR in a holistic manner and allow you to determine the most appropriate role for your IT group within your company.

The elements that should be included in your plan will extend beyond the walls of the IT department, so you'll need to form a project team with expertise in several areas. [Figure 1.4](#) shows some of the areas that might be included, depending on the type of products and services your company creates.

You're no doubt familiar with the concept of *reliable system design* and *single point of failure* when it comes to designing, implementing, managing, and repairing the IT infrastructure for your company. Briefly, these concepts relate to building in redundancies and safeguards so that if one key component fails, the entire company doesn't come to a screeching halt. You probably also understand that having two servers or routers in the same rack leaves your network vulnerable—the single point of failure could be as simple as someone tripping and spilling a large cup of coffee on

**FIGURE 1.4**

Subject matter expertise needed for BC/DR planning.

the rack itself (granted, they have no business bringing coffee into the data center, but that's another issue that goes back to how much data loss is caused by humans...). You might conscientiously make backups, verify the backups, and store them securely but leave them on-site. The single point of failure could be as minor as something falling on the rack holding your tape backups or as major as a serious fire in the server room or building.

The reason for discussing this concept at this juncture is that as you look at your BC/DR options, you need to assess your risks with regard to reliable systems and single points of failure. For example, you may want to evaluate your availability solutions as part of an overall business strategy to reduce operational risks, minimize the occurrence and cost of downtime, and maximize data and IT service availability. These availability solutions will also likely impact your compliance with a variety of regulations by providing protection and reliability of information resources as well. Additionally, these solutions will impact your BC/DR risk assessment and planning.

If these solutions are not currently in place, this BC/DR planning process may help you build the business case for implementing some of these technologies. If they are currently in place, you can look at them with a fresh perspective to determine how they contribute to an overall business continuity strategy. We'll discuss this in more detail in [Chapter 4](#).

With that, let's look at contingency planning basics: the steps to be taken to create a solid BC/DR plan for your company. The basic steps in any BC/DR plan, shown in [Figure 1.5](#), include:

- Project initiation
- Risk assessment
- Business impact analysis
- Mitigation strategy development
- Plan development
- Training, testing, and auditing
- Plan maintenance



FIGURE 1.5

Basic business continuity and disaster recovery planning steps.

Those of you familiar with project management (PM) methodologies will notice the similarity in the BC/DR planning process to PM processes and with good reason. Creating a BC/DR plan can (and should) be approached as a discrete project that has a defined start, middle, and end. As with many other IT projects, once the BC/DR plan is completed, it must be maintained so that it stays current with changes in the company, its technology, and the broader business landscape. We'll discuss each of the sections here briefly to provide an overview, and we'll delve more deeply into each of these areas in subsequent chapters.

Project initiation

Project initiation is one of the most important elements in BC/DR planning because without full organizational support, the plan will be incomplete. As an IT professional, there may be limits to what you can do to create an organization-wide functional BC/DR plan. For example, you may know how to set permissions for a particular business application, but do you really know how users interact with it and what would be required to get the business back up and running with regard to that particular business function? If the application server is destroyed and you have data backups, do you also have a way to access those backups? Do you have a way to allow users to connect to the application securely? Where are users located?

How will business resume? Can it resume without that application in the near term or not? You will not likely be able to answer these questions. It requires the input and assessment from subject matter experts in other departments and divisions. Therefore, getting executive and company-wide support for the BC/DR planning process is absolutely key to its success. We'll discuss this in more detail in [Chapter 3](#).

Risk assessment

Risk assessment is the process of sitting down with key members of your company and looking at the potential risks your company faces. These risks run from ordinary to extraordinary—from a fire or minor flood in a server room to a catastrophic loss such as an earthquake or major hurricane and everything in between. You can refer to [Appendix A](#) for a list of the most common types of threats as a starting point (also see [Chapters 4](#) and [5](#)). Again, as an IT professional, you can certainly lend your expertise to this process by helping define the likely impact to technology components in various types of disasters or events, but you can't do it alone. For example, it's likely that your transportation manager understands the potential business impact of bad weather around the country, not just in your local area. Your marketing manager might best understand the potential business risk of a contaminated product or a Web site breach. Some of these areas may fall into pure BCP and may be more suitable for others in your organization. However, in almost all companies, IT expertise must be included in the BC/DR risk assessment process. In [Chapter 4](#), we'll discuss risk assessment in depth.

Business impact analysis

In a sense, this is where “the rubber meets the road.” Once you've delineated your risks, you need to turn your attention to the potential impact of these various risks. This is one area that, as an IT professional, you clearly need input from your company's experts. As mentioned earlier, you might understand the technical aspects of an application server going down, but what is the actual business impact and can that be tolerated? For example, you might determine that your Enterprise Resource Planning or your Electronic Medical Record application cannot be down. Period. E-mail, Web servers, and reporting tools, however, can go down, even though both events would be disruptive. Once you understand these parameters, you can develop an IT-based strategy to meet the requirements that result from this analysis. We'll look at business impact analysis and how IT interacts with this process in [Chapter 5](#).

Mitigation strategy development

If you're part of a small company, your mitigation strategy might be quite simple. Keep critical data backed up to a secure cloud location, keep several copies

of backups off-site, and keep several copies of key information such as employee list, phone numbers, emergency service phone numbers, key suppliers, and customers in a binder off-site in a secure but accessible location. That might be the extent to which you choose to mitigate your risks. However, for most companies, the process is a bit more complex. For each identified risk that has a significant business impact, you need to look at your options. How can the risk and impact be tolerated, reduced, avoided, or transferred? We'll discuss mitigation strategies in [Chapter 6](#).

Plan development

After you've gone through the analysis steps, you'll be ready to develop your plan. As with other types of IT project plans, you'll want to outline the methodology you're going to follow so that you improve your chance of success and reduce your chances for errors and gaps. This includes standard processes such as developing business and technical requirements, defining scope, budget, timeline, quality metrics, and so forth. We'll discuss these elements in [Chapter 7](#), and we'll use standard IT PM methodologies to help you create a solid plan, regardless of the size of your company.

Training, testing, and auditing

Once the plan has been developed, people need to be trained on how to implement it. In many cases, scenario-based case studies can be a good first step (though this may be part of the plan development stage as well). Running through appropriate drills, exercises, and simulations can be of great help, especially for disasters or events that rank high on the list of "likely to occur." In [Chapter 8](#), we'll discuss emergency preparations. Then, in [Chapter 9](#), we'll look at some of the ways you can train, test, and audit your plan so that you can develop a process that closely tracks with your company and the way it operates.

Plan maintenance

Finally, plan maintenance is the last step in the BC/DR planning process, and in many companies, it is "last and least." Without a plan to maintain your plan, it will become just another project document on a file server or sitting in a binder on a shelf. If it doesn't get maintained, updated, and revalidated from time to time, you'll find that the plan may be rendered useless if a disaster does strike. Maintenance doesn't have to be an enormous task, but it is one that must be done. Most importantly, there must be an organizational commitment to do so and someone within the company to own it. We'll look at this in [Chapter 10](#) and provide some tips on how to incorporate these tasks into your day-to-day operations to reduce the ongoing burden of plan maintenance.

LOOKING AHEAD...

IT, Security, Disasters...and the Law

One of the strong trends in IT and IT security is the increased demand that companies secure private data such as social security numbers, credit card numbers, home addresses and phone numbers, financial data, medical data, and more. As the amount of electronic data collected and stored increases, so too does the risk to individuals. Recent headlines are rife with examples of personal data being lost, stolen, hacked, or modified. Companies can no longer say “we did our best” without proving that their best was at least up to current industry standards. Looking ahead, companies can expect three major trends to impact how they manage IT security. These standards will apply during normal business operations and emergencies—companies won’t be able to easily blame breaches and theft on emergencies that were foreseeable and manageable, as is the case with many of the disaster events listed earlier in this chapter. These three key trends, which you should monitor for your IT organization, are:

- The continuing expansion of the requirement to provide IT (and data) security
- The emergence of a standard definition of “reasonable security”
- The imposition of the duty to notify after a security breach

Consumers and regulators alike are raising their expectations regarding IT security, and companies are both legally and ethically bound to make serious, effective efforts to safeguard private data. Emergency and disaster conditions may soften those requirements just a bit but don’t assume your company will be able to hide behind a disaster or event if data are lost, stolen, mishandled, or inappropriately disclosed. If your firm deals with data that are sensitive, confidential, or private in nature, consult with your firm’s legal counsel to understand fully the legal and regulatory requirements your firm will be subject to during a crisis, emergency, or disaster. In [Chapter 2](#) and the case study that follows it, we provide examples of the need for due diligence in handling electronic data regardless of whether you’re facing normal operational challenges or a major disaster.

SUMMARY

BC/DR are not new concepts to business, but the need to consciously assess and plan for potential problems certainly has been underscored by disastrous events in the past decade including earthquakes, tsunamis, hurricanes, typhoons, and terrorist attacks. Companies need to plan for potential disasters that will impact their ability to continue operations and earn income. Without a plan to recover from any disaster or event, no matter how large or small, many companies fail. The statistics speak for themselves. The odds are between 40% and greater than 50% that a company will fail after a fire or significant data loss, and only 6% of companies survive long term after a major incident.

When developing a BC/DR plan, you need to look at the three core components of business: *people, process, and technology*. When you take a holistic view of the company and its operations through the lens of these three elements, you’re more likely to understand the best approach to your own unique BC/DR planning process. People, process, and technology must be considered in an integrated and holistic manner since they are closely tied together.

Through your BC/DR planning process, you may find additional information you can use to support the purchase or implementation of a particular technology or service. If that technology or service will not only help day-to-day operations but will also fit nicely into a BC/DR strategy, you have effectively doubled the usefulness of the technology and reduced the perceived cost. Building the business case can help tilt the budget decisions in your favor. In addition, through reviewing business processes for your BC/DR plan, you may discover new or improved ways to run daily operations, which will add to the perceived value (or reduce the perceived cost) of your BC/DR activities.

In some companies, even a little downtime can be devastating, but in the majority of companies, some downtime can be tolerated, though it will be disruptive. You and your planning team will need to thoroughly assess the company's tolerance for downtime and disruption in order to develop an effective plan. We'll discuss this in later chapters in more detail. It's important to keep the business failure statistics in mind as you make your plans. Without a well-defined BC/DR plan, your company is putting the welfare of its employees, stakeholders (or shareholders), suppliers, vendors, and the community in which it operates at risk. Many BC/DR planning activities and remedies cost little or nothing to implement, so doing nothing is not an acceptable "no cost" option. It is simply imprudent and irresponsible for companies of all sizes to fail to plan.

Disasters impact different types of companies in assorted ways. A flooded retail location has a different set of challenges than a flooded nursing home. The impact of a biohazard incident is far different if it occurs at or near a day care center than near a remote manufacturing facility. As an IT professional, you and your team should fully understand the potential risks to your company in your location(s). As we move through this book, you'll learn how to prioritize and address a variety of risks and threats your company might face.

Also, we'll rely upon standard PM tools to help develop the BC/DR plan. For those of you with formal PM training and skills, these steps will be familiar. For those of you less familiar with these methods (or for those of you who hate a lot of "process"), don't be concerned. We'll review the necessary steps and provide plenty of guidance along the way. We'll avoid getting bogged down with the very fine, detailed aspects of PM. Instead, we'll simply use it as our framework to help guide us through the process of risk assessment; business impact analysis; mitigation strategy development; plan development; training, testing, and auditing; and plan maintenance.

KEY CONCEPTS

BC/DR defined

- Business continuity focuses on a company's ability to continue operations regardless of the nature of potential disruption.
- BCP is a formalized methodology that can be studied and for which practitioners can be certified.

- Disaster recovery planning is typically a subset of BCP because it deals with stopping the effects of the disaster or event.
- Once the effects of the disaster or event have been addressed, business continuity activities typically begin.

Components of business

- Businesses are comprised of people, process, and technology and related infrastructure. Each of these must be addressed in BC/DR planning.
- People are responsible for creating and implementing BC/DR plans. They are susceptible to the effects of a disaster including being overwhelmed with a variety of emotions, being physically injured (or killed), and being unable to perform their duties due to these and other influences that occur during a disaster.
- Processes are used in businesses to maintain an orderly and consistent flow of business operations.
- Business processes must be evaluated during BC/DR planning in order to determine which are the critical business processes and how they should be implemented in the face of a disaster or event.
- In some cases, you may find ways to streamline everyday business processes as a result of your BC/DR planning activities.
- Technology is implemented through people and processes. Therefore, an integrated approach to emergency planning for technology is needed that considers people, process, and technology.
- Understanding how technology is used in day-to-day operations is important for BC/DR planning.
- As an IT professional, you may understand how to implement technology, but you will need to collaborate with others in your organization to understand the broader business impact of technologies on operations so you can effectively plan for emergencies.

The cost of planning versus the cost of failure

- Fire is the most common emergency (disaster) companies face. 40-50% of companies that experience a major fire go out of business because most do not have BC/DR plans in place.
- Despite the high likelihood that a company will go out of business after a disaster, more than 90% of small businesses lack a disaster recovery plan.
- Even though many companies say they understand the need for a disaster recovery plan, very few actually make it a priority.
- There may be substantial financial and legal implications for failing to plan and for failing to take reasonable precautions. This can add to a company's burdens after a disaster strikes.

Types of disasters to consider

- Disasters fall into three general categories: natural hazards, human-caused hazards, and accidental/technical hazards.
- Natural hazards include weather problems in both hot and cold climates as well as geological hazards such as earthquakes, tsunamis, volcanic eruption, and land shifting.
- Human-caused hazards can be accidental or intentional. Some intentional human-caused hazards fall under the category of terrorism, and some are less severe and may be “simply” criminal or unethical.
- Human-caused hazards include cyber-attacks, rioting, protests, product tampering, bombs, explosions, and terrorism, to name a few.
- Accidents and technological hazards include such issues as transportation accidents and failures, infrastructure failures, and hazardous materials accidents, to name a few.

BC/DR planning basics

- Using standard PM methodologies will help you throughout your BC/DR plan development process. It will help reduce errors and avoid potential gaps in your planning activities.
- The basic steps of BC/DR planning are project initiation; risk assessment; business impact analysis; mitigation strategy development; plan development; testing, training and auditing; and plan maintenance. Each is discussed in subsequent chapters.

References

- Disaster Recovery Journal. Home. Retrieved May 25, 2013, from Disaster Recovery Journal, www.drj.com/; 2013.
- DRI International. Retrieved May 25, 2013, from Disaster Recovery Institute International, www.drii.org/; 2013.
- Global Continuity. Retrieved May 25, 2013, from Global Continuity Group, <http://www.globalcontinuity.com/home/>; 2011.
- Harris Interactive. Survey reveals lack of understanding by business executives of the value of business continuity and disaster recovery to organizational success. Wayne, PA: Harris Interactive. Retrieved May 24, 2013, from http://www.harrisinteractive.com/vault/Cient_News_SunGard_2009_06.pdf; 2009.
- Harris V, Hart D, Hibbard B, Jurgensen J, Wells J. Case study: The Johnson & Johnson Tylenol crisis. Retrieved May 25, 2013, from University of Oklahoma Department of Communications Crisis Communication Strategies, <http://www.ou.edu/deptcomm/dodcc/groups/02C2/Johnson%20&%20Johnson.htm>; n.d.
- The Business Continuity Institute. Retrieved May 25, 2013, from The Business Continuity Institute, www.thebci.org; 2013.

- U.S. Federal Emergency Management Agency. Ready. Prepare. Plan. Stay informed. Retrieved May 25, 2013, from FEMA Business Ready, www.ready.gov/business/index.html; 2013.
- U.S. Small Business Administration. Disaster planning. Retrieved May 25, 2013, from U.S. Small Business Administration, <http://www.sba.gov/content/disaster-planning>; 2013.
- U.S. Small Business Administration Advocacy. Frequently asked questions about small business. Retrieved May 25, 2013, from SBA.GOV, http://www.sba.gov/sites/default/files/FAQ_Sept_2012.pdf; 2012.
- Woodie A. Human error the number one cause of data loss, survey says. Retrieved May 25, 2013, from IT Jungle, <http://www.itjungle.com/tfh/tfh072610-story10.html>; 2010.

Legal and Regulatory Obligations Regarding Data and Information Security

2

IN THIS CHAPTER

- Impact of recent history
- Sources of legal obligations
- Scope of legal obligations
- Definitive legal standard
- Responsibility for compliance
- Required elements of a written information security plan

WARNING

The information presented in this chapter is intended to inform readers of potential issues, responsibilities, and requirements of the law with regard to data security. It is not legal advice and should not be construed in any manner as such. The publisher and the author make no legal warranties of any kind and nothing in this chapter should be taken as legal advice. For more information, contact your firm's legal counsel or an attorney who specializes in Internet, e-commerce, and electronic data security law.

INTRODUCTION

The privacy and security of personal information first became an area of concern in the 1960s and 1970s with military-based security data and the passage of the 1970 Fair Credit Reporting Act (FCRA). Since then, the emergence of the Internet and the proliferation of networked information systems, while providing businesses and governments with far-reaching economic benefits, has resulted in widespread abuse and theft of personal information as well as acts of cyber terrorism that have exposed grave risk to the nation's critical infrastructure and defense.

The reaction to these incidents has been a significant expansion of government oversight into the information technology (IT) systems and data maintained by both businesses and government. As of the writing of this book, no single federal law or regulation governed the security of all types of personal or other sensitive information. As a result, states have stepped in with their own laws resulting in a complex

patchwork of federal and state requirements that affect nearly all businesses. Until the 1990s, legislative regulation was largely limited to specific sectors of the economy (e.g., credit reporting, government, healthcare, education). However, with the significant rise in security breaches over the past 10 years, the United States has implemented many federally based security protection laws, with most state-mandated regulations proliferating since 2008.

From this complex patchwork of laws and regulations, a definitive legal standard is emerging which mandates nearly all businesses in the United States be subject to two key legal requirements:

1. The requirement to provide *reasonable security* for their corporate data and information systems;
2. The requirement to disclose security breaches to those who may be adversely affected by such breaches.

Within the first requirement, a legal definition of “reasonable security” has emerged from applicable law. All of the major security-related statutes, regulations, and government enforcement actions over the past few years show an amazing consistency in approach. When viewed as a whole, they establish a clearly defined standard for legal compliance—one that requires a process-oriented approach to the development and maintenance of a written information security program (WISP). In addition, the emerging legal standard has helped to clarify the scope and extent of a company’s obligation to implement an information security program. Under the standard, the obligation to provide reasonable security requires both (1) implementation of an ongoing process and (2) addressing certain categories of security measures. Moreover, evidence suggests that even in cases not subject to such laws, this process-oriented approach is the definitive standard against which legal compliance is measured.

The second requirement, which has also received extensive legislative support, is a legal corollary to the requirement to provide reasonable security. Born out of years of data breaches involving sensitive personal information and resulting cases of identity theft, this requirement primarily stipulates that security breaches be disclosed to individuals whose personal information has been compromised. In addition, the requirement also dictates that security breaches be disclosed to the government by certain entities, such as those involved in certain types of financial transactions or critical infrastructure. As of 2012, the requirement to disclose security breaches is the law in 46 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands, and is likely to become federal law in the near future, as well.

In addition to direct financial losses that stem from the data breach itself, noncompliance of either of these legal requirements has resulted in high costs in litigation, settlement fees, and fines imposed by government regulatory agencies. Lawsuits may be filed by customers, company shareholders, vendors, and other business partners. Even more costly (and more difficult to quantify) is the loss of public goodwill arising from a breach of data security.

The only thing that can make a major security breach even worse is a regulatory investigation or civil action alleging that you failed to meet your obligations under applicable law, and that such a failure resulted in the breach.

—Pros Auer Rose LLP ([Neuburger and Newman, 2010](#))

For both the requirement to provide “reasonable security” and the requirement to disclose breaches, this chapter will examine (1) recent history which has resulted in broad regulatory change, (2) the current regulatory environment, including the nature and scope of requirements, and (3) what companies should do to manage their information security in order to address their compliance obligations.

In terms of BC/DR planning efforts, it is important to understand that security breaches, including theft of personal or other sensitive data, are a significant cause of disasters and this risk includes both direct financial losses as well as losses from a tarnished reputation and potential legal action. As you develop your BC/DR plan, you’ll need to pay special attention to the types of data your company deals with and how those types of data need to be managed, particularly in terms of mitigating (avoiding) the risk and recovering from an incident. More information on risk and impact assessment, including how to properly evaluate security threats and determine their potential impact, can be found in [Chapters 4 and 5](#). In addition, more information on recent legal developments surrounding data privacy and security can be found in the [Case Study from Deanna Conn](#) following this chapter.

IMPACT OF RECENT HISTORY

Several recent highly publicized data security breaches involving the loss or disclosure of sensitive personal information have put added pressure on federal and state lawmakers to continue to enhance federal and corporate legal obligations to implement security safeguards. It all began on February 15, 2005, when data broker Choice Point Inc. disclosed that sensitive personal information it had collected on 145,000 individuals had been compromised. In the 5 months that followed, over 60 additional companies, educational institutions, and federal and state government agencies, almost all household names, also disclosed breaches of the security of sensitive personal information in their possession, affecting a cumulative 50 million records. Among the records compromised, perhaps the most significant were the chairman of the Federal Trade Commission (FTC) and as many as 60 U.S. Senators ([Federal Trade Commission, 2006](#)).

More recently, it appeared as if things went from bad to worse. In 2007, TJX, which owns and operates over 2500 retail outlets including Maxx, Marshalls, and Bob’s Stores, disclosed that in 2005, an unknown intruder illegally accessed one of the company’s payment systems and stole the credit and debit card information of 94 million customers across the United States, Canada, Puerto Rico, as well as the United Kingdom and Ireland over an 18-month period ([Federal Trade Commission, 2008](#)). This made the TJX breach the worst up until that time in terms

of compromising consumer personal information. In June of 2009, TJX announced that it agreed to pay \$9.75 million to settle investigations by 41 states attorneys general who were examining the company's data security policies and practices. Under the agreement, TIC will pay \$45.5 million in settlement fees, plus \$41.75 million to cover the fees associated with the investigations. Additionally, the company agreed to contribute \$2.5 million toward the creation of a data security fund that states will use to create a number of security-related initiatives such as developing best practice models, new legislations, and establishing consumer information and outreach programs. This does not include the cost of preventing this type of break in the future. ([U.S. Securities and Exchange Commission, 2007](#))

In March 2008, the Hannaford supermarket chain revealed that approximately 4 million debit and credit card numbers were compromised when Hannaford's computer systems were illegally accessed while the cards were being authorized for purchase. There were 1800 reported cases of fraud connected to the computer intrusion ([Privacy Rights Clearinghouse, 2009](#)).

In June 2010, the Connecticut Attorney General, the first by a State Attorney General under new Federal laws, launched an investigation when Health Net, an insurance provider, lost a computer drive that contained unencrypted health information, such as claim forms affecting nearly 1.5 million plan members (including patients in Arizona, New Jersey, and New York). The company reached a settlement agreement for violation of Health Insurance Portability and Accountability Act (HIPAA) regulations under the Health Information Technology for Economic and Clinical Health Act (HITECH Act). In the settlement, Health Net agreed to pay \$250,000 to the state, offer 2 years of credit monitoring to affected plan members, purchase \$1 million identity theft insurance, and reimburse plan members for security freezes. An additional \$500,000 will need to be paid in the event the information is used for fraudulent purposes. Health Net has not provided the costs of preventing this type of breach in the future, which could be substantial ([Connecticut Attorney General's Office, 2010](#)).

2011 turned out to be a banner year for security breaches as we witnessed some of the biggest data breaches in recorded history. On March 2011, Epsilon Interactive, a Texas-based database services company for such firms as Capital One, Citigroup, Chase, Marriott, Target, Best Buy, and Walgreen, announced customer information was retrieved by unauthorized access into the company's e-mail system, thereby exposing customers to spam and possible phishing attacks. Epsilon has claimed that the information stolen was limited to e-mail address and customer names only. A rigorous review determined that no other customer data were exposed ([Mills, 2011](#)). How were affected customers notified of this breach? By e-mail, naturally.

Shortly after the Epsilon incident, around April 19, 2011, Sony discovered an external breach on its PlayStation Network (PAN) and Priority music service and subsequently shut down access to these services for 7 days. Sony reported the criminal hacker(s) obtained names, addresses, e-mail addresses, dates of birth, PSN/Qriocity password and login, and online IDs for multiple users. The attacker may have also stolen users' purchase history, billing address, and password security questions. Over the course of the next several months, Sony discovered that the hackers

gained access to 101.6 million records, including 12 million unencrypted credit card numbers ([Privacy Rights Clearinghouse, 2011](#)).

Data breaches involving sensitive personal information, such as the ones above, have resulted in identify theft and financial crimes including credit card fraud, phone or utilities fraud, bank fraud, mortgage fraud, employment-related fraud, government documents or benefit fraud, loan fraud, and healthcare fraud. Identity theft involves the misuse of any identifying information, which could include name, social security number (SSN), account number, password, or other information linked to an individual, to commit a violation of federal or state law. According to the FTC, identity theft is the most common complaint from consumers in all 50 states ([Stevens, 2012](#)).

Since 2005, the Privacy Rights Clearinghouse (PRC) chronicles and reports that nearly 3,750 data security breaches have occurred in the United States alone, resulting in more than 608 million leaked records containing sensitive personal information. The real number of exposed records is significantly higher since, in many cases, the number of exposed records is either not known or is not reported to the news media or state and federal reporting authorities. These data breaches have exposed more than 100 million Americans to identity theft within an 8-year time period ([Privacy Rights Clearinghouse, 2013](#)).

CURRENT REGULATORY ENVIRONMENT

The legal issues surrounding information security are rooted in the fact that, in today's business environment, virtually all of a company's daily transactions, and all of its key records, are created, used, communicated, and stored electronically using networked computer technology. Consequentially, most businesses are now fully dependent upon IT and the underlying IT infrastructure.

Source of legal obligations

Corporate legal obligations to provide information security come from an ever-increasing complex patchwork of federal and state laws, regulations, enforcement actions, as well as common law fiduciary duties and other implied obligations to provide "reasonable care." Legal obligations in the United States are typically industry specific (e.g., financial, healthcare, utility) or data specific (e.g., personal information, financial data, or information related to the operation of critical infrastructure). In all cases, they have been steadily expanding, in part, due to the number and severity of high-profile security breaches going back to 2005.

Key legal protections, which have been in place for some time, have led us to the current state of information security legislation. These legal protections include (but are not limited to):

- Corporate governance laws to protect companies, shareholders, investors, and business partners (e.g., Sarbanes-Oxley (SOX) requirements for corporate financial information, SEC regulations);

- Laws to protect personal interests of employees, customers, and prospects (e.g., FCRA, Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act);
- Laws to protect government regulatory interests or evidentiary requirements (e.g., federal and state electronic transaction statutes (E-SIGN and UETA), IRS regulations requiring companies to implement information security to protect electronic tax records, SEC regulations, and FDA regulations);
- Laws governing federal government agencies (e.g., Federal Information Security Management Act (FISMA)); and
- Common Law (tort resulting from failure to provide security).

Furthermore, expansion of legal coverage of corporate security obligations has continued with successful claims of unfair or deceptive trade practices brought by the FTC, which regulates all businesses involved in interstate commerce. Section 5 of the FTC Act (FTCA) prohibits “unfair or deceptive acts or practices in or affecting commerce.” Unfair practices are practices that cause or are likely to cause consumers substantial injury that is neither reasonably avoidable by consumers nor offset by any countervailing benefit to consumers or competition. A representation, omission, or practice is deceptive if (1) it is likely to mislead consumers acting reasonably under the circumstances and (2) it is material or likely to affect consumers’ conduct or decisions with respect to the product at issue. In deceptive practice cases, the FTC has used Section 5 to challenge deceptive claims companies have made about the privacy and security of their customers’ personal data. The FTC has alleged that the companies had made promises to take “reasonable steps” to protect sensitive information yet they did not implement “reasonable and appropriate measures” to protect the sensitive personal information obtained from customers against unauthorized access.

Although no single federal law exists (as of the writing of this book) which covers all U.S. corporations with respect to information security, recent developments suggest that the federal government has sufficient provisions in existing statutes and regulations to require all U.S. corporations to provide appropriate security for all data, at least where compromise of such data may damage the interests of corporate shareholders. In this chapter, our primary focus is on distilling the legal obligations written into the broad patchwork of laws into a succinct, understandable format. As such, we will not delve deeply into every security-related provision for every law which may apply to your organization. However, if you are interested in learning more about which laws may apply to your business, the *CSO Magazine* Web site has compiled a very handy and comprehensive reference of security and privacy laws, regulations, and guidelines, containing summaries plus links to the full text of each law, up at: <http://www.csoonline.com/article/632218/the-security-laws-regulations-and-guide-lines-directory>. Here, you can find information on broadly applicable U.S. laws and regulations, industry-specific guidelines and requirements, applicable state laws, and applicable international laws which have an impact on U.S.-based global companies (*CSO Magazine*, 2012).

TIP**The Security Laws, Regulations, and Guidelines Directory**

A handy guide detailing security and privacy laws, regulations, and guidelines can be found at: <http://www.csoonline.com/article/632218/the-security-laws-regulations-and-guidelines-directory>. The directory includes current information on broadly applicable U.S. laws and regulations, industry-specific guidelines and requirements, applicable state laws, and applicable international laws which impact U.S.-based global companies. Summaries along with links to the full text of each law are included.

Scope of legal obligations

As previously discussed, the scope of legal obligations for most U.S. companies is limited to two essential requirements; however, you should be aware that additional requirements may apply depending on the industry sector in which you operate or the type of data you manage. We will now explore the legally mandated elements of each of these two requirements.

Provide “reasonable security”

A single, definitive legal standard has recently emerged which requires all U.S. corporations to provide “reasonable security” for their corporate data and IT assets, regardless of industry sector. Even though laws or regulations rarely specify what specific security measures should be employed, it is critical to know the *desired security objectives* specified in applicable laws, regulations, and consent decrees or enforcement actions.

The set of legal requirements for any U.S. company pertaining to information security obligations are derived from both industry-based (e.g., healthcare companies, financial companies) and data-based (e.g., personal information, financial data) information security statutes and regulations. Regardless of how your company’s specific legal requirements are derived, it is important to note that nearly all applicable laws define an amazingly small, well-defined set of desired security objectives. Therefore, you are able to reasonably protect your company from legal action in the United States related to information security laws without necessarily knowing the minutia involved in every applicable law, regulation, or enforcement action.

The well-defined set of desired security objectives found in nearly all applicable U.S. laws and regulations governing information security include:

- Ensure reliability/availability of information systems and data
- Control access to systems and information
- Ensure confidentiality, integrity, and/or authenticity of information
- Prevent unauthorized access, use, disclosure or transfer, modification or alteration, processing, and accidental loss or destruction
- Security measures must include physical, technical, and organizational or administrative controls
- Cover data in any form (e.g., databases, e-mails, pictures, video, sound recordings, etc.)

The definitive legal standard fully recognizes what IT security professionals have known for some time: *Security is a process, not a product.* In law after law, regulation after regulation, enforcement action after enforcement action, the requirements repeatedly dictate a fact-specific process leading to development of a comprehensive WISP.

This “process-oriented” requirement was first established in financial industry regulations required by the GLBA, later incorporated into FISMA, HIPAA, and FERC regulations, and since adopted as “best practice” by the FTC, National Association of Insurance Commissioners, and several State Attorneys General.

The “process-oriented” WISP is very different than the traditional view of simply employing strong security measures. Merely employing strong security measures has largely been deemed insufficient to comply with applicable statutes. Security measures must be responsive to existing threats and must constantly evolve in light of changes to threats, technology, business, etc.

As part of your WISP, it is required that you implement measures that are reasonable and designed to achieve the *desired security objectives* as written in laws and regulations. It is also required that you employ an ongoing, repetitive process which identifies new developments and threats, assesses risk, identifies and implements appropriate security measures, and verifies implementation.

Provide security breach notification

The requirement to provide security breach notification is a distinctly different requirement, separate from providing reasonable security, which has been enacted by 46 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands as of 2012. Proposed federal legislation in Congress is likely soon to become federal law as well.

Although the requirements vary somewhat from state to state, the key legal requirements are as follows:

- Data type—requirement generally applies to unencrypted sensitive personally identifiable information (PII)—first name or initial, and last name, plus one or more of following: SSN, driver’s license or state ID number, financial account number, credit card number, or debit card number + PIN/access code;
- Breach definition (triggering event)—give notice following unauthorized access of data that compromise the security, confidentiality, or integrity of personal information (CA); not required unless there is reasonable likelihood of harm to individuals (e.g., Arkansas, CT, DE, LA); not required unless breach is material (MO, NV);
- Who to notify—any affected state resident; and
- When to notify—as soon as possible, without “unreasonable” delay (e.g., 60 days); extension provided for law enforcement criminal investigation and taking necessary measures to determine scope and restore integrity to the system.

It is important to note that a key prerequisite to properly preparing for disclosure is to identify any unencrypted sensitive PII held by your company or a third-party

service provider, and confirm that everywhere it is collected and stored, it is necessary. In addition, to the extent possible, you should encrypt all relevant PII at rest (i.e., disk-based encryption) and in transmission (e.g., using Secure Sockets Layer or Transport Layer Security).

The key deliverable for this requirement, as part of your overall WISP, is to implement an incident response plan which specifies the steps to contain the breach (e.g., immediately take system off network, notify law enforcement) as well as steps to notify potentially injured persons. In addition, it is wise to include key provisions of applicable law in the incident response plan, including definition of whether a triggering event has occurred and how and when notification is required. Moreover, it is critical that you include business partners or third-party service providers in the incident response plan as well as include adherence to the incident response plan in your contract language.

INFORMATION SECURITY MANAGEMENT

As stated earlier, the obligation to provide reasonable security requires both (1) implementation of an ongoing process and (2) addressing certain categories of security measures. We have covered the essential elements of the process based WISP. Now, we will tackle the development of the WISP document itself and its legally mandated requirements. But first, who's responsible, legally, for ensuring compliance?

Responsibility lies at the top

Based on an analysis of the most recent, more developed information security statutes, responsibility for compliance increasingly rests with the Board of Directors (BoD) or CEO. The following titles are called out specifically by statute, case law, or among private sector business groups as the responsible party for ensuring compliance:

- CEO/CFO (SOX)
- BoD (GLBA—required to approve WISP, oversee development, implementation, and maintenance of program, and requires annual BoD reports regarding status of program, compliance status, and material matters related to program)
- Security Official (identified HIPAA official required to develop and implement policies and procedures, FTC consent decrees involved in a variety of nonregulated industries)
- Head of Federal Agency (FISMA—required to ensure information security management processes are integrated with agency strategic and operational planning processes)
- BoD (case law involving fiduciary duty)

- Caremark International Inc. Derivative Litigation—Delaware court said, “it is important that the board exercise a good faith judgment that the corporation’s information and reporting system is in concept and design adequate to ensure the board that appropriate information will come to its attention in a timely manner as a matter of ordinary operations, so that it may satisfy its responsibility.” ([Wikipedia, 2013](#))
- CEO/BoD (private sector Business Roundtable—association of chief executive officers of leading U.S. corporations with a combined workforce of more than 10 million U.S. employees)

Although the nature of legal obligations is often poorly understood by the levels of management responsible for compliance, by technical experts who implement, and by lawyers who ensure compliance, it is important to note that the requirement for an ongoing process can and should involve all three in order to mitigate risk.

Written Information Security Program (WISP)

The development and maintenance of a process-oriented WISP is critical to the ability of a company to meet its legal obligations as it relates to the management of information security. There is no “one size fits all” approach. Negligence law and security regulations take similar approaches to relevant factors to take into consideration when performing risk assessment, including:

1. Probability and criticality of potential risks
2. Company’s size, complexity, and capabilities
3. Nature and scope of business activities
4. Nature and sensitivity of the information to be protected
5. Company’s technical infrastructure, hardware, and software security capabilities
6. State of the art, regarding technology and security
7. Costs of the security measures

It is interesting to note that cost is mentioned most often as a factor in risk assessments, which explains one reason it is impossible to provide perfect security. This is why the law allows for providing *reasonable* security instead. The goal is to reduce risks and vulnerabilities to a reasonable and appropriate level.

The following is a summary of major federal statutory language (e.g., GLBA, HIPAA, FTC consent decrees, etc.) which directly addresses WISP requirements for nearly all business sectors. This legally mandated seven-step process depicts the *minimum requirements* necessary to ensure compliance:

1. Asset assessment—identify and document the system and information that needs to be protected
2. Risk assessment—conduct periodic assessment of the risks faced by the company
3. Security measures—design and implement reasonable physical, technical, and administrative security measures to control identified risk
4. Address third parties—oversee third-party service provider arrangements

5. Education—implement security awareness training and education
6. Monitoring and testing—to ensure the program is properly implemented and effective
7. Reviewing and adjusting—to revise the program in light of ongoing change

Security measures must be designed to protect against any anticipated threats or hazards to the security or integrity of the information and systems to be protected. For example, technical security measures such as firewalls or intrusion detection software don't protect against careless or malicious employees who inadvertently (or intentionally) disclose passwords or protected information. However, administrative security measures, such as separation of duties, do mitigate this risk.

Categories that must be addressed

In order to ensure you are providing reasonable security, the legal standard requires you to address all of the following in your design of security measures:

- Physical facility and device security controls
- Physical access controls
- Technical access controls
- Intrusion detection procedures
- Employee procedures
- System modification procedures
- Data integrity, confidentiality, and storage
- Data destruction and hardware and media disposal
- Audit controls
- Contingency plan (data backup, disaster recovery, emergency mode operation)
- Incident response plan (to specifically address security breach requirements)

Third-party service provider arrangements

Proper oversight of third-party service provider arrangements requires you to do all three of the following things:

- Exercise due diligence in selection
- Contractually require providers to implement appropriate security measures
- Monitor performance

Education

Proper education of the WISP should include the following four things:

- Development of a security awareness program
- Periodic security reminders
- Development of relevant employee training material
- Appropriate sanctions if failure to comply

DID YOU KNOW?

- The odds of a firm being sued in federal court are 3.5 times greater when individuals suffer financial harm, but over six times lower when the firm provides free credit monitoring following the breach ([Romanosky et al., 2012](#)).
- Being a slow adopter means that you defer the initial costs to increase security; but, if a particular risk triggers, it's likely to be more expensive for slow adopters. If the worst happens, it could shut your business down due to expense or reputation damage if your competitors chose to be early adopters.
- Research sponsored by technology giant HP found that the average cost of resolving a cyber-attack was \$416,000 in 2011, up from \$250,000 in 2010 ([Knowledge@Wharton, 2012](#)).
- Under most state data breach laws, encryption at rest provides businesses with safe harbor from notification in the event of a data breach.
- Some breach notification laws provide a safe harbor for companies that maintain data security policies which include breach notification provisions consistent with state and federal law.
- Bring-your-own-device (BYOD) legal issues have recently surfaced in case law. It is imperative that BYOD be treated like any other hardware asset and be included as part of the WISP asset and risk assessment processes, in order to ensure compliance with the legal standard for information security laws and regulations.
- The FTC regulates all individuals and businesses involved in interstate commerce, regardless of size. Therefore, it is imperative that businesses of any size which participate in interstate commerce follow a process-oriented WISP approach to ensure compliance with legal information security requirements. See www.sba.gov/community/blogs/community-blogs/business-law-advisor/how-small-businesses-can-protect-and-secure-cus for more information on how small businesses can best protect and secure customer information ([U.S. Small Business Administration, 2011](#)).

SUMMARY

In this chapter, we examined the sources of the definitive legal requirement of most U.S. companies, regardless of size or industry sector, to (1) provide “reasonable security” and (2) provide security breach notification. We also examined that responsibility lies with top management of a company to develop a process-oriented WISP in order to sufficiently mitigate risk and meet current federal and state legal obligations. We also discussed the specifics of the legally mandated, seven-step process necessary for any WISP to ensure compliance.

KEY CONCEPTS

Impact of recent history

- Since 2005, the PRC chronicles and reports that nearly 3,750 data security breaches have occurred in the United States alone, resulting in more than 608 million leaked records containing sensitive personal information.

Current regulatory environment

- The source of legal obligations for protecting sensitive data stems from a patchwork of federal and state data security and privacy laws.
- Legal obligations in the United States are typically industry specific (e.g., financial, healthcare, utility) or data specific (e.g., personal information, financial data, or information related to the operation of critical infrastructure).
- Key legal protections in place today include (1) corporate governance laws to protect companies, shareholders, investors, and business partners, (2) laws to protect personal interests of employees, customers, and prospects, (3) laws to protect government regulatory interests or evidentiary requirements, (4) laws governing federal government agencies, and (5) tort law.
- The FTC has used Section 5 of the FTCA to challenge deceptive claims companies have made about the privacy and security of their customers' personal data.
- The scope of legal obligations for most U.S. companies is limited to two essential requirements (a.k.a. the "legal standard"): (1) provide "reasonable security" and (2) provide security breach notification.

Information security management

- Based on an analysis of the most recent, more developed information security statutes, responsibility for compliance increasingly rests with the BoD or CEO.
- The development and maintenance of a process-oriented written information security program (WISP) is critical to the ability of a company to meet its legal obligations as it relates to the management of information security.
- The legal standard dictates minimum requirements your WISP must address, limited to: (1) specific security measures—including a contingency plan (data backup, disaster recovery, emergency mode operation) and an incident response plan (to specifically address security breach notification), (2) specific requirements for third-party service provider arrangements, and (3) specific requirements regarding the education of the WISP.

References

- Connecticut Attorney General's Office. Attorney general sues health net for massive security breach involving private medical records and financial information on 446,000 enrollees; 2010. Retrieved May 25, 2013, from George Jepson: Office of the Attorney General: <http://www.ct.gov/ag/cwp/view.asp?A=2341&Q=453918>.
- CSO Magazine. In: Slater D, editor. The security laws, regulations and guidelines directory; 2012. Retrieved May 26, 2013, from CSO Magazine: <http://www.csomagazine.com/article/632218/the-security-laws-regulations-and-guidelines-directory>.
- Federal Trade Commission. ChoicePoint settles data security breach charges; to pay \$10 million in civil penalties, \$5 million for consumer redress; 2006. Retrieved May 25, 2013, from Federal Trade Commission: <http://www.ftc.gov/opa/2006/01/choicepoint.shtm>.
- Federal Trade Commission. Agency announces settlement of separate actions against retailer TJX, and data brokers reed Elsevier and Seisint for failing to provide adequate security for consumers' data; 2008. Retrieved May 25, 2013, from Federal Trade Commission: <http://www.ftc.gov/opa/2008/03/datasec.shtm>.
- Knowledge@Wharton. Protecting your data from a new generation of hackers; 2012. Retrieved May 26, 2013, from Wharton School of the University of Pennsylvania: <http://knowledge.wharton.upenn.edu/article.cfm?articleid=3049>.
- Mills E. Who is Epsilon and why does it have my data?; 2011. Retrieved May 25, 2013, from CNET: http://news.cnet.com/8301-27080_3-20051038-245.html.
- Neuburger JD, Newman N. The bay state raises the bar on personal data security: are you in compliance? (66). Washington legal foundation; 2010. Retrieved May 25, 2013, from <http://www.wlf.org/Upload/legalstudies/contemporarylegalnote/NeuburgerFinal.pdf>.
- Privacy Rights Clearinghouse. Hannaford Bros. Supermarket chain, Portland, Maine; 2009. Retrieved May 25, 2013, from Privacy Rights Clearinghouse: <http://www.privacyrights.org/data-breach-asc?title=hannaford>.
- Privacy Rights Clearinghouse. The top half dozen most significant data breaches in 2011; 2011. Retrieved May 26, 2013, from Privacy Rights Clearinghouse: <https://www.privacyrights.org/data-breach-year-review-2011>.
- Privacy Rights Clearinghouse. Chronology of data breaches: security breaches 2005-present; 2013. Retrieved May 25, 2013, from Privacy Rights Clearinghouse: <http://www.privacyrights.org/data-breach>.
- Romanosky S, Hoffman DA, Acquisti A. Empirical analysis of data breach litigation; 2012. Retrieved from Social Science Research Network: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1986461.
- Stevens G. Data security breach notification laws; 2012. Retrieved May 25, 2013, from Federation of American Scientists: <http://www.fas.org/sgp/crs/misc/R42475.pdf>.
- U.S. Securities and Exchange Commission. Form 10-K annual report: the TJX Cos., Inc.; 2007. Retrieved from U.S. Securities and Exchange Commission: <http://www.sec.gov/Archives/edgar/data/109198/000095013507001906/b64407tje10vk.htm>.
- U.S. Small Business Administration. How small businesses can protect and secure customer information; 2011. Retrieved May 26, 2013, from U.S. Small Business Administration: <http://www.sba.gov/community/blogs/community-blogs/business-law-advisor/how-small-businesses-can-protect-and-secure-cus>.
- Wikipedia. In re Caremark International Inc. Derivative Litigation; 2013. Retrieved May 26, 2013, from Wikipedia: http://en.wikipedia.org/wiki/In_re_Caremark_International_Inc._Derivative_Litigation.

Case Study: Legal Obligations Regarding Data Security

IN THIS CHAPTER

- Background
- The Sony PlayStation incident
- State laws regarding data security
- Federal laws regarding data security
- Conclusion

CONTRIBUTOR PROFILE

Deanna Conn, Partner, Quarles & Brady, LLP

Deanna Conn is a partner at the law firm of Quarles & Brady, LLP. The firm provides broad-based, national-level legal services through a strong network of regional practices and local offices with over 400 attorneys nationwide. She practices in the areas of commercial and intellectual property litigation, intellectual property transactions, internet law, e-commerce, licensing and technology transactions, copyright, trademark, and trade secrets. She also specializes in advising direct selling companies on online distribution policies and regulatory compliance issues. She was a senior editor at the Columbia Law Review where she earned her law degree.

Ms. Conn practices law in the Tucson, Arizona office of Quarles & Brady, LLP and has worked closely with numerous clients on the issues surrounding electronic data security.

WARNING

The information provided in this chapter is intended to inform readers of potential issues, responsibilities, and requirements of the law with regard to data security. It is *not* legal advice and should not be construed in any manner as legal advice. The publisher, author, and contributor make no legal warranties of any kind, and nothing in this Case Study should be taken as legal advice. For more information, contact your firm's legal counsel or an attorney who specializes in internet, e-commerce, and electronic data security law.

BACKGROUND

Since 2005, there have been more than 3600 public data security breaches affecting more than half a billion records.¹ According to some reports, hacking accounted for approximately 81% of these incidents and 10% has been attributed to stolen or lost devices (Feffer, 2012). One of the largest data security breaches to date occurred in connection with Sony PlayStation Network in April 2011, when hackers stole more than 77 million records, including unencrypted credit card data (Privacy Rights Clearinghouse, 2013). Incidents involving Sony, described below, as well as many others, have confirmed concerns among federal and state legislators that something needs to be done to address the problems of data security. In fact, security breaches have been occurring for years; however, publicity regarding these breaches was more limited. In 2003, California was one of the first states to pass a law requiring companies to notify affected consumers regarding security breaches. Since then, many other states have passed similar notice laws. These public notice requirements have heightened consumer and public awareness regarding data security breaches.

THE SONY PLAYSTATION INCIDENT

Sony PlayStation Network had approximately 90 million users as of 2012. Users can purchase and download games and movies using Netflix and other accounts (D'Angelo, 2012). Users may pay for content by submitting credit card data online via the Play Station Network. In April 2011, Sony discovered an intrusion on its network. In response, Sony blocked users from playing online games or accessing services for 7 days. Later, Sony again took down the system in an attempt to block any further hacking attacks. Sony's investigation revealed that hackers obtained names, addresses, email addresses, dates of birth, PlayStation password and login information, password security questions and online ID, as well as unencrypted credit card information. In response to this security breach, Sony expects to spend more than \$170 million on its personal information theft protection program, customer support, and legal costs associated with the breach. A total of 55 class action complaints have been filed against Sony, including a complaint by Sony's insurer seeking to deny any insurance coverage for the event. On October 19, 2012, however, a federal judge dismissed most claims relating to one class action lawsuit based on Sony's privacy policy, which expressly disclosed that Sony could not guarantee system security (Privacy Rights Clearinghouse, 2013).

¹See data collected by Privacy Rights Clearinghouse regarding the number of data security breaches at <http://www.privacyrights.org>.

STATE LAWS REGARDING DATA SECURITY

As a result of these many data breach incidents, state legislators concluded that the federal government was not acting swiftly enough to combat data security problems. A patchwork of state laws has now been passed attempting to address the problems of data security. Whether these laws are successful, even if they simply shift the burden of security to companies, and ultimately, to consumers, remains unclear. Because each state's law is different, companies doing business with consumers throughout the United States must navigate many different laws. Most of the new state laws are vague, however, offering no clear guidelines on security requirements.

There are two new types of data security laws: (1) laws that require companies to notify customers regarding personal data security breaches and (2) laws that require safeguarding of personal information.

Notice of security breach laws

As of late 2012, at least 46 states and the District of Columbia have enacted laws requiring companies to notify consumers if they suffer a data security breach. These laws require companies and, in some cases, state government agencies, to disclose security breaches involving personal information.

Definition of personal information

There is no established definition regarding what constitutes personal information. At a minimum, however, any individual's name in combination with another element of identifiable data, including social security number, driver's license information, account number or credit card number, constitutes personal information. A number of states make the further distinction of only requiring notice if there is a breach involving *unencrypted* data.²

To the extent that companies have not already taken the step of encrypting sensitive personal data, state laws such as California's, which only impose notification requirements when there is a breach of unencrypted data, should encourage companies to encrypt data. Presumably, however, a breach involving encrypted data will also trigger notification requirements when the breach is linked to the encryption itself, such as when the encryption key is compromised.

Some states only trigger notice obligations if there is a "reasonable likelihood of harm." No guidance is offered regarding how to assess this issue. Companies may be likely to err on the side of avoiding disclosure. If, however, the failure to provide notice is later deemed unreasonable, the company will be subject to penalties for failing to comply with notice requirements.

²See Cal. Civ. Code §1798.82(a) ("Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose *unencrypted* personal information was, or is reasonably believed to have been, acquired by an unauthorized person.") (Italics added).

Notification procedure

Although the procedures vary by state, most laws require that companies provide consumers whose data may be affected with written notice, electronic notice, or “substitute” notice. Written notice is the standard method; however this can be costly if the breach involves thousands of consumers. Electronic notice is inexpensive, presuming the company has information regarding the consumer’s email address. The company must also comply with federal law regarding electronic contracts, which imposes certain additional disclosure requirements pursuant to the federal E-SIGN law (the Electronic Signatures in Global and National Commerce Act), 15 U.S.C. section 7001. Substitute notice may be used if the cost of providing written notice exceeds certain thresholds.

In California, substitute notice may be used if the cost of notice exceeds \$250,000, or if more than 500,000 people are involved. In that case, substitute notice requires the company to conspicuously post notice on the company Web site. In addition, notice is required to “major statewide media.” This requirement can cause a public relations firestorm, however. In the past, when California was one of the few states that required notification, some companies chose to only notify California consumers. When media outlets found out that notice was only being provided to California consumers, there was a public outcry.

The timeline for providing notice is typically not specified. Most states, such as California, require companies to notify consumers in “the most expedient time possible and without unreasonable delay.”³ Some states, however, such as Vermont, have specific time periods for providing notification. Vermont provides that notification “shall be made in the most expedient time possible and without unreasonable delay, but not later than 45 days after the discovery or notification.” However, the company must also “notify the attorney general of the date of the security breach and the date of discovery of the breach and shall provide a preliminary description of the breach within 14 business days...”⁴

Penalties

Most states do not impose statutory penalties for breach of timely notification. In contrast, some states impose administrative fines for failing to meet the timelines for notification provided by law. Florida law allows fines of up to \$1,000 per day for the first 30 days after the 45-day deadline. Thereafter, the fine can reach up to \$50,000 per day that the breach goes undisclosed for up to 180 days. If the breach is not disclosed within 180 days after the 45-day deadline, any person required to make the notification under Florida law can be fined up to \$500,000.⁵

³See Cal. Civ. Code §1798.82(a).

⁴See Vt. Stat. tit. 9 § 2435(b)(1) and (b)(3)(A)(i).

⁵See Fla. Stat. § 817.5681(b)(1)-(2).

Safeguarding personal data state laws

At least 29 states have enacted laws that require safeguarding of personal data, including laws that require companies to destroy, dispose, or otherwise make personal information unreadable or undecipherable. Most of these laws provide no guidance on the steps that should be taken to protect personal information, instead simply providing that “reasonable measures” should be taken. As an example, California law provides that:

A business that owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification or disclosure.⁶

On the other hand, as a practical matter, what qualifies as “reasonable measures” will necessarily depend on the particular circumstances, including the sensitivity of the data, how they are stored, and changing technology standards. At a minimum, however, companies need to develop and implement data security and destruction policies, audit those policies for compliance, review third-party contracts, request audits of third-party security policies, and conduct independent audits of the company’s own security policies and systems.

One guide that may be helpful in achieving these goals is the best practices standard set forth by ISO 17799:2005, accessible at www.iso.org. This standard has been promulgated by the International Standards Organization as a code of practice for information security management.

In addition, companies should keep track of what records they keep, where those records are stored, as well as contact information for their customers in the event the company has to provide notice of a security breach. Obtaining email address information would be particularly useful to reduce the cost of complying with these notice requirements. Information regarding the state of residency is also important to ensure that the notice complies with that customer’s state laws.

FEDERAL LAWS REGARDING DATA SECURITY

To date, there is still no comprehensive federal law governing data privacy or security. There is, however, a federal law governing data destruction policies. The Fair and Accurate Credit Transactions Act of 2003 (FACTA) is primarily directed to credit reporting agencies; however, provisions of the act relating to data destruction have broader application. Section 682.3(a) of FACTA provides that:

Any person who maintains or otherwise possesses consumer information for a business purpose must properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information with its disposal.

⁶See Cal. Civ. Code § 1798.81.1(b).

This law clearly has broader application and suggests that all companies must take care to develop data destruction policies and undertake routine audits to ensure compliance with those policies. The law recognizes that “reasonable measures” will vary depending on the sensitivity of the data, the costs and benefits of different disposal methods, and changes in technology. However, the FTC does provide some examples of “reasonable measures”:

1. Establishing and complying with policies to: burn, pulverize, or shred papers containing consumer report information so that the information cannot be read or reconstructed;
2. Destroying or erasing electronic files or media containing consumer report information so that the information cannot be read or reconstructed;
3. Conducting due diligence and hiring a document destruction contractor to dispose of material.

Due diligence steps could include (but are not mandated) reviewing an independent audit of a disposal company’s operations, obtaining and checking company references, or relying on certification by a recognized trade association ([Federal Trade Commission, 2005](#)).

Aside from FACTA, the U.S. House of Representatives and the U.S. Senate have proposed numerous bills regarding data privacy and security over the years. If passed, these bills could preempt state law, which would at least have the benefit of creating uniform requirements and protections. More recently, Congress has focused on data security needs, as opposed to privacy-related concerns. H.R. 624 is the latest of many proposed House bills that focus on data security.

U.S. House of representatives proposed bill

H.R. 624, the proposed Cyber Intelligence Sharing and Protection Act (CISPA), was passed by the U.S. House of Representatives on April 18, 2013. CISPA would extend immunity to companies for sharing information regarding cyber threats with the federal government. Critics, including the American Civil Liberties Union, have complained that this law does little to advance privacy and instead is simply yet another law designed to help law enforcement at the expense of civil liberty and privacy rights. In response to these complaints, several “privacy amendments” were added to the bill, including an amendment to ban the selling of personal information linked to cyber threat information sharing. Some exclusions were also added to the bill, exempting medical records and tax returns from the information that must be voluntarily shared with the government. On the other hand, the House voted down an amendment that would have required companies to take “reasonable” steps to remove irrelevant personally identifiable information when sending cyber threat data to the government ([Alexis, 2013](#)).

U.S. Senate response

While the House is focused on responding to cyber hacking threats, some legislators in the Senate have complained that there needs to be more comprehensive data security and privacy provisions, including creating standards for U.S. critical infrastructure operators, as well as a national data breach reporting requirement that would likely preempt state laws. In 2012, the Senate twice struggled unsuccessfully to pass such a comprehensive privacy bill. Against that backdrop, the Obama Administration recently issued an Executive Order regarding cyber security. Congress may end up waiting to gauge the impact of that Order on data security ([Martinez, 2013](#)).

Executive order-improving critical infrastructure cyber security

On February 12, 2013, the Obama Administration released an Executive Order addressing cyber security. Among other provisions, the Executive Order provides for information sharing by the U.S. government with the private sector to better protect against cyber threats. It also has called for development of a set of standards, methodologies, and protocols designed to reduce cyber risks to critical infrastructure which it has designated as the “Cybersecurity Framework.” The Order states that these initiatives must also ensure that privacy and civil liberties are protected by coordinating with the Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties of the Department of Homeland Security ([White House, 2013](#)).

Implementation of this Executive Order may have a significant impact on standards and rules that are put in place regarding data security and privacy.

CONCLUSION

To date, existing state laws regarding data privacy and security offer little practical guidance on what companies must do to comply with state laws. Proposed federal bills are similarly general in nature. More concrete standards regarding data security and privacy may result when the Obama Administration’s recent Executive Order is implemented. In the interim, companies must look primarily to standards and guidelines that are coming from within the data security industry.

At a minimum, companies should keep an inventory of the information they license or own, implement data security and data disposal policies, audit compliance with those policies, regularly update security systems, and finally, act quickly to notify customers in the event of a breach, recognizing that notification obligations vary based on the state of residency of the individual who is affected.

References

- Alexis A. Key Senate democrats not satisfied with house-passed cybersecurity bill. Bloomberg BNA, Electronic Commerce & Law Report. <http://news.bna.com>; 2013 [Retrieved 21.04.2013].
- D'Angelo V. How Many PS Vita, PS3 users are on the PlayStation Network. PSP World. <http://www.pspworld.com/sony-psp/news/how-many-ps-vita-ps3-users-are-on-the-playstation-network-014761.php>; 2012. [Retrieved 22.04.2012].
- Federal Trade Commission. FACTA Disposal Rule Goes into Effect June 1. <http://www.ftc.gov/opa/2005/06/disposal.shtm>; 2005 [Retrieved 22.04.2013].
- Feffer M. The 2012 Breakdown of Data Breaches. Ho ho ho. <http://news.dice.com/2012/12/18/the-2012-breakdown-of-corporate-data-breaches-ho-ho-ho/>; 2012 [Retrieved 22.04.2013].
- Martinez J. Cybersecurity debate moves to Senate. The Hill's Hillicon Valley. <http://thehill.com/blogs/hillicon-valley/technology/295113-cybersecurity-debate-now-centered-in%20the-senate.html>; 2013, [Retrieved 22.04.2013].
- Privacy Rights Clearinghouse. Chronology of Data Breaches. <http://www.privacyrights.org/data-breach/new>; 2013 [Retrieved 22.04.2013].
- White House. Executive order-improving critical infrastructure cybersecurity. <http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure.html>; 2013 [Retrieved 22.04.2013].

Project Initiation

3

IN THIS CHAPTER

- Elements of project success
- Project plan components
- Key contributors and responsibilities
- Project definition
- Business continuity and disaster recovery plan
- Summary
- Key concepts

INTRODUCTION

Business continuity and disaster recovery are two distinct activities related to ensuring critical data are available to the organization when needed. Each can be planned as a separate project using standard project management (PM) methodologies, or they can be planned as one larger, integrated plan. The steps needed to deal with the immediate aftermath of a disaster and the steps needed to ensure the business stays up and running may be one and the same for some companies. Only you and your project team will be able to make that distinction. However, regardless of the approach you take, you'll need to design your BC/DR projects as formal IT projects in order to avoid costly mistakes such as erroneous assumptions or gaping holes in your plan. If you're working in a medium- to large-sized business, the risk of using two separate plans (BC, DR) is that you're likely to have gaps where the transition points need to occur. In this case, it may be advisable to create one master project plan and then parse out tasks or sub-projects into manageable sets of deliverables. Whatever your approach, it needs to be clear, concise, and consistent.

A project is defined as a set of tasks having a defined start and end point and specific objectives, requirements, and goals. Clearly, both business continuity and disaster recovery planning qualify as projects under this definition. The BC/DR planning process can, and should, be constructed as a project plan, and each component (BC, DR) can then be implemented as a project. There is a good cause for mentioning this. One of the reasons many companies fail to develop effective plans is that they do not approach BC/DR planning as a *project*. They see it as an

all-encompassing, all-consuming, never-ending task; it becomes overwhelming or vaguely defined. No one can get in gear or stay motivated to complete a never-ending task. This also adds to the erroneous belief that BC/DR planning is just for large companies with deep pockets. That said, once the planning process is complete, BC/DR should become an ongoing process. Your efforts should result in procedures and processes that become part of your standard operating procedures so that the work of the project becomes ingrained into everything you do. If you're able to do this, you'll find that maintaining your BC/DR readiness improves dramatically.

In this chapter, we're going to look at the process of creating a project plan for your BC/DR activities. If you're already familiar with IT project management, these steps will be familiar and should serve as a good reminder. If you're not familiar with formal IT project management, this chapter will help you become better acquainted with IT PM best practices and guide you through the process. You won't find an overly technical or detailed plan here; what you will find is a framework you can customize to the unique needs of your organization. If you're a certified Project Manager, you will find that these steps follow general guidelines but may not adhere to the PM methodology of your choosing.

As with any IT project, there are numerous elements that tend to contribute to the likelihood of success. We'll begin by discussing these factors and how they relate, specifically, to your BC/DR planning efforts. We'll continue by looking at the elements you should include, how you might want to organize the project and your team(s), and how to develop success criteria so that you can mark your progress and recognize success.

Whatever you do, don't skip this chapter. It creates the framework for the rest of the book, and it will be relatively painless to get through this chapter without having nightmares or falling asleep. Throughout the remaining chapters, we'll refer to our progress diagram to help you keep a visual image of where we are in the overall process. **Figure 3.1** shows we're in the first step, project initiation.



FIGURE 3.1

Business continuity and disaster recovery project planning progress.

ELEMENTS OF PROJECT SUCCESS

Numerous studies through the years show there are a set of factors that, when present, tend to make projects more successful. The Standish Group International began researching project success and failure back in the 1990s. They've published a report

called the CHAOS Report every 2 years. The 2011 report indicates that only 37% of all projects succeed (Curtis, 2012). Success is defined as a project being delivered on time, in budget, and in scope. So, your odds are less than 50-50 that you'll deliver a successful BC/DR project. While that may sound depressing, the good news is that there are defined success factors—and the more success factors you can leverage, the higher your likelihood of success. Each time the Standish Group's CHAOS list is updated, the order of success factors changes slightly, but the same factors consistently show up in the top eight positions. These factors are:

- Executive support
- User involvement
- Experienced project manager
- Clearly defined project objectives
- Clearly defined project requirements
- Clearly defined scope
- Shorter schedule, multiple milestones
- Clearly defined project management process

In this section, we'll discuss each of these factors as it relates to your BC/DR project.

Executive support

Executive support for any IT project is always among the top success factors. It makes sense that support from the top of the organization for an IT project tips the odds of success in your favor since executives have the ability to provide funding, resources, staffing, and political clout. If they are convinced there is a clear business need, they will go to bat for you and help ensure you get what you need to succeed.

How does that translate to BC/DR planning? BC/DR planning has to be a comprehensive plan that covers *every* critical aspect of your business. In order for your plan to be successful, you *must* work with people from all key areas of your company. In order to do so, you clearly need the authority and reach that executive support can provide. You'll need to pull people away from other projects and tasks to participate on this project, and their managers are certainly going to be asking questions like—Who authorized this? How will this impact my other projects? Who is responsible for making this decision? If the senior managers or executives of your organization are behind you 100%, your authority to move forward on this project will be supported and others within the organization will typically fall in line. Granted, they may not be happy to shift their priorities to make room for this project, but they will if their boss and their boss's boss say so. Related to this, if you and your project run into resistance that you cannot overcome, you can escalate the issue through the proper channels and expect to find support as it reaches the executive ranks (assuming you're in the right).

CRITICAL CONCEPT**Gaining Executive Support**

Some people in IT find it difficult to garner executive support for projects, and there are three common reasons and some fairly straightforward solutions to these challenges.

1. In many cases, IT staff get too wrapped up in the technology and fail to acknowledge and highlight the business need for the solution. The further away from IT the executive is, the less he or she understands the details. They are focused on the organization and the big picture. They want to make sure the large investments they've authorized for all that IT gear in the data center and all the effort the organization put into generating data used to run the business is protected. It's about risk management for executives. You need to think like an executive instead of a technologist. The risk/reward ratio is critical to executive support. There's absolutely no point in spending \$100,000 to protect \$50,000 worth of data or equipment. It's very worth spending \$100,000 annually to protect \$10M worth of equipment and data assets. If you make the case around technology, you will likely run into problems. If you make the case around business, competitive capabilities, risk management, and risk/reward, you're speaking the language of business and are likely to be heard. Throughout this book, you'll read about cases and examples of the business case for BC/DR planning that you can use in your discussions with executives.
2. Another common reason for failing to get support for BC/DR planning is a simple failure to communicate clearly, concisely, and convincingly. You don't need a huge presentation with graphics and Flash animation to make your point. You need to figure out who your audience is, what you want them to understand when you're finished, and how you should present the information. Some audiences want a PowerPoint presentation with bullet points; some audiences want a one-page written summary; still other audiences want a 5-minute verbal presentation with a one-paragraph written summary. There is no one single correct way to present the information other than this: Determine the preferred format for your intended audience and create a short, concise presentation using nontechnical language. Most executives have heard of VoIP, NAS, SANs, and TCP/IP but don't really understand these terms. Therefore, keep it nontechnical and clear. Keep your objectives in mind and lay out your information in a logical progression. If you can't explain it to a complete stranger on the street, you haven't gotten it clear in your own mind. You should be able to explain it to anyone in plain language—if you start there, your executives will certainly understand. They're really smart folks whose area of expertise is business, not technology, *per se*.
3. Finally, a third common reason for failure to get executive support for IT projects is that IT projects sometimes appear (to executives) as bottomless pits into which time, money, and resources fall. You'll need to provide executives with a ballpark estimate for how long you believe the project will take and roughly how much it will cost (time and money) to complete. Here's the danger—until you've completed the initial project work, you probably won't know the answers to these questions. It becomes a circular problem because you can't give an estimate until you do some planning and you can't do the planning until you've provided executives with an estimate.

One way to short-circuit that problem is to tell executives you don't know how long it will take or what it will cost, but that it is critical that you be given the OK to find out. If you view your project as a two-part process where the first part is to create a rough estimate for time and cost so you can get approval for the larger planning project, you might gain support early. Alternately, you may be able to work with a few key people in the organization such as your financial person, one or more of your key Ops people, and your facilities person to come up with a ballpark estimate you're all comfortable with. Building this coalition early on may also help solidify your project team and could provide critical mass within the organization for the planning project.

Executives understand business and finance—they don't necessarily understand technology. Many are comfortable using technology, and a vast majority understands the need to utilize technology effectively within an organization; few understand the terminology and the underpinnings of technology. Therefore, the most successful approach with almost all executives is to use business terminology and be clear, concise, and correct. Rather than saying "we need to investigate availability solutions for WAN and LAN support," you need to break it down and say "we need to investigate our options for providing data access across the entire company, both here in the building, nationwide and across the globe." Both say roughly the same thing, but the second statement is business-centric, and the first statement is techno-speak. If writing (or nontechnical writing) is not your strong suit, write up what you want to say and ask someone in a nontechnical department to work on it with you. For example, go to your Human Resources or Marketing department and ask someone to assist you. It would be better to get feedback from someone outside the decision-making loop than to submit your technical document to a decision-maker who doesn't understand it and won't take the time to ask you to explain it. Executives are typically very busy and they like when things are boiled down to their essence in plain language. It helps them quickly understand the situation and make a rational, well-informed decision. You want to help them do just that.

REAL WORLD

When the Answer Is "No!"

The ideal scenario rarely matches reality. In today's IT world, budgets and capabilities are stretched to the breaking point and highly charged issues such as security and regulatory compliance garner the most visibility. You may very well find that your company is reluctant (at best) or unwilling (at worst) to devote time or money to developing a business continuity or disaster recovery planning project. Though BC/DR solutions are required in just about every industry these days, some companies are still trying to skirt this responsibility. If your firm is required by regulation to have a BC/DR plan, there's really no avoiding it. If your firm is not required by law to have a plan, it may be a bit harder to "sell" the concept and they may want to slap together a quick plan on paper to create the appearance of compliance. That's the equivalent to a "no" in your world. Even though this is a suboptimal long-term business decision, the demands on a company's resources can sometimes be such that BC/DR planning is just not valued or appreciated. If you're an IT professional pushing for BC/DR planning in your company and you find you're hitting a brick wall, there are a few things you can do to help facilitate this process. Although you may not be able to set aside time (or money) to create a fully separate project for BC/DR, you can incorporate BC/DR concepts in all your other IT project plans. For example, if you're evaluating the implementation of a new server, new application, or new technology, include an assessment of the BC/DR concepts and include elements that will help you mitigate risk and plan for outages as you would within the scope of a formal BC/DR plan. The most basic BC/DR plan is to have redundancy and backups, and most IT staff work to develop these attributes in the normal course of IT operations. There is a fair amount of coverage you can get if you begin adding BC/DR elements to your basic IT planning, projects, and operations. It won't ever substitute for a full BC/DR plan, but at least it will begin to move your IT operations in that direction without putting undue pressure on your time or your budget. So, if your company won't move beyond "no" when you discuss BC/DR plans, use the

Continued

REAL WORLD—cont'd

information throughout the remainder of this book to incorporate key elements into your IT operations. And remember, if BC/DR is required by governmental regulation, you should clearly articulate the requirement to your executives, so they can decide what steps they would like to take to become or maintain compliance.

User involvement

You've probably been involved with projects that were going to dramatically impact end users, and yet no one talked with end users for months, if ever. These projects are almost always doomed to fail. User involvement consistently shows up in one of the top three spots on the list of success factors for IT projects. Many technology projects have failed because users were not involved and key decisions were made that were directly counter to user needs and wishes. Clearly, you can create any solution you want, but you can't force users to use it. You can't force users to understand and accept convoluted processes for doing their once-simple tasks, to flex *around* awkward requirements of the technology. Although there can be compelling business drivers that force users to change their processes and methods, these should be created with user input and collaboration, not in the dark recesses of the IT department.

So, who are the users in a BC/DR planning project? There are essentially two sets of users. The first set includes those who will be involved in planning the BC/DR project itself. These folks may or may not be the same ones who will implement these plans should disaster strike. Therefore, you would do well to have both sets of users involved in this project. For example, you might want to have one team that focuses on defining the critical business processes that need to be addressed in the plan. A second (or subsequent) phase of the project plan could include a second project team that includes those people from around the company that would be responsible for implementing a BC/DR plan and would therefore define the implementation phase. If you work in a small company, this might be the same group of people. In larger companies, it might be two overlapping or two separate teams.

Whatever your approach, be sure to include the key people in the project from start to finish. Later in this chapter, we'll discuss who should be involved. For now, keep in mind that if you and your team create a great plan without input from those who will be the "boots on the ground" in an emergency, your plan is highly likely to fail under the stress of a disaster.

Experienced project manager

In the most recent Standish Group CHAOS report, an *experienced project manager* was the number one factor for project success ([Curtis, 2012](#)). That has shifted in position, up slightly from a few years ago. Experienced project managers bring a wealth of knowledge and skill to the table. They often have had some formal project management training or education, and they may have achieved a standardized

certification in one or more methodologies. Most importantly, though, they have been in the trenches managing projects and have realistic understanding of what it takes to get the job done.

When we're looking at BC/DR specifically, an experienced project manager is likely to be more effective at working across organizational boundaries and in bringing together a diverse group of people and interests. Working effectively with people at all levels of the organization and in all areas of the company is critical to the success of a BC/DR plan. An experienced project manager is more likely to understand how to navigate the political waters as well as the organizational red tape that inevitably crops up during the development and implementation of cross-departmental projects. One very key trait of experienced (and successful) project managers is the ability to speak up, hold people accountable, be assertive when things are drifting or heading south, and know how and when to escalate for key issues. These traits are learned on the job and over time, thus an experienced project manager can make a project successful even when other factors are pointing toward a failed project.

In addition, an experienced project manager will utilize a defined set of steps, a methodology, to deliver consistent results. Most experienced project managers have developed a system of defining and managing projects that delivers positive results. Many have spent years honing their methods to generate an optimal outcome. Most adhere, in general terms, to standardized methodologies but each experienced and successful project manager undoubtedly will have customized those methodologies to suit their specific needs. This is key to delivering a successful BC/DR project plan. With the actual survival of your company at risk, it's imperative to have the most successful outcome possible. An experienced PM will increase your odds of such an outcome, though no single (or multiple) success factor guarantees success.

Clearly defined project objectives

Clearly defined project objectives might sound incredibly obvious, but you might be surprised at how often projects are launched without clearly defined objectives. Or maybe you're not surprised at all because it happens all the time in your company. Regardless, clearly defined objectives are quite important because your BC/DR plan must be scaled to your organization's unique needs. Without defining the objectives, you and your team might spend a disproportionate amount of time planning and implementing a part of the plan that is less important, or you might short-change a very important area.

The simplest project objective can be derived by simply asking "What problem are we trying to solve?" Get more specific than "protect critical information assets." At a high level, which critical information assets? Customer data, sales data, inventory, circuit locations, medical records, software code—all are critical information assets, but which are specific to your business? Starting with defining the problem to be solved can focus you in on your project objectives.

One way the task of defining objectives can contribute to BC/DR success is to develop a high-level list of functional areas of your company and invite key people

from those areas to help define the objectives. This accomplishes two critical project outcomes: it ensures that key functional areas are included in the planning process and it brings together the people most able to develop appropriate objectives. As an IT professional, you are not in a position to develop objectives for BC/DR planning for, say, the Human Resources or Marketing department. You understand the technology but not the business or operational objectives, in most cases. In addition, you need to get these stakeholders together to agree on objectives because you will have to prioritize. During an emergency or disaster, many business operations, tasks, and objectives become secondary to the survival of people and the survival of the company. Determining these needs helps determine the project's objectives, and this will help focus you and your team on the critical aspects of the business.

TIP**Something Is Better Than Nothing**

Don't start with a "blank sheet of paper." You'll find if you start from scratch, your constituents will flounder. They have neither the time nor expertise to sit down and hash through the elements you need from them. So, come prepared. Start with something. Look at your organization's high-level functional areas and key information assets. Start with a grid that lists out your assumptions of operational owners and key information assets. Let your constituents (stakeholders, end users, whatever phrase you use) tell you how wrong you were—at least you started with something they can edit.

Clearly defined project requirements

Related to objectives are project requirements. Developing clear and complete requirements can also make the difference between success and failure, especially for an IT-related project. The requirements are those capabilities, attributes, and qualities that must be part of the final project deliverable. Defining these early in the project development cycle is important because going back to add them in later (called *rework*) is inefficient, costly, and fraught with both errors and additional project risk.

Requirements are not the same as project objectives. The objectives should drive the requirements. Objectives are what you want to accomplish, requirements are how you will accomplish those objectives. For example, if an *objective* for your BC/DR plan is continuous availability of three key business applications and related data, your *requirements* would have to delineate this objective. Requirements may have to be refined or developed later in the project definition process as details about the project become clear. However, clear requirements before project work begins are absolutely critical to project success. Unclear requirements cause confusion, duplication of effort, rework, and wasted work. If your objective is continuous availability but you never specify which applications, which data, which users, which business functions, which locations, which customers, etc., fall under that objective, you will undoubtedly find your project wandering off on its own.

Requirements typically fall into three categories: business, functional, and technical requirements. *Business requirements* help you determine what the business needs to survive a disruption. This helps you understand the major building blocks of your company, how they work together, and what key areas should be prioritized. Business requirements might also include things like response time, availability of data, and tolerance for downtime. While this might be drilling too far down into the details at this juncture, these elements are sometimes known. For example, a healthcare organization can state that availability of key medical data for patients is required 100% of the time. An e-commerce site can say that site uptime must be 99%. A manufacturing plant may say that key control systems must be up to 100% of the time. These are details that you'll address later, but often these key business applications are well known, well-defined and their criticality has been well articulated. *Functional requirements* detail things such as which processes, methods, and resources need to be available during and after a business disruption. *Technical requirements* delineate things such as servers, network infrastructure, and business application requirements. The more specific your requirements, the more likely you are to have a successful outcome—a BC/DR plan that works when implemented. You can think of it this way. If you get in your car with a destination in mind but no particular route, you are more likely to take longer to get there than if you mapped out your route before you left the house. For those of you who immediately think “Yes, but I’d use my GPS navigation system,” remember, defining requirements is the project equivalent to GPS though you may need to make several passes through your requirements definition phase to add detail and clarity as you *define* and *organize* your project, you should not begin the actual work deliverables (*work breakdown structure* (WBS) tasks) until you have clearly defined requirements. Lack of clear requirements will absolutely tank your project. Don’t leave home without them.

Clearly defined scope

Related to clearly defined project objectives is a clearly defined project scope. Some of you may laugh out loud when reading about a clearly defined project scope. How many times have you started a project and had your scope yanked out from under you? It’s more likely to occur than not. Still, agreeing on scope and documenting that agreed upon scope can mean the difference between success and failure. If you document agreed upon scope and it then changes, you can use your documentation as a negotiating tool to determine whether you’ll need to be given more time, more money, or less depth in any particular deliverable (aka “quality” in project management terminology). *Scope* is defined as the total amount of work to be accomplished. Technically speaking, scope is the description of the total amount of work to be accomplished and constrained, or defined, by the budget, the timeline, and the quality required. Scope typically is defined through the project’s objectives. Making sure payroll can be run during a disaster may be one objective; making sure your company can still take, fulfill, and invoice customer orders is another objective.

If these are the only two objectives for your BC/DR plan, you can fairly easily determine the project's scope. Therefore, clearly defined objectives lead to a clearly defined project scope.

Scope creep happens to many projects, and BC/DR is a project type that is perhaps more susceptible to scope creep than many other types of IT projects due to the cross-functional nature of BC/DR planning. For example, it's not hard to imagine that you decide that being able to process payroll during a crisis will be critical to the well-being of your firm's employees, so you include a high-level objective to that effect. However, as the project planning stages progress, someone mentions that the Human Resources director also wants the ability to easily set up direct deposit for people during a crisis in the event they cannot come to their work location to pick up a check. Your scope has just experienced creep—as you may know or suspect, it's one thing to ensure that payroll can be processed per usual, but another thing entirely to suddenly add the ability to go to direct deposit in an emergency. Clearly, additional steps must be included in the project plan to enable this capability, especially if it does not currently exist or if it will need to exist in a different way. For example, it is likely that people who want to use direct deposit currently have to submit a form with a voided check from their bank account and it must go through one or two payroll cycles before it is effective. During a disaster, employees will not have access to the form, they may not have access to their checkbooks, and they won't know how to accomplish that without talking with someone from HR. Additionally, it might be unacceptable for it to take two payroll cycles for this to occur during an emergency. Therefore, your team will need to develop possible solutions or alternatives for this new requirement and address it in your plan. So, although the HR director may have wanted this to be accomplished, he or she may not realize what it will take to accomplish this. Be sure to have clearly defined objectives, make sure that each objective is necessary during an emergency, and have the people (in this case, HR) responsible for that business function develop the potential solutions to the objective. This helps reduce scope creep and helps manage clearly defined objectives and clearly defined scope.

TIP

Though this book is not about process improvement, it's worth noting that there's ample opportunity during your planning phases to review current process and improve upon it. At minimum, think through your BC/DR planning processes. Keeping plans simple during a disaster or other "event" can make that plan successful. Using the example above, if people need access to funds during an emergency and payroll can be processed but direct deposit cannot, what other methods can be used by your company to ensure staff have timely access to their wages? It might be an incredibly manual process—maybe you do print checks, maybe you set something up with a local bank, maybe you encourage staff to use direct deposit before a disaster event—selling them on the convenience, the savings on banking fees (typically), the security, etc. There are numerous steps that can be taken to address staff needing to be paid during a disaster, look for the simplest plan to ensure it has a chance for success.

Shorter schedule, multiple milestones

Studies have repeatedly shown that shorter schedules with more milestones generate more successful results. How does this apply to BC/DR planning? In most cases, BC/DR planning is a comprehensive look at the business and its processes to determine critical functions and emergency procedures for those critical functions. You may choose to break your BC/DR planning project down into smaller projects—for example, one project plan for each functional area and one master plan that ties these all together. You may choose to perform your planning in an iterative mode so that during the first pass, you develop just the most basic, mission-critical solutions, and each iteration builds on the one prior. Only you and your project planning team can determine the best approach to this, but keep in mind that long schedules typically just get longer. People lose focus, enthusiasm, and interest. Resources start being pulled away from the project the further out in time you go.

Milestones are, by definition, project markers that help you gauge progress. Milestones are checkpoints that can help you stay on budget, on schedule, and on scope as your project progresses. The more milestones (within reason) your project has, the more likely it is to be successful because you are consistently comparing where you stated you wanted to be with where you actually are. This regular course correction can certainly keep your project on target far better than an occasional checkpoint that may leave you wondering how you got so far off course.

Your company may be reluctant to undertake a full BC/DR project because executives might fear that it will go on forever and never produce a result or might cost far more than the company can afford in terms of staff time and money. If you run into massive resistance, you might want to parse your plan out into well-defined stages and get executives to sign off on the phased approach. Then, when you can show success with the first phase, you may more easily gain support for subsequent phases.

TIP

Phased Planning

If you take a phased approach to your planning, be careful to clearly delineate what is and is not part of each phase. You want to avoid executives believing that Phase One will cover something in another phase. You also want to be sure that Phase One delivers a meaningful barebones BC/DR plan at the very least. The phased approach is most often useful when executives are uncertain about the potential costs and benefits, and success in the first phase can engender support for subsequent phases, but it can also lead to a false sense of security. You'll have to find the appropriate balance for your organization.

Clearly defined project management process

A clearly defined project management process typically goes hand in hand with an experienced project manager. As mentioned, an experienced PM is likely to have a set of methods, procedures, and associated documents that he or she has used successfully in the past. Most experienced PMs will hone those processes and

procedures over time so that they become almost second nature. If you're an inexperienced project manager, you can increase your odds of success by using a well-defined project management process. Throughout the remainder of this book, we'll use standard PM processes that will help you develop a more successful BC/DR project plan. If you have a methodology that you've used successfully in the past, feel free to utilize that in conjunction with the material presented in this book. You'll find that the presentation of PM processes in this book follows a fairly standard format and should be compatible with any standardized process you choose to use. The key is to select a process and use it from start to finish, so there are no gaps in the process, which inevitably lead to gaps in the plan.

TIP**Lean, Agile and BC/DR**

There has been a lot of interest in the past few years in methodologies like Lean and Agile. Evidence has been pointing toward the success of these frameworks when fully embraced by an organization. If you are just starting out on your project management process journey, or even if you've been at it a while, it's worth looking at Lean and Agile. A Lean IT framework can help you engineer your project plan and subsequent BC/DR processes in the most efficient manner possible (value stream mapping, reducing waste, etc.). Agile project management methodologies are often associated with software engineering (agile vs. traditional "waterfall" approach), but can be used successfully with any project. While discussion of these methodologies is outside the scope of this book, you may be interested in researching these for use in your BC/DR planning process.

As you can see from the success factors listed, achieving project success is not rocket science, but it does require a consistent approach and attention to detail. As business continuity and disaster recovery continue to show up in the news headlines, executives are certainly becoming more aware of the need to invest in BC/DR plans. Clearly, regulatory pressure, shareholder requirements, and vendor initiatives also have pushed this to the forefront of many executive's awareness. Some companies' executives, however, are still a bit behind the curve, usually because they do not have regulators or shareholders pounding on their door asking for their BC/DR plans. If you work in one of these companies, you may still face a bit of an uphill battle, but by reviewing the project success factors and developing a strategy for approaching this planning, you are likely to find a solution that fits your company's needs.

REAL WORLD**Even Small Companies Need a Plan**

If you're an IT service firm, you may be able to provide a great service to your customers by talking with them about their business continuity plans. There are millions of small companies out there, from sole proprietors to partnerships to small companies of 5 or 10 employees. At a very basic level, they should have a solid data backup plan. If an author is working on a manuscript while traveling, what happens if the laptop is lost, stolen, or broken? Though this

Continued

REAL WORLD—cont'd

may sound very basic to you, be assured that millions of people don't give this much thought until they have an unfortunate incident that costs them thousands of hours, dollars, or headaches. Whether you work in a small company or in a service firm for small companies, you should keep BC/DR plans in mind when looking at how they work and how they should be protected. Most companies (including individuals) are thankful when you bring a solution to the table that helps them prevent a catastrophe. For the author, it might be as simple as backing up to a CD, USB drive, or online backup location to prevent a serious, costly data loss. Remember—keep it simple, especially for small companies and individuals. Find the minimum they'll need to stay in business and make sure that is what's protected.

PROJECT PLAN COMPONENTS

Now that we've reviewed the success factors, let's look at standard project management plan components. If you have a methodology you use, this should track (generally) with yours. If you don't have a methodology you use and you're not familiar with project management, this will give you a basic overview. Our goal is not to delve into the details of project management—for that, you can pick up a copy of *How to Cheat at IT Project Management* by the author ([Snedaker, 2005](#)).

The basic steps in a project are:

- Project Initiation or Project Definition
- Forming the Project Team
- Project Organization
- Project Planning
- Project Implementation
- Project Tracking
- Project Close Out

Let's look at each of these briefly, and as they relate to BC/DR planning. Keep in mind that project planning and project management are both linear and iterative processes. This means that there is a logical flow that defines the order in which steps are taken; at the same time, many steps are revisited over time to add additional detail that helps more clearly define the project. For example, some elements cannot be known at the beginning of a project, so an estimate is used until enough detail is developed to go back and refine the original estimate. Although this sounds like it could lead to interminable planning (and it could), the goal is to continually move forward and to refine and hone details as they become known. This approach actually prevents "analysis paralysis," in which planners feel they cannot move forward because they do not have enough information or detail yet. Instead, this approach allows you to use estimates or placeholders, so you can move forward and develop the additional detail as quickly as possible. A good example of this conundrum is the budget for a project. In many cases, it's difficult, if not impossible, to give a useful estimate for the cost of a project until you've defined the project's scope, objectives,

and requirements. At the same time, it can be all but impossible to get the go-ahead for a project until executives have some idea of what it will cost. In some companies, this becomes a circular problem that causes projects to just spin in a loop, going nowhere fast. To overcome this, you may have to do some initial project definition work to develop a ballpark estimate to get the OK for the project to develop additional detail to give a more refined estimate of the cost. It may sound like a lot of rework, but it's actually refining instead of redoing, and this typically leads to forward progress.

TIP**Negotiating For Your BC/DR Budget**

If you're having trouble getting a budget approved for your BC/DR project plan because you don't yet know what it will cost or how long it will take to accomplish it, you may have to do some savvy negotiating with decision-makers. For example, in some companies, it might be effective to ask for a specific budget to investigate the cost of a BC/DR planning project. If you can get some staff time and a small budget allocated to investigate this, you may be able to come up with a fairly realistic ballpark estimate for the actual BC/DR planning project. In other companies, it might be more effective to look at annual revenues and talk to one of the financial people in the company to estimate the cost, in terms of lost revenue, lost market share, and lost customers, if a disaster were to hit. Using some estimate from a financial analyst within the company will lend credibility to your estimate and should at least help you get a budget for the first phase or for an investigation into the potential cost of developing a full BC/DR plan. In other companies, the only real constraint might be money, so you might get a go-ahead to use staff time and corporate resources as long as you don't spend any cash outside the company. This might be acceptable in the near-term and help you get your planning project underway with executive support.

You'll have to be creative and persistent in some cases, but the importance of creating a BC/DR plan cannot be overemphasized. Finding the right approach within your organization is probably the most important first step.

Project initiation or project definition

Project initiation or project definition (terminology may vary depending on your organization, the framework you use, etc.) is the first phase of any project. [Note: From here forward, we'll refer to it as "definition" because "initiation" tends to lead people to believe the project work has begun (i.e. the WBS is defined and tasks are underway), which is not the case.] In some companies, it's easier to get approval for a subproject plan whose only deliverable is a clear idea of what the project will be. The definition phase can include a variety of elements; we're going to look at this from both a BC/DR planning perspective and an IT perspective.

First, let's talk about project origins. In some cases, you may be approached by the CIO or another executive in the company about creating a BC/DR plan. In other cases, you may be pushing your organization to create a plan. If the former is the

case, it's quite common that someone has given you marching orders to which you're expected to produce a result. The problem is that without doing the requisite research and planning activities, a directive to create "a BC/DR plan with *x*, *y*, and *z*" in it will likely be off-target. It will have gaps or will include things that are not needed. So, how should you proceed if this project is dropped in your lap? The first step is to talk with the person who handed you the project. He or she is most likely the project sponsor. Get a clear understanding of expectations and what the project should entail. Ask what problem you're trying to solve. Typically, you can extrapolate key elements that should be included in the plan and from there, you can check back with the project sponsor. This step should never be skipped, and unless your company is run in a very old-fashioned "do as you're told" manner, you should always make sure you come back with questions, suggestions, and revisions. Rarely will a project be handed to you that is so well-defined that you can just put together a plan to accomplish the objectives and achieve success. Remember that executive objectives are usually quite different than the objectives needed for a solid BC/DR plan. For example, an executive may need to show compliance with a particular regulatory requirement. Your job would be to develop project requirements that would, when implemented, result in regulatory compliance. Although closely related, you can see that the executive's objectives and the project's objectives are not always one and the same.

Problem and mission statement

Often the most effective starting point is a problem statement. In the case of BC/DR, it might be as simple as "Our company operates in two geographic locations and generates \$25M in annual sales. We do not currently have a disaster plan for either location and the company is at risk as a result." Remember, you don't have to over-engineer this, but a clear problem statement helps keep you focused as you move forward so you work on solving the *right* problem. A brilliant project that solves the *wrong* problem is useless.

Next, you should create a mission statement. This, too, can be a fairly simple statement (and should not require a 3-day off-site to accomplish it) such as "To create a business continuity and disaster recovery plan for both of our company's locations that will address the major risks to our company and that will provide a path to recovery of the basic, mission-critical systems including *a*, *b*, and *c*." When you define a problem and then define what the desired outcome (mission statement) looks like, you have created your start and end points. This helps you define the scope of the project and gives you a clear end in sight, so you can begin planning a finite project. Looked at another way, you can define the current problem then define the desired future state. If you can articulate what success looks like, you can develop your outcome or mission statement and provide a clear target for your team. If you can develop a concise statement around what success looks like, you can use that in your meetings, as a summary at the top of BC/DR documents, etc., to consistently keep the target in mind.

Potential solutions

Once you've defined your start and end point, you can develop a list of potential solutions. This is an important and often-skipped step in project planning. One potential solution to be evaluated in all projects is "do nothing." Although it's often not a viable option, it keeps things real and helps you evaluate all potential solutions against the do-nothing option. Even though it's highly unlikely that a do-nothing solution would be appropriate for BC/DR planning, it should, nonetheless, be included. You can then measure other options against the cost of doing nothing and use it as a reality check with both your project team and your executive team.

Looking at all potential solutions will help ensure you don't pigeon-hole your project early on. The creative process of getting the project team together to brainstorm potential solutions may yield surprising results. For example, you might find that there is a vendor that sells solutions that will address all your BC/DR needs. You may find that you already have implemented many of the needed systems, and emergency procedures are all that are needed to create a solid BC/DR plan. Until you brainstorm all potential solutions based on the start and end point you've defined, you won't know what your options are.

That said, we're assuming that the solution will be to develop some sort of BC/DR plan. Though standard project management steps make sense throughout, the specific subject does need to be considered. After you've completed the risk assessment phase, which is part of the actual project work, you'll be in a much better position to determine the potential solutions. Then, you can select the one that meets project and organizational constraints and requirements.

Requirements and constraints

Another important element is to understand project requirements and constraints early on. Every project will have a stated or implied budget, timeline, and expected deliverables. You *will* have to revisit these once you select a solution, but you often can't select a solution until you have some basic requirements in mind. If the project was handed to you, you should go back to the person for clarification about these expectations. If you're initiating the project, you should try to develop some realistic expectations that you can bring to your boss or the decision-maker for feedback. If you're way out of the ballpark, this is a great time to find out. If expectations are significantly misaligned, this is the best place to find out that and correct it. It only will get worse from here. For example, is your budget likely to be \$10,000 or \$10,000,000? The budget will have a huge impact on the solutions you may choose to consider. Is your timeline 4 weeks or 4 months or 4 quarters? Again, your project will need to meet time requirements. What about technical requirements? Does your company have multiple locations? Are there employees who travel or work in the field? Do your customers purchase your products online? Do you provide technology services to end users? Are there regulatory requirements to be met? Understanding some of the high-level technical requirements will also be needed before you can select the optimal project solution.

Once you've developed your initial list of requirements and constraints, you should be able to identify which solution(s) best meet your project's problem statement and mission statement (problem and desired outcome). If more than one solution appears to be feasible and desirable, you may have to look at other factors to find the most optimal solution. What factors? Sometimes they're political—perhaps your CIO is partial to a particular vendor because they deliver the best customized solutions; perhaps your timeline would be better met by one solution; perhaps your budget constraint is really the most important aspect and one solution fits your budget better. The first major objective in a BC/DR plan is a risk assessment, which will drive many of your requirements. This is an excellent example of the iterative process needed in IT project management. You may have some requirements and constraints that are known at the outset of project planning; others may have to be developed later when more data have been collected.

Success criteria

Another element often skipped in project planning is success criteria. How will you know your project is a success? If you know this, you have a better chance of creating a successful project plan. If you develop the criteria by which you'll judge or evaluate success, you're less likely to find yourself chasing after ever-changing definitions of success. It doesn't mean they won't change or that you won't have to work hard to maintain these success criteria once the project is underway, but it gives you a known starting point. If you're not familiar with success criteria, here's a rather mundane example that should help. Let's say you need to clean up your office because it's a mess. Your success criteria might be these: (1) all loose papers are filed in marked file folders, thrown out, recycled, or shredded, as appropriate; (2) all books are stored in a bookshelf or the company library in Conference Room A; (3) all writing utensils are stored in a pencil holder or a desk drawer; (4) desk top is free of extraneous equipment not currently in use; and (5) all computer hardware and software (other than desktop or laptop computer and associated devices) are restocked in the lab or an appropriate location (not your office or your desk). Even though this might seem obvious, it essentially tells you what your office will look like once you finish cleaning it up. Most of us don't need a list of success criteria to know if we've successfully cleaned our office, but you can probably see how this could be extremely useful in project planning.

For a BC/DR plan, success criteria might look something like this:

- Enterprise Resource Planning (ERP) software 100% available.
- ERP data are available within 2 hours of any business interruption.
- Key systems (list them) are available within one business day of any business interruption.
- All data are 100% secure (maintain confidentiality, integrity, availability).

Remember, these are what success looks like. You may reasonably conclude that the first item, 100% availability of ERP system, is neither required nor feasible. It IS possible to over-engineer a solution. However, you may choose to start from an ideal

state and dial it back as you go. You may discover, for example, that as you talk with people in your organization, 100% is actually not required. Perhaps 95% or even 90% is acceptable in the event of a business interruption. While that may sound a bit crazy at the outset, it's a possible answer. If 90% availability is acceptable to the organization, it should be acceptable to you. You may strive for 100%, but the cost differential between 90% and 100% may be exponentially higher and may not be worth it.

Project proposal

Once you select your optimal project solution, you'll need to put together a brief project proposal. Essentially, the project proposal should include all the elements we've just delineated. It should be submitted to the project sponsor (we'll discuss the project sponsor in a moment) or to your boss. If your organization has a process for submitting project proposals, use that format. If not, include the elements listed here (you can modify to meet your specific needs):

- Business case (can include the problem and mission statements)
- Financial analysis (if appropriate)
- High-level scope, timeline, budget, and quality metrics
- Requirements, constraints, assumptions, exclusions
- High-level resource needs
- Phase schedule (if a phased approach will be used)
- Success criteria
- Risks, mitigation, and alternatives (risks to the project, not BC/DR risks)
- Recommendations

The project proposal can serve several purposes simultaneously. First, it can be used to convince executives that a business continuity and disaster recovery plan is needed and that you've given serious thought to the subject. It can be used to rally others in the organization around the need for a BC/DR plan and begin the process of gathering support and critical mass for such a project. Finally, it documents the beginning of the project so that you don't have to needlessly and repeatedly revisit these decisions and these data in the future. This can help the project move forward instead of sideways and help momentum build instead of just spinning in circles.

TIP

Document Version Control

Once you document these initial elements, you may want to start a decision document, with version control, to document decisions made along the way. Since a BC/DR project can span multiple departments, multiple stakeholders (who may change over time through promotion or attrition), and multiple iterations, it's always helpful to document key decisions. Simply recording *who, what, when, where, and why* for each key decision can reduce confusion and rework later.

Estimates

Although it's outside the scope of this book to discuss estimating in detail, it is worth talking about briefly. First, estimates are dangerous. More often than not, they become targets. The vice president catches you in the hallway and asks how much this BC/DR plan will cost. Without thinking too hard about it, you reply that you think it shouldn't really take more than a few months and about \$25,000. Congratulations, you've just committed yourself to two targets! Though you may preface your response with, "Well, it's really too early to say for sure, but I'm guessing . . .," you still have a problem. The VP may simply remember 3 months and \$25K. She's a busy person, after all, and she remembers just the facts. So, use extreme caution when tossing around estimates, especially ones that are just wild guesses. Remember, too, that your pre-amble (too early to say for sure) is completely lost, the VP remembers facts you've presented. The flip side is dangerous as well. If you're pressed for an estimate and you aim too high, the project could be in danger of being canceled. If you respond to your VP with "it's too early to say for sure, but I'm guessing two years and \$2,000,000," you may be in real trouble. Of course, for some companies 2 years and \$2M may seem like a very low target, it all depends on your industry, but the point is the same. Aim too low or too high and you'll be dealing with that problem for the remainder of the project.

Estimates can be generated based on past experience of similar projects, and these estimates, called *parametric estimates*, tend to be fairly accurate. When you can say, "The ABC Project was very similar in scope and requirements and it took six months and cost about \$50,000," you're in much better shape because the odds are good, if the projects really *are* similar, that estimates should be close. If you don't have a similar project you can use for comparison, you have to develop an estimate from scratch. These can be created top-down or bottom-up. The *top-down* approach is the fastest but least accurate method. The bottom-up is the slowest but most accurate method. A top-down estimate would start with an estimated budget, let's say, \$100,000. From past project experience (this is where the "experienced project managers" as a success factor comes into play), you might know that designing the requirements is usually about 10% of the budget, so you could estimate that designing requirements will cost \$10,000. You might also know that planning the project is typically 18% of the project budget, so planning should cost about \$18,000, and so forth. If you don't have a lot of project experience or a lot of experience at this company, you generally cannot create realistic top-down estimates. *Bottom-up estimates* typically are developed after you've created your detailed WBS, after you know what your tasks and deliverables are. Once that is known, it's a simple matter of adding up the cost of each task and developing a total. The biggest problem with bottom-up estimating is that you won't end up with an estimate early in the planning cycle. If you're trying to get project approval based on an estimate, a bottom-up approach won't work because it will require you do a fair amount of planning before you ever develop an estimate. In fact, the result of bottom-up

estimating is usually close to a real number you can use as a target or commitment (as opposed to an estimate that will need additional refinement).

As you can see, top-down and bottom-up estimating both have value, but it's a bit like trying to drill through a thick wall from two sides—you measure up from the floor and out from the corner and hope that the hole you're drilling from one side actually connects to the hole being drilled from the other—there's a good chance they come close but never actually connect. These two estimating methods are valid but are likely to not exactly line up. Keep this in mind—they're called *estimates* for a reason.

We've covered the basics of project definition very briefly. If there are elements you're accustomed to using or elements required by your company, certainly use them. If you're not familiar with these or other project definition elements, there are plenty of great resources on IT project management you can use, including one by this author mentioned earlier ([Snedaker, 2005](#)).

Project sponsor

A project sponsor often is the person that hands the project to you and assigns you as project manager. In other cases, especially situations in which you are initiating the project on your own, you'll need to identify a project sponsor. A project sponsor is someone in the organization who has the authority—both organizational and political—and desire to help you accomplish your project goals. He or she should have enough knowledge about the company and the project to help you make sound decisions, create a budget and timeline (or approve them), help remove obstacles, rally resources, and support and evaluate choices and decisions all along the way. If you haven't yet identified your project sponsor, you should do so early. Finding the right project sponsor can make all the difference to you and your project's success. If your project was handed to you, don't assume that person is also the project sponsor. Ask. The question that usually gets to the bottom of the issue is, "Are you the person who will approve the budget and schedule?" If no, you haven't found your project sponsor. He or she should be authorized to approve project documents, budget expenditures, and schedules. Some companies may operate differently, but the project sponsor normally has the authority and responsibility to approve expenditures, assign resources to your project, and remove obstacles to your success.

Keep in mind that your project sponsor for a BC/DR plan may be different than a typical IT project sponsor. The sponsor might be an executive vice president responsible for regulatory compliance; the sponsor might be someone who oversees facilities. It's hard to say who your project sponsor will be for a BC/DR project, but it should be someone who (1) understands the importance of a BC/DR project and (2) who has the organizational and political power to help a BC/DR project get off the ground.

REAL WORLD**Project Sponsor MIA**

Some project sponsors go missing in action (MIA) and become impossible to contact. If you're in search of a project sponsor, be sure to select someone you're confident will be available to you on a regular basis. You shouldn't have to run to the project sponsor for approval of every single item, but you should meet with your project sponsor regularly (via phone, net meeting, or in person) to discuss project progress. Should your project sponsor be someone who is not good at returning e-mail or voice mail, or regularly travels and is unavailable, your project will likely run into significant delays. Find a sponsor who will be available and then make sure you use your time with the sponsor productively. Be prepared, have an agenda, and get on with it. Some project sponsors go MIA if they find their time is not being used productively. Don't expect to chit chat over a double tall nonfat half-caf vanilla latte with your project sponsor—stay focused and your project sponsor may actually look forward to your meetings. Waste their time, and they'll dread (and then avoid) your meetings.

Forming the project team

You should form a project team pretty early in the project cycle for numerous reasons. You're unlikely to have all the knowledge you need to develop a sound plan by yourself and you will eventually need the input from various subject matter experts during the course of the project. Studies repeatedly show that those who help plan a project are more likely to contribute positively to the project because they feel a sense of control and ownership. Therefore, you would be ill-advised to create the plan on your own and unveil it to your project team. Instead, decide who should be on the project team, form the team, and create the plan.

There are times when it's not initially clear who should be on the project team. This may well be the case with a BC/DR project because it crosses so many organizational boundaries. One approach is to create a preliminary project team whose sole job it is to create the basic project definition and then determine who the right team members should be. In some cases, the original team might be suitable; in other cases, the team may require a few new members or the removal of a few existing members whose long-term participation just doesn't make sense. For example, it might be that the initial planning meeting(s) include area directors or vice presidents—especially if this project has high visibility, is related to ongoing regulatory compliance, or has been assigned by an executive. Once the high-level definitions are created, directors or VPs may then select members of their teams to join the project team and they, themselves, may bow out. This is entirely appropriate. The key is to develop your project team with an eye toward covering all your organizational bases. You want neither a team that's too narrow in focus nor a team that is so large as to be difficult to manage and coordinate. You can choose to look at your company in many different ways. One is to include the basic functions, which typically are operations, Human Resources, finance, facilities and security, logistics/purchasing, public relations and, of course, IT. Another way to look at it is by reviewing various categories. When forming your team, you could also consider these elements, which we'll touch on briefly next:

- Organizational
- Technical
- Logistical
- Political

Organizational

The first place to look is at your company's organizational chart. This will help you identify geographic locations, functional departments, or divisions of the company. These should all be included in your BC/DR planning process. Clearly, there will be some overlap that can help you pare down team members. For example, you may have an HR manager or a director at each of 10 worldwide locations. You may need all of them to work as a sub-team on HR needs during a crisis or you may select two of the most experienced to represent HR on our BC/DR team. If there are significant differences among your various worldwide locations, you'll need to look at the best way to approach HR needs, especially IT functions. For example, how is payroll processed in the Netherlands compared to how it's processed in Brazil or Australia? If it's all done through a single payroll processing company, you have different options than if each country processes its own payroll. There is no single right approach, so your best bet may be to form a preliminary team with the understanding that it probably has too many representatives and should be pared down once roles and responsibilities are known and understood.

TIP

Navigating Politics and Hurt Feelings

Things can get very political very fast when discussions of mission-critical areas of the business begin. Everyone wants to think of their part of the business as being critical to the company (i.e., if it's not mission-critical, why does it exist at all?). Many people become quite concerned when their area of business is not tagged as "essential to operations." Therefore, be on the lookout for power plays and bruised egos here. It's a delicate balance. You may need to resort to scenario-based questions to help people understand what BC/DR planning is and is not. For example, you might ask, "If this building caught on fire, what's the bare minimum we would need to get back up and running again?" This can help focus people on the project's objectives rather than on worries that their department or job function isn't included. Also, it often helps to indicate that work will be required of team members—that usually rids the team of the people who want to feel important but do not want to be held accountable for deliverables.

Technical

Which different technical specialties should be included? You may be unable to answer this question until you understand which areas of your business are mission-critical. The technologies used in areas of the business not considered mission-critical may not be represented in your planning. Alternately, they may be included in business continuity planning but not in disaster recovery planning. Some technologies may not be needed immediately but will be needed in the

long-term recovery of the business. Remember that technical issues involve not just the IT department but the facilities functions as well. How the building is heated, cooled, powered, maintained, and more impacts the IT function. If you have power but no heating or cooling, you may not be able to get systems up and running again. With the integration of the various technical components of your business, whether that's desktop computers, large server clusters, manufacturing systems, healthcare devices, and others, there are numerous technological factors to be considered in addition to IT-specific systems. Understanding how these work together and what elements truly are mission-critical in the aftermath of a disaster is an important area to explore in your project planning work. Understanding how you'll transition from disaster recovery to business continuity also requires a close integration of IT and non-IT technology management.

As more and more building automation systems now require servers (housed in the data center), network connections (housed in the data center or data distribution closets), and remote connectivity, even your basic building functions now rely on IT. Keep this in mind as you look at your BC/DR plans—the advanced needs of building systems are intrinsically tied to your IT shop.

Logistical

There are two logistical components—one related to disaster recovery and one related to business continuity. In the immediate aftermath of an emergency or disaster, the most important tasks are related to stopping the impact of the event. If there's flooding, one disaster recovery task might be to move servers or computers to higher ground or to contact your company's other locations and let them know they will need to pick up the slack. These steps "stop" the effect of the flood. After those tasks are underway, business continuity activities typically begin. How can the business get up and running again? To continue with the flood example, it might be locating a temporary office building or arranging with a contractor to come in and begin pumping water out and start repairs. These all involve logistics of various kinds. Those in your company responsible for logistics and/or purchasing should certainly be included in the BC/DR planning activities.

As mentioned, it's often quite helpful to contract for emergency services before an emergency. You can lock in better rates before demand spikes the cost. You can calmly and rationally order what you need rather than ordering whatever comes to mind during the emergency. You can develop and maintain a relationship with a variety of firms to provide those services; as an existing customer, you're likely to get preferential or priority service during an emergency. Your logistics staff needs to be involved with negotiating contracts for these mission-critical needs before disaster strikes.

Political

One element often overlooked is the political aspect of managing a crisis. Your company may need to communicate publicly after a crisis to assure stockholders and key customers that the company is intact and prepared to maintain or resume operations.

In addition, there may be internal political ramifications related to managing a crisis or emergency in your firm that should be addressed as part of your BC/DR plan. As an IT professional, you may not be aware of these political needs, so you should include people on your team who will be up to date on internal and external political requirements for your plan.

PROJECT ORGANIZATION

The project organization includes how you will organize and run your project. It begins with identifying the right project sponsor. Assuming you have a project sponsor, one of your first organizational tasks will be to define the elements that must go to the project sponsor for approval. Typically, the project sponsor approves the project scope, budget, and schedule, and any significant changes therein. Avoid having to get sponsor approval for every single expenditure and change or you'll forever be chasing your project sponsor trying to get requisite approval rather than getting project work done. Other organizational elements are discussed briefly next. Again, it's not an exhaustive or comprehensive list but just a reminder of the top level items and how they relate to BC/DR planning. In most cases, these are developed with your project team.

Project objectives

You've developed the problem statement, the mission statement, high-level requirements, constraints, and an optimal solution through the project definition stage. Now, you need to develop project objectives. The objectives for a BC/DR plan can be very narrow or very wide, depending on your company's specific situation. In this section, we'll list some of the types of BC/DR plans companies create. From there, you can develop specific objectives suitable to your company.

Business continuity plan

This plan focuses on sustaining the company's business activities, particularly those related to revenue generation and management of corporate obligations (employee payroll and health care insurance are two notable examples). A business continuity plan can be written for a specific business process or for all key business processes. As mentioned earlier, projects with smaller scope and more milestones tend to be more successful, so it might make sense for you to break your BC plan into smaller sub-plans, each addressing a specific set of mission-critical business processes. In most cases, a BC plan addresses the long-term recovery processes needed for the company to resume normal operations. Clearly, almost every company's BC plan will have an IT component since almost every company operating today (in industrialized nations) utilizes IT to some extent.

Continuity of operations plan

This plan focuses on restoring mission-critical operations at an alternate location and performing these functions for an extended period of time. This type of plan addresses a wide variety of companywide concerns and typically is developed independent from a BC/DR plan, but clearly there are overlapping components that may need to be coordinated across the projects. A continuity of operations plan might be developed as the overarching project and the BC and DR plans may be considered sub-plans. IT operations and alternate IT arrangements clearly are an important part of any continuity of operations plan.

Topics like high availability come into play in this realm. High availability looks at IT systems' architecture and builds in redundancy and fail-over capabilities to ensure critical business IT assets are always (or highly) available. This is very much related to both BC and DR but is a separate consideration. High availability will include hardware, operating systems, software (databases, middleware, applications), and overall infrastructure, among other things. It's entirely possible to have no "high availability" solution in place and still have very solid BC and DR plans.

Disaster recovery plan

This plan focuses on restoration of key business processes immediately following an emergency or disaster. Unlike a BC plan, the DR plan typically does not include processes and procedures for ensuring the continuing and ongoing operations of the company long term. Within the DR plan, there should be an IT section devoted to the technological needs of the company during an emergency and a section on the initial steps needed to restore all affected IT systems including business applications, servers, network infrastructure, and computer facilities to normal operations. It will also include the identification and specifications for an alternate operations site following an emergency. In some companies, noncomputer technologies such as communications equipment (cell phones, walkie-talkies, emergency radios, etc.) fall under the purview of the facilities manager rather than the IT department. As an IT professional, you are in an excellent position to understand how all corporate technologies can be effectively deployed and utilized during an emergency, so your input on this topic, even if it's ultimately managed by some other department, can be extremely helpful.

Crisis communication plan

A crisis communication plan should be developed, either as part of your BC/DR plan overall, or as a separate, but related, project. Communicating effectively during a crisis can make a difference in determining whether the company ultimately succeeds or fails. It also can help employees maintain a sense of calm and order by giving them important information they might not have access to otherwise. During normal operations, employees gather information about the company from a variety of informal sources—instant messaging, chat, e-mail, and hallway conversations with coworkers. During a crisis, employees often are cut off from one another or unable to use normal communications channels. Planning for this and providing

consistent and clear communications for employees and external parties helps organize recovery efforts and helps reduce some of the anxiety employees' face when a disaster hits their company. Questions such as, "Was anyone injured?" "Will I still get paid this Friday?" and "Where should I report to work on Monday?" can be answered through the processes developed in advance.

In addition, you may have a large enough community or market presence that the media is swarming in the aftermath of a serious event. Even if you're a small company and you experience a large fire, the local media may show up asking questions about how and when the company will resume operations. Without a clearly articulated crisis communication plan that kicks into gear when a disaster hits, you could end up with an uninformed employee talking inappropriately with the media, sharing unflattering information rather than having an official company spokesperson answering questions in an intelligent and thoughtful manner.

Cyber incident response plan

This is certainly a plan that should be developed within the IT department and is most likely separate from the BC/DR plan. Although we typically think of disasters as large, physical events such as earthquake, fire, or flood, a security breach into a corporate network's critical areas can be a huge disaster on a number of levels. Recent examples of cyber threats include the hacking of the New York Times, the Federal Reserve, and numerous attacks by the Anonymous group. While the targets have been large, high profile organizations in the past, cyber criminals have (unfortunately) begun to understand that small- and medium-sized organizations can be target-rich environments. Smaller companies tend to have desirable data and less than state-of-the-art security, making these companies much more desirable than in the past. Therefore, your firm will need a cyber incident response plan (CIRP) as part of the DR portion of the BC/DR.

The CIRP establishes procedures to immediately address cyber-attacks against the organization. Procedures to identify the nature and extent of the attack, the ability to mitigate and stop the damage, and to recover from and resume IT operations should all be included. Clearly, cyber threats are ever-evolving, and your CIRP will need to continue to evolve and be updated on a regular basis. Incidents such as unauthorized access, denial of service, data theft, data alteration, and unauthorized system reconfiguration are all examples of problems to be addressed by a CIRP. Like the BC and DR plans, the CIRP plan requires a specialized team that is trained and ready. A Cyber Incident Response Team should be formed and trained to quickly and effectively take action immediately upon discovery of a cyber-incident. Typically, the faster and more decisive the action taken, the less damage done to the company's electronic assets.

Occupant emergency plan

This type of plan is related specifically to the building's occupants. It includes how to safely exit the building in the event of a fire; where to gather outside the building or where to congregate inside a building if the best option is to *shelter-in-place*. It also

details procedures for contacting emergency personnel including fire, police, and medical assistance. This plan is typically part of the Facilities department, but in the absence of such a department, you should include these types of plans in your BC/DR plan, either as part of the overarching BC/DR plan or as a sub-plan that ties in. Clearly, if the building experiences structural damage as part of the effects of an earthquake or bomb, it will impact other aspects of the company's operations and a BC/DR plan will be implemented. Developing fire drills and evacuation procedures (for example) may or may not be considered part of your company's BC/DR plan, though these details should be managed by someone at your company. In the absence of a Facilities department or manager, these functions often are handled by the Human Resources department.

We've run through six different types of plans that are all related, in one way or another, to business continuity and disaster recovery planning. Clearly, they all overlap to some extent. It's important that you evaluate your company's emergency and disaster readiness and determine which of these types of plans will most suit your company's needs. Some of these plans may be developed independently from the BC/DR plan. In other cases, you may form a steering committee or designate a Program Manager to oversee the development of a number of related sub-plans.

Project stakeholders

Broadly defined, the stakeholders for a BC/DR plan can include the government, various regulatory agencies, financial markets, public shareholders, private shareholders, employees, vendors, suppliers, contractors, and the community at large. That's a large list and clearly, it's not appropriate to invite them all to your planning sessions. However, it is important that your project team consider the broadest scope possible so that you can ensure that various stakeholder interests are considered and included when appropriate. For example, if your firm is subject to financial, legal, or environmental regulations, these must be considered as part of your overall BC/DR plan. If your firm is subject to these regulations, you will most likely require input and assistance from specific subject matter experts such as your financial or legal counsel. If you have in-house experts responsible for maintaining compliance to various regulations, these folks can be invaluable resources as part of your planning team.

However, let's narrow the scope for a moment. *Stakeholders* are, by definition, those who have a stake or interest in the outcome, results, or activities of the project. This is important because we're not only talking about the *results* of the project but the *activities* of the project. That means that if you need to pull people from other departments or off of other projects, those department or project managers are stakeholders in your project—they have a stake in the activities of your project. Their interest may be limited to when they can get their personnel back in the department or project. As you develop your BC/DR planning project, keep in mind all potential stakeholders. If your project is going to pull resources from other departments, for example, be sure to include those department managers in high-level project progress

reports (if appropriate), so they are aware of the project's progress and have a contact person they can go to for status update or timelines. In small companies, this probably won't make much sense, but in larger companies or companies that are geographically dispersed, it can make the difference between gaining support for your project and irritating a bunch of people who have the distinct ability of making your life as project manager difficult.

The usual suspects should also be included in the list. Executives are stakeholders since they have a vested interest in the outcome (and effectiveness) of the project; they certainly are concerned with the cost as well as the risk/reward data. They may also have legal obligations, so they may be very closely tied into the project's objectives and outcomes. Even if there are no legal obligations, the executives or senior managers of the company should certainly care about the project's outcomes and objectives since the very survival of the company may depend on how well you define, create, implement, and maintain your BC/DR plan. Other stakeholders include facilities management, Human Resources (representing both HR functions and employees as a whole), supply chain, operations management, marketing/sales/PR management, financial/legal management, and of course, IT management. If there are other departments in your company not represented by the preceding categories, include them if appropriate.

At this point, you may have a long list of project stakeholders. That's OK. At this point, you need to be *inclusive* rather than *exclusive*. As you move through your project planning process, you will develop communications plans to address the various *categories* of stakeholders so that you don't have a list of a thousand people to whom you have to report every day. Stakeholders' interests and concerns must be addressed, but it doesn't mean they need to participate in the project itself.

Project requirements

Poorly defined project requirements can cause project failure, so it's important to take affirmative steps to develop better project requirements. It begins with project definition, which we discussed earlier. What problem are you trying to solve? What is your mission statement or big-picture outcome? When you know what problem you're solving and what you're trying to achieve, you have defined the boundaries of your requirements.

Another activity that adds to the success of project requirements development is involving the right people early. If you wait until your plan is 75% complete to bring the Facilities Manager into the loop, you're likely to have missed something important or you have to rework much of your plan. Failing to bring the Facilities Manager into the loop at all would be even worse. It's not inconceivable that a plan would be created by the IT folks and completely omit facility issues such as heating, cooling, drainage, and other issues. IT folks are smart but, like any other specialists, can become myopic and miss things that are obvious to others. So, word to the wise. Bring in the right experts early and have them help develop the project requirements.

It's easier to pare down requirements than to try to add to them when you discover an omission or gap later on.

Let's look at some examples of project requirements for a BC/DR plan. Clearly, you'll need to create your own list and modify it as you move through your project in order to address the specific needs of your company, but this should give you a running start. You should start by delineating requirements known at the outset of the project, but accept that project management is an iterative process and you will have to revisit your requirements as more information becomes known and details become clearer. So, let's look at some samples.

- E-commerce functionality (*define which functionality this includes*) must remain up to 99% of the time, enabling customers to place and manage orders and to receive order status. Functionality includes product presentation, price and product information presentation, search, shopping cart, payment, order processing, credit card processing, customer order notification, warehouse order notification, warehouse pick tickets, shipper notification, customer shipment tracking notification, and inventory management.
- E-commerce customer service must remain available 85% of the time, enabling customers to interact with company representatives to answer questions and resolve problems.
- Customer order fulfillment must remain in place, regardless of company warehouse status.
- Employees must be paid on a regular basis or on the normal schedule during an emergency.

Notice that the first requirement describes functional and technical requirements. Sometimes they're closely intertwined, other times you can list technical requirements and functional requirements separately. In this case, the e-commerce functions are required and the technical requirements of that functionality are described. Don't get caught up in whether something is a functional or technical requirement at first, just be sure to capture the requirements. You can always move them around later once you've capture the requirements.

This example shows a company that does 100% of its business via a Web site (or Web sites). Clearly, Web site uptime is critical and will be the primary focus of BC/DR planning efforts. However, there are a lot of backend functions required to ensure that the Web site does more than electronically keep track of orders. Product must be in stock in inventory somewhere, someone must pick it, pack it, and ship it, and notify the customer it's been shipped. The on-hand inventory must be updated, credit cards have to be charged, income accounts must be updated, and so forth.

Let's look at another, more complicated example—a hospital IT department. What must be in place for this organization?

- 100% availability of key medical data ("key" should be clearly defined) for patients currently in the hospital.

- Availability within 4 hours for all key imaging data (“key” should be clearly defined) for patients currently in the hospital (X-rays, CT scans, etc.).
- Ability to access full medical record for patients in the hospital within 8 hours of disaster event.
- Ability to recover full medical record for all patients (historical) within 2 weeks of disaster event.
- Ability to collect and process billing and insurance information within 1 day of disaster event.
- Ability to pay staff according to established payroll timelines.

The list can go on, but the point is clear. The key elements of the business of a hospital include patient safety, patient care, and the ability to collect revenues and continue operations. When we look at this more complex example, it becomes very clear that you’ll need subject matter experts from across your organization to effectively develop project requirements.

Well-defined project requirements will help you ensure that your project works once it’s implemented. Although people rarely feel there is adequate time to plan (including creating project requirements), they will be forced to find the time to deal with the aftermath of a disaster. Thus, the choice is to take time to plan now to reduce the time to recover later, or extend the time to recover later with the high likelihood that recovery will fail and the business will close its doors.

Project parameters

Project parameters are scope, budget, schedule, and quality. The scope of a project typically is defined by the objectives and resulting technical and functional requirements. However, you can also create scope statements. One method that is particularly helpful is to state what *is* and *not* included in the project. Often by creating paired statements, you generate a clear picture of what the project work will entail. Although it may seem redundant to state what is not included, it helps avoid making incorrect assumptions. We all know that 100 people can read a statement and come away with 100 different interpretations of that statement. When you include both IS and IS NOT statements, you help narrow down the interpretations so that you are more confident that everyone is literally and figuratively on the same page. Scope is defined as the total amount of work to be accomplished; budget is the total cost; timeline is the schedule or total duration of the project; and quality is the number of defects or the overall level of rigor you’re willing to accept. In this case, defects might be total hours of downtime per incident. Remember, it’s possible to over-engineer a solution, so keep your eyes open for this potential. For example, you may have a lot of miscellaneous data on your storage systems that if lost might be unfortunate but not mission-critical. Is your organization willing to let that data go in a disaster event? Possibly. What’s the cost to back that data up and make it available? Maybe it gets backed up, archived off-site, and recovered as time allows in the event of a disaster. That’s a choice that must be made consciously (using IS and IS NOT statements) and can help you scale down your BC/DR plans as you go.

You may find that your plan is too all-encompassing to start with as you try to cover all your bases. As you continue to hone your requirements and your project parameters, you may be able to find areas to scale back. [Hint: Record these in your decision document for future reference.]

The budget and schedule for the project will certainly require multiple refinements. However, you may be handed a deadline or a specific budget amount to which you must manage the project. In most companies, there is neither unlimited time nor unlimited money, so you will be required to limit one or more parameters. Just as a quick review, [Figure 3.2](#) shows the relationship of scope, budget, schedule, and quality.

The project's scope should be defined at the outset by the amount of time and money you can devote to the project and also by the level of quality you require. Any change to the project's schedule, budget, or quality requires a change to the scope or to another parameter. For example, in [Figure 3.3](#), you can see that if you reduce the budget and keep the schedule the same, the scope is reduced by a corresponding amount.

Another alternative to reducing scope is to increase another parameter. If you have to reduce your budget by 30%, you may be able to increase your schedule by some amount to offset the reduction in budget. If you have to reduce your schedule (meet a tight deadline), you really have only four choices: increase your budget, reduce your quality, reduce your scope, or cancel the project. In the case of a BC/DR project, canceling the project is not a viable option (though often done), but in many other types of IT projects, it may actually be a viable alternative to consider.



FIGURE 3.2

Relationship of scope, budget, schedule, and quality.

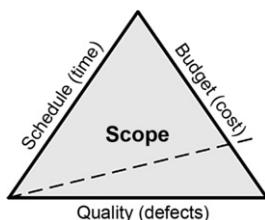


FIGURE 3.3

Impact of reducing budget on project plan.

Figure 3.4 shows the impact on other project parameters of reducing the schedule to meet a deadline. In this case, the option is to cut the scope significantly. In other cases, you might choose to keep the scope the same but reduce quality or keep the scope the same and increase the budget. The bottom line is that you cannot reduce the schedule without impacting one or more of the other parameters.

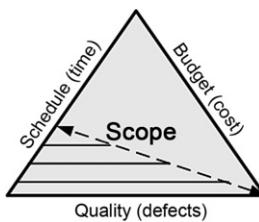


FIGURE 3.4

Impact of reducing project schedule.

If you decrease the schedule and don't want to reduce the scope, you typically have to increase the budget. Sometimes you can reduce the quality, but that gets tricky. Quality usually is defined as the number of defects or level of rigor you're willing to accept. In a BC/DR plan, it might mean the difference between requiring 90% critical systems availability and 75% critical systems availability. Although 75% might be considered a lower-quality metric, it doesn't mean you're actually accepting a "poor"-quality project deliverable. There are various areas in your BC/DR plan where you may say that a certain number or percentage is acceptable. This typically is done to address the interplay between planning for business continuity and working within known constraints. Though we've stated it before, it's worth repeating: be cautious of over-engineering. If 75% is perfectly acceptable, don't aim for 90%. The additional cost and effort may not provide any significant gains and may take away resources for other critical elements of the plan.

If you have a specific budget or timeline, you'll have to compromise throughout your project planning process. Although it's best to start with the most optimal solution and scale it back from there, you may also start out knowing that you have significant constraints within which you have to work, and you begin your planning process there. Remember, it's unlikely that any realistic plan you devise will be perfect. The goal is to create a plan that is workable and that ultimately will keep you in business after you experience a business disruption such as a natural disaster or a security breach. In many cases, the cost of the project will be predetermined—an executive might say, "We understand this is important but our funds are stretched. We can devote \$25,000 to this project over the next three months and not a nickel more." Therefore, your budget will be your *least flexible* parameter. This means that everything else will have to flex around your budget. Often this forces you to take longer to complete a project or to accomplish less work than desired. Regardless of whether or not you feel the parameters are optimal, you will have to manage your project to them.

TIP**Clearly Document Concerns**

If you are forced to make compromises that you deem to be unacceptable, it's highly recommended that you state your concerns in clear, concise business language and bring them to your executive sponsor or your manager. Put it in writing (e-mail is a great method of ensuring delivery) and verify your sponsor or manager is aware of the risks. If you allow the company to cut corners that ultimately have a negative impact on the organization, you are culpable. If you bring these issues and concerns to light and advocate for taking a different path, one you believe will lead to success, then you're fulfilling your fiduciary responsibility to the company. If you ultimately are out-voted or out-ranked and sub-optimal choices are made, you will have documentation indicating you advocated for another solution. This is not about covering yourself, it's about documenting choices and decisions made so that as time moves on, it will be clear who made key decisions and why they were made. Organizations get amnesia and often make the same mistakes repeatedly. Documenting issues and concerns can be one way of preventing those repeated mistakes even if you can't prevent them this time around. On the upside, if you are successful at articulating your concerns, you may sway your sponsor or manager to take the path you're advocating. Just be sure you're right.

Project parameters need to be ranked from *least flexible* to *most flexible*. The least flexible item is usually the one to which you must manage the entire project. In this example, we're assuming that the *least flexible* parameter will be your budget. Another parameter must be designated as *most flexible* in order to provide your team with the flexibility it needs to develop and implement the project successfully. The most flexible parameter is the one that will change when things go wrong (and they will go wrong). The other two project parameters may flex or not, depending on your company's constraints and the project's needs. As you develop these parameters, you will have to come back and make modifications once more detail is known. This typically occurs during or after the development of the WBS (discussed later in this chapter). Once you know what tasks are involved in your project, you'll be able to create a better timeline, a tighter budget, and a more realistic view of the total project scope. Parameters can then be marked as less flexible, most flexible, or not labeled. By default, any project parameter not labeled as least flexible will flex only if needed.

Keep in mind that the project parameters are all interrelated. You can't change one without impacting the others. It's a certainty that something will go wrong in your project—the project management adage, “Things are more likely to go wrong than likely to go right,” sums up how projects tend to run. Therefore, one of the project parameters must be able to flex. In a BC/DR project plan, this could be the scope, the timeline, or the quality. If your budget is least flexible and your scope is most flexible, you would do less project work if you find yourself straining your budget. If your timeline is most flexible, you would push your schedule out into the future to accommodate a tight budget. This might mean that you avoid overtime or that you schedule this project work around other higher-priority projects. Finally, your quality might be the most flexible item and you might decide that your organization can put

up with longer outages than originally identified. Sometimes a company will look at the cost of a BC/DR plan and determine that if the cost of creating the plan is X, then it is willing to put up with an outage of $0.25X$ at any given time.

Some people think that designating a parameter as the one that will flex is a crafty way of saying you don't have to make a solid commitment and hit real targets. Not so. The reality is you will find that, as the project moves forward, unanticipated things happen to which you must respond. When you have your project parameters labeled as most to least flexible, you know how to make appropriate decisions. If you go into your project saying that you will hit all four project parameters on the nose, you have very little chance of success. It doesn't mean that you won't give your absolute best effort to meeting the metrics to which you've committed, but it does give you (and your project sponsor) a solid framework in which you can make decisions when things change or go wrong. Also keep in mind that as you move through your project definition and project planning stages, your project parameters will become better defined. You may have to settle for estimates in the early stages and redefine these parameters as detail becomes known. Once you have a project plan in place, you will have to commit to those parameters as targets, but you'll still need to understand the interplay of these parameters to make appropriate adjustments as project work progresses.

Project infrastructure

Project infrastructure refers to the tools and resources you'll need to have at your disposal as you develop your BC/DR project. This might include computers, software applications, testing labs, communications equipment, and more. For example, if you're working with a team located in several countries around the world, your project infrastructure might include some sort of collaboration software, net meeting capabilities, along with e-mail and instant messaging. Since you'll likely be working at different hours, depending on the time zones involved, you'll need tools that allow you to manage a cohesive team while working within the local constraints. Your infrastructure needs for your team should also be viewed with an eye toward your BC/DR planning. Which of these tools might be useful if one location were to experience a natural disaster or business disruption? Which of these tools would be completely useless or inappropriate? Whenever possible, you should look at the technology and infrastructure tools you use in your planning process to determine whether it would also be a good tool during a disaster or event. This is also a way to start building BC/DR elements into your operational budget and operating procedures if you are having trouble getting a formal go-ahead for a full on BC/DR project. The intent is not to be sneaky but to intelligently leverage resources to meet organizational goals and objectives. It can be argued that in almost all business cases, a key organizational objective is always "survival of the organization."

The infrastructure for a BC/DR planning project may be as simple as e-mail, instant messaging, and a shared folder on a network drive or a secure cloud storage solution. It might be quite a bit more complex, especially if you work in a large,

geographically dispersed organization with multiple sites or many different business units. Clearly, the infrastructure for a 10-person software development company or a 50-person nonprofit social agency is very different than the infrastructure needed for a 100,000-person, 400-worldwide-location, and 50-business-unit type of company.

Defining the infrastructure you'll use to plan and implement your project is important at the outset so that you know what you will have access to, what you can use, and what's off limits. Defining your infrastructure needs may impact your budget if you don't have the infrastructure in place. In most cases, though, it's a matter of defining what infrastructure you'll need, how you'll acquire it, and how you'll utilize it to accomplish project objectives.

Remember that geographically dispersed teams may have varying levels of access to infrastructure such as conference calling, video conferencing, net meetings, e-mail, instant messaging, shared team intranet Web sites or portals, and so on. For example, some members of the team may have access to wireless Internet access; others may have to be at a corporate location to connect. Some members of the team may be able to make international phone calls, others may not. Some members of the team may have reliable communications lines, others may not. Keep these considerations in mind as you plan your project's infrastructure.

Project processes

Processes needed for developing and running a BC/DR plan are similar, if not identical, to running any other sort of IT project. If you're an experienced project manager, you probably have notes on processes and procedures you've used in the past, which you can pull out, dust off, and review. In most cases, these processes and procedures can be reused, though usually with slight modification. If you're not an experienced project manager, you might be wondering what sorts of processes you'll need. There are numerous resources you can reference; we've included a few of the basics here to give you a jump start.

Clearly, you'll need to adjust existing processes to address the unique needs of your BC/DR team. In many cases, an experienced PM has a set of documents he or she uses for every project, modifying the processes slightly each time to fit the circumstance. If you're not an experienced project manager, you will need to define all the project processes you plan on using. Some may argue against documenting these processes, stating they are a waste of time to document. It may not be useful to document every process, but it is well worth your time to define and document (and later archive) these processes for two primary reasons. First, it will reduce problems later if you have a set process for handling common project tasks or processes. Consistency in project work typically yields higher-quality results, so defining processes that can be reused during the project (such as the process for generating progress reports or the process for running team meetings) will help save time and lead to better results. For example, if you're stumbling around during each team meeting because you don't have or aren't following a set process for running team meetings, you're wasting everyone's time. You'll find that people begin to skip

team meetings because they view them as unproductive. This leads to other problems that ripple through the project. A second compelling reason for creating these processes and documenting them is that at the end of your project, you can review these processes, make adjustments, and file them away. When your next project comes along, you simply have to pull out the files, review them for appropriateness, make minor modifications, and move along in your project work. Using processes that have been used and tested over time usually leads to higher productivity and lower stress for you and your team. You should take advantage of any opportunity to save yourself time and aggravation.

BEST PRACTICES

Repeatable Process

It is well established that repeatable processes generate higher-quality results. They also tend to reduce stress for team members. When processes are known and followed, staff are freed up to use a more creative and intelligent set of thinking skills. So, the next time someone chafes at having a defined process for mundane tasks such as meetings or meeting minutes or change management, remind them that their talent is needed to solve real problems, not chase after routine issues.

Team meetings

Project processes in a BC/DR planning project are basically the same as those used in any other type of IT project plan, with one exception. BC/DR plans typically span across organizational and functional boundaries. Many IT projects do not. You'll need to determine how the team works together and how information will be shared, stored, and archived. You'll also need to address the logistical aspects such as determining how, when, and where the team will meet. Letting team members know how meetings will be set, at what interval, how they'll be notified or reminded, how agendas are determined, what they'll be expected to prepare, how they'll be expected to participate, and how meetings will be run in all part of defining the team meeting process.

Reporting

You'll need to develop a two-tiered reporting process. One level of reporting will be you, as IT Project Manager, reporting to your project sponsor regarding the overall status of the project and any challenges or roadblocks you encounter that impact the project or with which you need sponsor assistance. The other level of reporting will be reporting from your project team to you, as IT Project Manager. You'll need to develop reporting methods using processes and procedures familiar to those in your company. Whenever possible, you want to avoid reinventing processes and procedures for two reasons. First, developing new procedures often leads to resistance because team members are unfamiliar with them. Second, new procedures can cause unintended effects that can ripple through the team or the department's productivity. Whenever possible, keep reporting requirements focused. Avoid dragging a wide net

gathering every last detail. There may be an appropriate place to create a repository, such as creating a project-related *wiki* into which team members can dump all their collective knowledge. Keep formal reporting to the elements that actually impact the project's progress and ultimate success. Your teammates will appreciate your lean operating style and you won't have to pour through reams of documents to find pertinent details.

Escalation

How will problems within the project or external problems that impact the project be escalated? It's important to define this process before it's needed. You'll need to know which problems require sponsor notification or sponsor approval versus problems that require escalation through a different channel than the project sponsor. If you have a problem with a team member that cannot be resolved, how will that be handled? By you? Your manager? The team member's manager? If you have a major problem getting payment for an approved expenditure to a vendor, how should that be escalated? If you run into a serious project roadblock and all work has to come to a stop until it's resolved, how is that escalated? Your basic escalation procedures may include a division of internal and external problems. Problems that are internal to the team will be treated in one manner, problems external to the team (i.e., within the company at large) will likely be treated in a different manner. Similarly, problems internal to the company will be addressed in one way, and problems external to the company (i.e., with vendors or regulators) will most likely be handled in a different manner.

The escalation procedures for each category should include *boundaries*—which issues qualify for escalation? If possible, create specific and quantifiable metrics for deciding which issues are escalated. In most cases, these escalation procedures should be provided to the team, so they understand how issues will be resolved. There may be a subset of the escalation procedures you choose not to share with the team, but, in general, the more the team knows about how things will work, the more effective they can be in making project-related decisions. For example, if a needed item is not received within 14 days of purchase, a team member can escalate directly to the purchasing department for resolution. If a needed item is not received within 21 days of purchase, a team member must escalate to the Project Manager. These kinds of clear parameters for key items can facilitate fast decisions and empower team members to resolve issues within certain boundaries.

Escalation procedures should also indicate the chain of command for various types of problems so that you know the appropriate resource to utilize should a problem arise. Which types of issues should be brought to your manager, to your sponsor, to someone else's manager, to the executive team?

Finally, delineate how escalated issues will be tracked and closed. Some project managers like to dispatch issues as Closed—Resolved, Closed—Unresolved, Open, and Deferred. Whatever categories you choose, define how they'll be used and use them consistently.

Project progress

How will the progress of project work be tracked? You might choose to have task and project progress tracked through team reporting, through an interactive team Web site, or through other tools you may have used in the past or have available to you for this project. Again, as with reporting, keep it simple. It's human nature to fabricate reports and progress notes if the requirement for producing such documentation is overly burdensome. In plain English, encourage your team to give you the real data you need with as little effort as possible. Think about how you'll need to report project progress to the executive team and to your project sponsor, then determine the bare minimum you need to know from your team. Start from there and add to the tracking requirements only as needed. Also, just because certain data may be available to you or your team, it doesn't mean that data help you monitor project progress or help move the project forward any better. Keep it streamlined and simple whenever possible and be sure that you're asking for data that actually are useful in monitoring or managing the project.

TIP

Only Collect Data You Need

If you find you're collecting status reports, statistics or other data you're not finding useful, stop collecting it. It can be hard to pull back from a defined process of information sharing, but there's such a glut of unused data sitting in everyone's Inbox that you'll be thanked for stopping the flow of useless data.

Change control

Most projects encounter the need for some sort of change along the way. In a BC/DR project, one of the most likely sources of change is that a new technology is being implemented. For example, if your firm decides to implement a customer relationship management (CRM) solution, you'll need to add that to the scope of your BC/DR plan so that you can address the specific needs related to this application. The business will not stand still while you're planning your BC/DR project, so there's a good likelihood some sort of change will be required as you move forward. What process will you use to control change?

Though it's outside the scope of this chapter (and book) to discuss change control in detail, a few reminders will probably help. First, though it may sound clichéd, it's still true: Control change or change will control you (and by extension, your project). Define a change request process so that needed changes must be formally requested. This provides you and your team the opportunity to evaluate the requested change. In too many companies, someone (usually an executive) with clout will demand a change to the project and everyone on the project team will scurry around trying to incorporate that change. Without a formal process for managing it, change will be introduced into your project in a random fashion. Once you have a defined process for requesting change, you should develop a defined process for evaluating change.

The evaluation should include the risks involved with making the change; the risks involved with not making the change; and the impact to the scope, schedule, budget, and quality of the project if the change is implemented. Finally, you should have a change tracking process that indicates that a change was requested, reviewed, accepted (or rejected), and incorporated.

BEST PRACTICE

Close Out Change Requests

Always close the loop on change requests. If you have change requests that have been evaluated and deemed too risky, too expensive, or simply undesirable for any reason, you should have a mechanism in place for declining these changes and communicating with the requestor. Most people can deal with bad news, but they can't deal with no news. Don't leave people hanging. Give them a "quick no" when the answer is *no*. It saves everyone time and aggravation.

Quality control

Quality control is a topic that can fill volumes on its own, so we'll limit our discussion to quality control as it relates to BC/DR projects. Clearly, one error in the project plan could mean the difference between getting a critical system back up and running in 1 hour versus 1 month. However, it's unrealistic to expect that you will have zero defects in your project plan and implementation. How much quality is enough? There's always interplay between how much time and money you have and how critical the systems are. For example, you might decide to spend a disproportionately greater amount of time testing your CRM or ERP BC/DR functions and a disproportionately lesser amount of time testing some other part of your plan. If your CRM or ERP application is the most critical application from a corporate perspective, you may choose to devote the most planning, implementation, and testing to this area to ensure as close to 100% quality as possible. Although specific quality metrics for BC/DR plans may be difficult to develop or measure, you can use qualitative methods to determine what level of quality is required for each element of your plan.

There are many other project processes that you'll no doubt develop or use, but these are some of the basics to get you started thinking along these lines. If it's something you do repeatedly, you should consider developing a process for it so that you can perform more consistently and not have to think about (or reinvent) the process over and over again.

Project communication plan

Technically speaking, the communications plan may be considered part of the project processes. However, communications are so vital to the success of any project that it's listed as a separate entity because it has a unique level of importance and awareness. With a BC/DR plan, your need to communicate across departmental, positional, and geographic boundaries may be greater than in any other IT project plan you've worked on. That can be a tall order for even the most seasoned project

manager. How can you be sure you're communicating to the right people with the right language in the right frequency and the right medium? One of the best ways is to check with your subject matter experts, many of whom will be founding members of the team. If you're going to be working with technology plans that touch the entire organization, you will probably need to communicate with all corners of the organization. Those people on the team who represent the various areas of the company are probably in the best position to provide input as to how, when, and in what format to communicate with their constituents. It will ultimately depend on where your BC/DR plan falls in the overall list of priorities. If your plan is low on the list of priorities, timely and positive communication might help boost its rating. On the other hand, there are times when you might want to communicate only as needed in order to keep your project flying below the radar (to avoid it being canceled or reduced in scope, for example). Typically, communicating project progress is good for the project and a bit of positive PR can go a long way. However, in BC/DR projects that may not be too popular to begin with, you may decide your best move is to keep your team and your project sponsor fully informed but avoid more expansive communications. A discussion with your manager or project sponsor on this topic will help you develop an effective communication plan that fits in with the overall political climate of your organization.

REAL WORLD

Communicating Results of a Low Priority Project

We can emphasize the importance of business continuity and disaster recovery planning until the cows come home, but the truth of the matter is that some companies just don't care. You might find IT professionals creating BC/DR plans almost on the sly or as part of another IT initiative, so they don't have to formally announce a project that will get stonewalled from the start. Depending on how your company runs, it may be possible that you're working on a BC/DR plan without a formal charter—without formal recognition or approval from existing corporate authorities. As mentioned, some basic BC/DR planning can be incorporated in other IT activities. Though this is not an optimal situation, it is better than doing no BC/DR planning at all. So, how do you communicate to the organization if you have no formal BC/DR plan or if you know that your BC/DR activities might be thwarted if they came to light? Your communication plan, in that case, may be limited to those individuals who will be impacted by your plan. You may choose not to use the terms business continuity or disaster recovery. Instead, you may ask, "What would happen if this system went down?" This is clearly something that must be addressed in any organization, so if using the phrase BC/DR planning will get you off-track, don't use that language.

For those of you who might think this is a bit underhanded, remember that IT staff have to deal with the reality of system outages every day, whether a server fan goes out and the unit overheats or whether a vital cable is disconnected from a router. The point is that business disruptions will occur, regardless of whether you plan for them or not and regardless of what you call them. So, you might as well build in some BC/DR planning to your IT activities and avoid an all-out communications blitz if that's what it takes to protect your company, your employees, and your job. Granted, if you don't have executive level authorization or support for your BC/DR project, you will not be able to count on wildly successful results, but that doesn't mean you can't still make a positive impact...quietly.

PROJECT PLANNING

Planning the BC/DR project involves all the typical steps you'd undertake in any IT project planning process. However, there are two key elements in the project planning process worth discussing here. Developing the WBS for your BC/DR plan essentially defines the scope of the project. By definition, the WBS is the list of outcomes that must be accomplished in order to successfully complete the project; it describes 100% of the required work. Therefore, a well-developed WBS helps you deliver a successful project. The *critical path* is, by definition, all tasks in the project that if delayed will delay the completion of the project. Why is this important? If you are trying to meet a deadline for completing your BC/DR plan, you'll need to understand which tasks in the WBS are on the critical path and which are not. Those that are on the critical path can delay project completion; those not on the critical path cannot delay project completion. As a result, tasks not on the critical path are more flexible as to when they can be scheduled. Let's look at WBS and critical path in more detail as they relate to creating your BC/DR plan.

Work breakdown structure

The top level of your WBS in your BC/DR plan will most likely follow the structure of this book: Risk Assessment, Business Impact Analysis, Risk Mitigation Strategy Development, Plan Development, Emergency Preparation, Training, Testing, Auditing, and Maintenance. As we move through the remaining chapters of this book, you can compare your WBS structure to the material in this book. You may have additional elements for your WBS that are specific to your company's BC/DR needs; feel free to include those.

Remember, the completed WBS should describe the total amount of work to be accomplished. If there is a mismatch at this point, you need to reassess your WBS or your project's scope. These two items should be aligned so that the scope is fully described in the WBS (or that the WBS fully describes the desired scope). The elements of your WBS may vary from those outlined in this book, but the overall elements should match fairly closely. If there are any discrepancies, be sure they are by intent and not by accident.

Critical path

The critical path in your BC/DR plan will describe exactly how long the project will take and which tasks will delay the project if you run into problems on those tasks. Remember, tasks not on the critical path are the tasks that provide you and the project team with a bit of flexibility. As you probably know, tasks not on the critical path, by definition, have some float. *Float* is (essentially) the time flexibility of a task—it can be completed this week or next week without impacting the overall timing of the project. Tasks can move on or off the critical path.

A noncritical path task that is delayed long enough may end up on the critical path. A critical path task may, for some reason, move off the critical path if you discover there is some flexibility in the timing of the task. The key is to understand the tasks that are on the critical path and make sure you keep a close eye on these tasks if you are working on a tight timeline. If your schedule is your least flexible element (as discussed earlier), then you will have to manage to your critical path more than to your budget. You might face this situation if you are required by a customer to provide a BC/DR plan by a certain date in order to close a large deal. You may also be required by certain regulatory or governmental agencies to complete and submit a BC/DR plan by a certain deadline in order to meet compliance requirements or to avoid heavy financial or legal penalties. In these cases, your critical path will define your project's timeline and will be the key to successfully managing to a required schedule.

LOOKING AHEAD . . .

Strategically Planning Your Project Schedule

In planning your business continuity and disaster recovery activities, you're likely to find that the risk assessment and business impact analysis are the most tangible aspects to the process and are therefore the phases that move along smoothly. Conversely, when you get into the actual risk mitigation and emergency response strategies, you may find the project getting bogged down. It's easier for most people to sit around and discuss theoretical issues (what happens if the building catches fire, how would that impact the business) than to devise practical solutions within given constraints. In scheduling your project, you may want to account for this and move the early phases along more quickly and allow more time for strategy development rather than giving equal time to each phase or section of the planning process.

PROJECT IMPLEMENTATION

Since we're focusing on the IT aspects of a business continuity and disaster recovery plan, we need to state the obvious: IT is a moving target. Unlike other areas of the business, which may be fairly stable and static, IT is always changing. From reconfigurations to new security threats to moving a data center, there's no shortage of change in the IT department. How does this impact your BC/DR project implementation? It means that you will need to build in a process for monitoring change in the IT department and assessing what should be incorporated into your BC/DR plan. Here's an example. A nonprofit agency decides it needs an IT BC/DR plan. The IT director, with her staff of four, creates a plan. In the meantime, they have funds that must be spent before the end of the fiscal year that are earmarked for a case management application. The application must be implemented and it requires the acquisition and installation of another instance of the latest versions of Windows Server and SQL Server. These should certainly be included in the plan, so BC/DR issues can be addressed. If the agency's location has a major fire, how will the server hardware be affected? Is it on-site? What about backups? What arrangements should be made

to have alternative server hardware available? What arrangements should be made for off-site backup and data recovery? How will this be shaped by the implementation of the new application? These are the kinds of questions that may come up throughout the lifecycle of your BC/DR planning process because other IT projects are in various stages of planning, design, implementation, and testing. Each of these must be assessed for their impact on your BC/DR planning, and each must be assessed for the BC/DR impact on these projects. The interaction between your BC/DR planning activities and all your other IT projects is a two-way street—each ultimately impacts the other.

Ideally, you should strive to add BC/DR types of assessments and considerations into your standard IT processes. Over time, you'll discover this makes keeping your BC/DR plan up-to-date a bit less onerous. You might also discover ways to save time and money or streamline processes along the way.

Managing progress

Managing project progress is often a matter of organizational and project manager traits. As unique as each company and each project is, there are a few things that you should keep in mind for your BC/DR planning project. As mentioned previously, you should have some method of ensuring that current IT changes and initiatives are evaluated in your BC/DR planning. It would make no sense to develop a risk mitigation strategy for a technology that is being phased out or to purchase a new solution that is easily rolled into a current or planned initiative. As simple as this sounds, it's often complex in practice. It's easy to suggest that various technologies be evaluated as part of your BC/DR plan; it's another matter entirely to make sure that happens. Your project processes (described earlier in this chapter) should include some method of keeping an eye on what's going on in the IT department across the enterprise. You should develop a method of evaluating and incorporating technological components. We'll look at risk assessment in detail in the next chapter and that will provide you with some of the tools to evaluate the risk to various technologies. Once you understand the risk and the potential strategies to reduce that risk, you will have a better sense of which IT initiatives underway in your organization will likely come into play. It might be at that point that you talk with the entire IT team to see how their work impacts your project and how your project might impact their work.

In addition to keeping an eye on changing technology, you'll need to make sure you use a consistent method to monitor and measure project progress including standard tools such as reporting, dashboards, or whatever tools you are accustomed to using. Since this type of project spans beyond the scope (and authority) of the IT department, you'll also need to use your best people skills to keep the project moving forward since it's likely you won't have complete control to require that project work be completed in a timely manner. This is true of many types of IT projects, but it's especially true of BC/DR projects that cross all organizational boundaries and often have a lower priority in the day-to-day scheme of things.

Managing change

Any experienced IT project manager will tell you that managing a project is managing change. Despite our best efforts, our plans are always subject to change in the dynamic world of business. Although there must be certain areas that are nonnegotiable (these are typically the least flexible project parameters), there must be some room for change in a project in order for it to have any chance for success. Earlier, we discussed the importance of managing expectations regarding changes to your project. Without requiring the consistent use of your defined change management process, you'll end up with a project scope that is all over the map and four times larger than originally defined. As an IT project manager, you're probably familiar with managing change, but perhaps not across corporate boundaries. Let's review a few pointers for managing change effectively:

1. Define a simple, easy-to-use change management process.
2. Require that all requested changes go through the change management process.
3. Evaluate each requested change as to how it will impact the current project plan.
4. Evaluate the risk of each requested change and determine if it increases or decreases risk in the plan.
5. If approved, incorporate the requested change into the plan and update all parts of the plan impacted by the change.
6. When possible, incorporate one change at a time, so each can be properly evaluated.
7. Do not allow random or informal change requests to become incorporated into the plan.
8. Communicate with those requesting change as to the status of their request.
9. If a change is rejected, communicate the rationale for rejecting that change and be willing to listen. It may be possible you overlooked a critical factor or misunderstood key data. Also be willing to (politely) stick to your decision, despite pleas, cajoles, and threats of (or actual) escalation. You may not be popular, but you will be successful.
10. Keep track of all requested changes and how they are ultimately handled (accepted, rejected, postponed) and why.

PROJECT TRACKING

The metrics used to track projects vary with each company and with each IT PM's systems of project tracking, so there is no single, universal method for tracking a project. One of the keys to a successful project is to create multiple milestones so that you can easily see where you are versus where you said you would be (and, of course, where you *need* to be). At minimum, you should create milestones for each phase of work. Using our framework as an example, you should have a milestone at risk assessment, business impact analysis, and at each additional phase. However, if these phases or sections are going to span months, you should create interim

milestones. If you have a small company and your risk assessment activities will span a week or two, one major milestone is probably sufficient. Milestones will keep you on track, but you shouldn't create so many that you drive yourself and everyone around you nuts.

As an experienced IT PM, you also know that tracking involves monitoring the budget, keeping an eye on the scope and quality, and making sure change is being properly handled. Depending on how your company operates and what tools are available, you can use any one of a number of programs to track project progress, schedules, expenditures, and such. With BC/DR planning, you'll need to make sure that whatever you ask of team members to enable you to track the project is available to them. Remember that the Facilities Manager or your HR liaison may not have access to the same tools you do or that they may not be as comfortable with project tracking tools as you are.

There are more advanced and detailed ways to evaluate and track project progress including Earned Value Analysis, Schedule Performance Index, Cost Performance Index, and Estimate at Completion, to name several of the more commonly used tools. Discussion of these tools is outside the scope of this book, but you can certainly learn more about these methods through a variety of sources.

PROJECT CLOSE OUT

In most IT projects, project close out involves a hand-off to some other team within your organization. When you deploy a new HR module, the HR folks become the operational owners. It might be that the new wireless infrastructure is now managed by a different subset of IT staff or that the new application is now maintained through normal application maintenance procedures.

As part of the project close out, steps should be taken to operationalize the elements of the project necessary to now manage and maintain the project result. The same holds true for your BC/DR plan. Once you have completed the plan, it must be kept up to date through some sort of maintenance procedures. In many organizations, this is as simple as an annual review of the plan and a paper walk-through of the business continuity and disaster recovery steps delineated in the plan. In other companies, it might involve actually testing out some of the BC/DR procedures and even testing some of the defined recovery processes. Maintenance of the plan is important if for no other reason than the plan took a lot of time and effort to create and it takes far less effort to keep it current. As we've mentioned, an outdated plan can be worse than no plan at all because incorrect assumptions might be made. For instance, if a legacy system was slated as a fail-safe backup technology and that legacy system has since been decommissioned, your fail-safe backup is gone. If a disaster strikes now, the assumption that there is a bottom line fail-safe option is incorrect and could spell the difference between the company surviving the incident or not. Be sure your project close-out activities include handing off the BC/DR plan in such a way as it will be maintained. It can be helpful to schedule the annual checkup at the close of the

project so that it will be on the calendar, though it's also likely that in 12 months, that calendar will change and your review plans may be impacted.

Also as part of best practices in project management, it's a great idea to have a post-project review session to review what worked, what went wrong, and how project processes could be improved in the future. Taking away lessons learned and best practices from each project you participate in (or lead) can help improve organizational results and your personal effectiveness as an IT project manager. It will also save you time and money in the future to avoid the obvious mistakes. The goal is not to completely avoid making mistakes—mistakes will always happen—but to avoid making the same mistake twice. Capturing best practices and lessons learned from across the organization might help you fine-tune other IT projects in progress and might also help streamline your BC/DR project review process.

KEY CONTRIBUTORS AND RESPONSIBILITIES

Thus far, we've talked in fairly general terms about the business continuity and disaster recovery planning process. In this section, we'll discuss key contributors to your BC/DR plan and what the roles and responsibilities should be in an ideal scenario. While we outline the ideal scenario, you'll need to take a look at your company specifically and make modifications as needed. For example, your company may be so small there is no Facilities manager and that task falls to the Purchasing director, the Ops manager, or an IT manager. Your company may be so large that there are multiple levels of Facilities management up to and including a vice president. You'll need to scale the information in this section to your company's size and needs, but this will give you a good overview to use as your starting point.

First, let's list the roles and contributors and then delve into the details of each:

- Information Technology
- Human Resources
- Facilities/Security
- Finance/Legal
- Warehouse/Inventory/Manufacturing/Research
- Purchasing/Logistics
- Marketing and Sales
- Public Relations
- Operations

Information technology

Since we're focusing on information technology in this BC/DR planning process, you clearly need representatives from the IT group on this project. Which members of the team should participate? Well, that largely depends on the size and scope of your IT department. If it's a 3-person IT department, all 3 of you probably have to

participate. If you have a team of 40, you will need to select those people best suited to this project. Some of the factors you can consider in making your decision can be:

- Experience working on a cross-departmental team
- Ability to communicate effectively
- Ability to work well with a wide variety of people
- Experience with critical business and technology systems
- IT project management leadership

Experience working on a cross-departmental team

Having IT people on your BC/DR team that have successfully worked on a cross-departmental project can help facilitate the success of your BC/DR project. They may have established positive working relationships with key people in other departments that you can draw upon for your BC/DR project. They may have learned how to navigate some of the tricky political waters in your organization or they may simply have developed a broader organizational perspective that can help as you work across departmental boundaries to develop a successful plan.

Conversely, you want to try to exclude those who have developed a reputation for being difficult and not working well with others (especially in other departments). Though you don't always have a choice as to who's on your team and who's not, avoid troublemakers from the start. If you need their expertise on the project, try to contain them and restrict their interaction with others to a bare minimum. For example, if you have a difficult person on the team who is the subject matter expert for a critical business application, try to have that person work with as small a subset of the project team as possible. It's better to annoy 3 people than 30.

Ability to communicate effectively

The business continuity and disaster recovery project planning process is all about being able to discuss risks, alternatives, and strategies that work for a variety of stakeholders. Without the ability to communicate effectively with all kinds of people—technical, nontechnical, executive, management, and front-line—your team and your project will suffer. It's not uncommon to find some of the best technical people are the most challenged in terms of interpersonal communication skills. If that's the case in your IT department, you may want to include a few generalists who understand the technology and can also communicate effectively with a variety of people. These folks can act as translators, taking very technical or detailed information and paraphrasing it for other non-IT members of the team. If you don't have at least one person on the team who is an excellent communicator with regard to IT, you may well find that you have some serious miscommunications that occur through the course of the project.

Ability to work well with a wide variety of people

The ability to work well with a wide variety of people often accompanies the ability to communicate effectively. IT members on the BC/DR team will have to interact with end-users, facilities people, financial people, and many others during the course

of the project. The last thing you need is someone from the IT department representing the BC/DR project in a way that alienates the rest of the company. An example that probably jumps to mind for many of you might be the stereotypical “know it all” IT person who talks down to those who don’t understand the intricate details of the technology. These people tend to simply make enemies where none existed and you don’t need the added problems this type of person brings to a cross-functional team project.

TIP**Project Communication**

Since your team may need to communicate with corporate vice presidents, department heads, or front-line staff, make sure that you, as project manager, or someone on your team is comfortable talking candidly and appropriately with people in all positions. Some people get nervous talking with those who are much higher up in the corporate hierarchy and are unable or unwilling to speak candidly. Others don’t understand what constitutes “appropriate” communication and they tend to drone on or disclose inconsequential or embarrassing information. Make sure you or someone on your team is comfortable with and capable of interacting at all levels of the organization into which this BC/DR project may take you.

Experience with critical business and technology systems

Having people from the IT department with experience in critical business and technology systems almost goes without saying, but we’ll say it anyway so it’s not overlooked. Clearly, the critical business systems from IT’s perspective may not be the same critical business systems from the CEO’s perspective or from the financial analyst’s perspective. You’ll have time to test out your assumptions as you move through your project. If you’re a small IT shop, this is probably a moot point. In larger IT departments, you’ll need to look at your staffing needs and determine who should participate. This almost always runs into problems because your IT staff have other roles, responsibilities, day-to-day tasks, and project tasks they need to address. Often you are forced to choose between the person who is your first choice and the person who has the time or bandwidth to deal with your project. Unfortunately, the person who gets things done and delivers the best results is probably the person with the least time and bandwidth available.

In addition, you’ll need to balance the needs of your project with the needs of the IT department’s ongoing activities. If you’re in the middle of a roll out of a new technology, it’s going to be tough to find the time and resources to also participate in BC/DR planning. This may impact your overall BC/DR schedule or it might force you to work creatively with those subject matter experts. One potential work around is to flag the technologies you think are critical but wait until you’ve confirmed this information with the rest of the organization. Once you’ve identified critical systems from an organizational perspective, you can then tap necessary resources. This small work around might provide a bit of flexibility so that you can still utilize the subject matter experts you need without reworking your schedule or theirs.

IT project management leadership

We're assuming you're the IT project manager and you're heading up this project. However, whenever you can tap others with leadership ability, you'll get that much more mileage from your project. Clearly, you want people with leadership abilities who can also work effectively as part of a team. You don't need four or five people all trying to manage the project. Good leaders usually know how to follow and to head up smaller groups or initiatives within a project team. Tap into these resources to take some of the burden off your shoulders as long as these folks won't be the cause of messy political maneuvers and power plays. Remember, a good project manager willingly delegates to others on the team and spends more of his or her time monitoring project progress. When you have competent people on the team who will take leadership roles, your job of delegating and monitoring will be that much easier.

Human resources

Depending on how your company is organized, you may find that Human Resources (HR) encompasses many of the other functions listed in this section. In small companies, HR ends up being the catch-all for all the miscellaneous functions that have no home. In large companies, the miscellaneous functions typically are large enough to require a distinct department such as facilities, security, or public relations. We'll stay focused on traditional HR functions in this section, but as you read through subsequent sections, keep in mind they may be housed in HR. Regardless of how or where the function is managed, they all need to be represented in the BC/DR planning process.

Human Resources typically is responsible for helping to recruit new employees; managing the legal issues around hiring, firing, and performance management; and managing the payroll process including periodic paychecks, contributions to retirement accounts or saving accounts, increases due to promotions or raises, and managing other required paperwork such as verifying citizenship or the right to work in the country.

How will these functions be impacted by a fire in the building or a flood or earthquake in the area? The best person to answer that question is someone (or several people) from the HR department. What computer systems do they use to process payroll and other HR functions? What applications do they use? What forms are required by law? What forms are required by the company? These are questions your HR specialists will have to answer when you get into the BC/DR planning process. For now, think of whom in your company is responsible for these functions and add them to the list of team members.

Facilities/security

As mentioned, the function of facilities and security may be handled by your HR staff if you're in a small company, or these functions may be handled by someone in operations. Regardless of where these two functions are housed, they are a critical part of

the BC/DR planning process and should be represented by subject matter experts. Facilities typically handles the management of the office, warehouse, manufacturing, or storage spaces including cleaning, maintenance, set up, build outs, and remodels. They deal with occupancy and tenant issues as well as other legal or licensing requirements related to business operations in the facility. The department (or function) also usually handles the installation, management, and monitoring of key building services such as electricity, gas, water, building controls, elevators, fire alarms, security cameras, and, in some companies, communications equipment (Internet connections, telephones, cell phones, mobile radios, mobile devices, walkie-talkies, etc.).

Security includes controlling and monitoring access to the building, facilities, and grounds, dealing with imminent dangers such as structural, mechanical, or electrical failures, and sometimes dealing with employees who have been terminated or who are behaving in a manner contrary to acceptable and safe means. Security provided by most companies is to secure the assets of the company, not to provide policing services. Therefore, you can't assume that your security staff deals with all aspects of security. Nevertheless, both facilities and security functions should be well represented in your BC/DR planning project. You'll need to answer questions such as these: What is our fire drill policy? How is the building evacuated in the event of a fire or other internal disaster? What plans are in place for protecting staff from external dangers such as nearby chemical spills, noxious fumes, or railroad derailment? If something happens to the building, how will access to and from the building be controlled? What tools, supplies, and equipment will be needed by the company's emergency staff to communicate with each other and manage the initial impact of a business disruption such as a fire, explosion, or earthquake? These questions should not be answered at this juncture, but these are the types of questions that will be asked and answered later, within the scope of your BC/DR project plan.

Finance/legal

In some companies, it is the finance department, not Human Resources, that handles the payroll processing function. Finance also handles the tracking and managing of accounts payable (money owed to others) and accounts receivable (money owed to the company). Clearly, the company's very survival depends on being able to keep track of what is owed and what is due. Without the ability to manage the income and outflow of funds, the company cannot survive for very long. Certainly, the bank with which your company does business has records of recent transactions, so the cash in the bank is relatively secure. The problem clearly is with the receivables and payables. No company can survive the loss of information related to these types of transactions, so understanding what systems track that data as well as where and how that data are stored, backed up, and archived will be critical to your BC/DR plan.

The legal aspects of data security, in the event of a disaster, are a topic too broad to discuss at length in this book. However, there are important legal considerations when looking at your company's responsibilities for data security and integrity in the

normal course of business as well as in the face of a major or minor business interruption. As you learned in [Chapter 2](#) and the case study presented earlier, “Legal Obligations Regarding Data Security” by Deanna Conn, partner at law firm Quarles & Brady, there are definite legal requirements to be dealt with. Although the legal aspects may not be your responsibility to address, as IT project manager your job is to ensure the project meets all requirements, and some of those requirements may be legal. You should contact your company’s legal counsel and discuss your BC/DR plans with them. You can then follow their recommendations as to how to ensure your BC/DR plans meet minimum legal requirements.

As with other corporate functions, you’ll need to be sure the financial and legal requirements are met within the scope of the BC/DR plan. This may include compliance with financial or legal requirements related to data security and integrity; it may include simply being able to process payroll after a significant business disruption or understanding how you’ll recreate your accounts payable and accounts receivable files, so you can resume the task of collecting money due and paying money owed.

Warehouse/inventory/manufacturing/research

If your company maintains warehouses or facilities with inventory, manufacturing, research, or other similar activities, you’ll need representatives from these areas to answer specific questions related to the BC/DR process. Certainly some of these areas are covered by facilities and security such as access to secure areas or repair of broken or ruptured pipes, for example. However, facilities staff will not be able to tell you which equipment is mission-critical, which research is vital to the ongoing success of the company, or which inventory is most important to the company. These are questions that can be answered only by experts in those areas. Because this may well be the heart of corporate operations, you may need to use a phased approach to BC/DR planning with this group. For example, what would it take to get back up and running in a minimal manner? Next, determine what it would take to get back up and running in a normal manner. These are often two distinct phases that must be planned out. We’ll address this in more detail later in the book.

BEST PRACTICE

Using the “What If” Method

Remember, it’s likely that just about everyone in every corner of your company will view their work as vital to the ongoing success and operations of the company. In reality, there are critical functions and important support functions, but not everything that goes on is actually mission-critical. Unfortunately, you’ll be caught in the middle of the stream. As IT project manager for this BC/DR project, you won’t necessarily have the expertise to say which are and are not critical functions, so you’ll be dependent upon subject matter experts to make that determination. At the same time, they are the very ones with the vested interest in their areas or activities being labeled “critical” or “vital” to ongoing operations. One method to

Continued

BEST PRACTICE—cont'd

sort this out is to ask specific questions rather than vague, values-based questions. Instead of asking, “What’s the most important function here?”, you may need to ask, “What if this system went down? What would you do?,” or “What if this room caught on fire and burned everything to down to the ground, what would you do?” Asking specific scenario-based questions can help you move past egos and agendas to the underlying issues. If you’re extremely lucky, you might actually get a team of people who are willing to clearly identify mission-critical, important, and support activities with the proper perspective.

Purchasing/logistics

Purchasing and logistics may be two distinct functions within your company or they may be handled by one group. They may go through finance or HR, or they may be tied to other departments such as warehouse or research. These functions may even be much more informal than that, such as departmental managers having the authority to purchase supplies as needed. Regardless of how this is handled in your company, you’ll need to ensure that these functions are addressed in your BC/DR plan.

Purchasing and logistics are involved in three distinct ways. First, if your company regularly purchases things like equipment, inventory, and supplies used in the normal course of business, you have to deal with the potential disruption of this function. Second, you may need to arrange for the purchase of services and supplies related to disaster readiness. For example, you may need to contract with a remote data center for backup computing services in the event of a disruption at your primary place of business. In this case, the purchasing folks may get involved in terms of preparing or reviewing contracts, developing requests for information, or requests for quotes, or requests for proposals. Emergency services provided by third-party vendors are typically less expensive and more reliable when contracted for outside the scope of a business disruption and your purchasing or logistics folks may be involved. In addition, there may be other emergency supplies your company chooses to keep on-site or available such as emergency medical supplies, food, water, office supplies, tents, clothing, whatever is appropriate to your company and its unique needs. Third, you’ll need to incorporate emergency methods for purchasing and logistics in the event of a disaster. If you urgently need to purchase three new servers, how will this purchase be authorized and completed if your company is temporarily running out of the CEO’s garage?

Marketing and sales

Marketing and sales activities rely heavily on customer information. Marketing staff typically mine corporate customer data or target market data to determine the best approach for marketing, advertising, and related activities to generate sales for the company. Sales data, whether generated online, by phone, or in a brick-and-mortar setting, are used to determine inventory levels, purchasing requirements, manufacturing lead times, and a whole host of other corporate decisions. What would

happen if your CRM system went down or the building in which the server hosting the CRM application caught fire? What would happen if your marketing and sales staff did not have access to key customer data, sales history, or order history? Marketing and sales are the engines that drive the revenues that make everything else in the company possible, so these deserve a special place in your BC/DR planning. These are the activities that get revenue coming in the door to help your company resume or continue operations after a business disruption. So, while IT systems and physical facilities rank high on the list of priorities in a BC/DR plan, pay special attention to what the marketing and sales folks have to say and be sure you include them in your planning sessions.

Public relations

You may ask “What does public relations have to do with your BC/DR plan?” Though this example is from early 2007, it’s a classic example worth exploring. In February 2007 JetBlue (NASD: JBLU), a low-cost airline, experienced system-wide problems due to bad weather across much of the United States. In some cases, passengers were held on planes away from the gate for up to 8 or 10 hours. Although this was not an IT failure, it was a serious business disruption caused by bad weather. This is exactly the type of scenario a BC/DR plan for an airline should account for. “What would happen if bad weather forced us to cancel or delay flights across the United States?” is the question the airline should have asked and answered prior to a weather event (and they may well have done so). However, they failed to address one of the most basic concerns. Many trapped passengers could not understand why the plane did not just taxi back to a gate and allow passengers to get off, or why portable stairs were not rolled up to the plane on the tarmac to allow passengers to disembark onto buses or other vehicles to take them back to the terminal. This was not done. News channels on TV and radio were quick to broadcast the news of these delays and passengers or those waiting for them alerted the media to these issues and the media frenzy began. When it was all said and done, all JetBlue could do was mop up the damage through its marketing and PR departments. In this case, they announced they were instituting a passenger’s bill of rights and would compensate passengers who were delayed or rerouted. Was it too little, too late? It’s too soon to tell what the long-term impact will be but the stock tumbled from a high of \$16.62 per share on January 16, 2007 to a low of \$12.56 on February 20, 2007, a drop of almost 25%. It continued its downward slide through 2007 reaching a low that year of \$6.00. But the bad news continued. In 2008, with the beginning of the real estate and banking meltdown, many companies’ shares were driving lower. JetBlue bottomed out at \$2.96 in early 2009. Could the company recover from the loss in its market capitalization (price per share x number of outstanding shares)? Could the company recover from the loss in consumer confidence? Today their shares are trading around \$6.00. While you may not be overly concerned with stock prices and valuation, you can clearly see the correlation between a company’s future prospects and a series of communication failures. Interestingly, the company did survive

and one of the ways it did so was to address these major gaps through communications. If you visit their Web site today, you'll see several plans including "Passenger Service Plan" and "Tarmac Delay Plan." They were fortunate, but remember the not-too-cheery statistics on recovering from a major failure. Even though this may not qualify as a major or catastrophic failure, it was a significant event that had an immediate impact on market capitalization and revenues—that's "major" in most people's minds.

Public relations can go a long way in smoothing over the public image of the company and soothing bruised and battered customers. There are numerous examples of companies owning up to a problem immediately, taking steps to stop or resolve a serious problem, and recovering consumer confidence over time. PR can be extremely helpful to your company should you experience a major disaster or outage. Suppose you are an e-commerce company and there is a breach of your Web site and customer names and other personal data are stolen? How will you deal with this? Certainly from an IT perspective, you'll lock the virtual doors and investigate. From a corporate perspective, however, you may need to engage in some serious PR to help manage the company's image.

If you're in a small company, this function may be handled by the owner, the general manager, or the HR staff. However, don't discount the need for these kinds of activities in the face of a business disruption. Even if you don't have a dedicated department or even a dedicated staff member for marketing and PR, you can identify a firm that specializes in PR and perhaps develop a relationship with them prior to a business disruption. At the very least, you may want to identify two or three firms in your area (both in and outside your immediate geographic area) that could be resources for you in the event of a business disruption. Perception impacts how your shareholders, stakeholders, vendors, suppliers, customers, employees, and community view your company. There is an opportunity to shape perception in the immediate aftermath of an event, even if it is to calm frayed nerves or reassure the public that immediate and decisive action is being taken. Don't miss this opportunity because you dismissed the value of PR in a BC/DR plan.

REAL WORLD

Marketing, PR, Spin—What's the Difference?

Many IT people are focused so intently on staying up to date with technology that they are not familiar with the difference between marketing, public relations, and spin. Let's take a brief detour to discuss these. Marketing includes the activities a company undertakes to make consumers aware of the products and services it offers or to create demand for those products and services. For example, Coca Cola airs commercials on television to make consumers aware of the attributes of the beverages it offers for sale in order to increase consumer awareness of the Coca Cola products as well as (hopefully) to increase demand for those products. That's marketing. Public relations or PR is done to announce pertinent corporate news and information to the public, typically through news outlets. For example, a press release may be issued when a company hires a new CEO or when it executes a new union contract or decides to implement a new enterprise software application. Any time the company wants to disseminate information about the company (and not specifically about a product or service), and it may engage in PR activities. PR is generally used to paint the company in a positive light without

Continued

REAL WORLD—cont'd

tying it directly to products or services. Clearly, there is some cross-over. If a company discovers a new process that is used in a new product or service it is offering, there is a mix between marketing and PR activities. “Spin” is a term often used in conjunction with PR, and it has negative connotations. It typically means that the company is putting a positive or company-biased slant on the information. PR activities may attempt to put the most positive face possible on a situation, whereas spin often implies disingenuous or dishonest motives. Unfortunately, some companies that experience a problem attempt to put spin on the situation rather than address it in an honest and forthright manner. To use an analogy, PR would say, “The glass is half full” rather than half empty. The statement is true, but it points the listener to the positive aspects of the situation. Spin, on the other hand, would say “It’s dangerous to fill the glass more than halfway, it could overflow and hurt someone.” It’s not true and they’re trying to make you think anything more than “half full” is bad simply because they can’t provide more than “half full.” Keep this in mind if you’re in charge of developing your crisis communication plan. It’s fine to put your best foot forward—just make sure that foot doesn’t end up in your mouth.

Operations

Depending on the type of business you’re working in, you may or may not have an operations department or just operations aside from all these other elements previously discussed. One notable example is healthcare—all the elements just discussed support clinical operations—the actual care of the patient. So, while this area is listed last, it may be first on your list of priorities. The operations of the company are those that carry out core functions and are generally responsible for revenue generation and operational expenditures.

Clearly, if you have operational activities that have not been included in any of the previous sections, there should be defined roles and responsibilities for these folks. Operations are the heart of every business and if they are in an operational group, they should be the first folks invited to the BC/DR table for planning and project execution.

We’ve delineated the more common functions found in small, medium, and large companies alike, but we know this list is not exhaustive. Take inventory of your company—look at your company’s Web site, intranet, or phone directory to make sure you have all the subject matter expertise from all the departments represented. Also keep in mind that during your project, you may interview these folks, but they may not be a formal part of the project team. In some cases, you might find it more productive to create a list of interview questions to ask each subject matter expert or departmental representative. You can then compile that information and rank system and information criticality based on your own assessment or (more ideally) the assessment of a small subset of subject matter experts. For example, you may gather and collate all this information and bring it to three corporate vice presidents or to the senior management team for discussion. You may want to avoid trying to be the referee among competing interests and you may not be in the best position to make some of those calls. You *are* in the best position to ensure you gather the relevant data from the subject matter experts and present it to those who can and should make those decisions. If it is left to you and your project team to cull through the data and make

those decisions, be sure to present your conclusions and decisions to your project sponsor for formal, written approval before moving forward. This will cover you in the event of a turf war and will hopefully help you avoid any organizational or political gaffes as well.

PROJECT DEFINITION

OK, let's take a moment to regroup. So far in this chapter, we've reviewed the basic process of creating an IT project plan with an eye toward the specifics of business continuity and disaster recovery. We've looked at the key resources and stakeholders you'll need to consider including in your project planning process. While we were looking at those key resources, we also discussed the various business functions and what kinds of questions you might ask to ascertain the criticality of those functions. So, we understand what the project plan should look like and who should be involved.

Now let's turn our attention to the project definition. As we discussed earlier in this chapter, first you'll need to define or understand what the basic project parameters are—the scope, budget, schedule, and quality for this project. In most companies, one or more of these parameters are assigned to you, but not in all cases. Next, you'll need to define the business, functional, and technical requirements. These need to be determined before you can begin your risk assessment, which is the first “work” phase within the BC/DR project plan and is discussed in the following chapter. The business requirements define the scope of the project. Will you be addressing the top three critical systems, all critical systems, or all business systems? The functional requirements tell you what the plan must do or accomplish to meet the business requirements. Do these critical systems need to have full redundancy or do they need to be available within 72 hours of any serious business disruption? The technical requirements tell you how these business and functional requirements will be met. Will you use a backup data center or will you rely on another location of your own company to provide the backup services or redundancy you need? What are the requirements to set up your critical applications in another location? How exactly will your data be backed up, verified, and archived? As you can see, by starting with your business requirements, you can develop functional and then technical requirements.

As IT professionals, the temptation is strong to begin with the technical requirements, but you clearly could miss some critical data with that “bottom-up” approach. That said, you no doubt already have some technical solutions in place, and these should be incorporated into your planning. For example, if you already have a solution in place for backing up and archiving data in a secure manner (i.e., data are secure while being backed up and backup itself is off-site in a secure location), then this should be rolled into your BC/DR plan. So, if you have the backup scenario figured out, you can then look at your business requirements and ensure your backup plan adequately addresses backing up the critical business applications defined in the

business requirements. You can also look at your backup process in light of your functional requirements to determine whether your backups meet those specifications. For example, perhaps you realize through developing functional requirements that the period between backups is too long. Perhaps trying to recover from an outage that occurs the day before a scheduled weekly backup would be too difficult or time consuming, or even impossible if it was due to a severe business disruption. You might conclude that it would be better to do a twice per week backup to not only meet your current business needs but to provide the kind of business continuity and disaster recovery capability called out in your business and functional requirements. As mentioned earlier, you may choose to have different subsets of your project team for different phases of the project. You may want to get all the major business units together to develop the business requirements. You may want to have subject matter experts from each of the business areas help develop the functional requirements, and you may then have just IT staff work on the technical requirements.

One last note here before we look at the details of business, functional, and technical requirements. You may find that it makes more sense for you to put together your BC/DR planning team and perform the first major task, the risk assessment. The risk assessment phase, discussed in the next chapter, will help you look at the potential risks to your systems and to your business. You might choose to create several deliverables from your risk assessment phase that help you develop or refine your project requirements. You may decide that it makes sense to create general business and functional requirements, so you can ensure your project falls within required parameters. That is, you might choose to create high-level business and functional requirements that fit into your budget, your timeline, or your overall objective for the scope of the project. You might then go into the risk assessment phase and come back to your requirements with more specific information. If you use this approach, it is more likely that your business and functional requirements will define a project scope (budget and schedule) that meet the goals or objectives you've been handed. From there, you can continue to refine. If you go into the risk assessment phase without a general understanding of the business and functional requirements, there's a good chance your scope is going to balloon quickly. So, keep in mind that both methods (define requirements then assess risk *or* assess risk to define requirements) have their own set of benefits, risks, and limitations. Be aware of these as you make your decisions and remember that the key is to use a process that works best for your business.

BUSINESS REQUIREMENTS

Business requirements are the first step in developing BC/DR project requirements because you must first understand the critical areas of your business. What questions should you ask to ascertain which are the critical business functions? As you know, if you ask users what the most important systems are, they'll give you a list a mile long. Rather than ask that type of question, many experts advise using scenario-based

questions to help focus attention and elicit useful information. This may take a bit longer in the short-term but will save you time and headaches later. Keep in mind, too, that the first major deliverable for your BC/DR plan is likely to be the risk assessment, which may lead you back to modifying your business, functional, and/or technical requirements. Each iteration should move more quickly and inject less change into the project than prior iterations. So, if you create your business requirements and then do your risk assessment, you may find the priorities for the business requirements change or that a critical system was omitted during the first round. This is a normal part of project planning. However, if you find that each iteration is injecting more change and more uncertainty or more confusion to the process, you need to step back and assess what's happening. It might be that the project is beginning to manage you (rather than you managing the project), or it could be some key assumptions were incorrect or that your organization is in the midst of a significant change. Be aware that a project plan that feels like shifting sand beneath your feet is in danger of getting out of control and failing. Let's look at some questions you can use to elicit the type of business information you need to create a useable BC/DR plan, understanding that some of the answers to these questions may change slightly over time. You can tailor these questions to the specifics of your organization, but this should give you a good start.

- What would happen if the server room caught on fire and the fire suppression system activated?
- What would happen if our power to the data center was cut and unavailable for 4 hours? 4 days?
- What would happen if our cooling system in the data center failed and replacement parts were not available for a month?
- What would happen if there was a fire in the building and we had to evacuate the building immediately? What would happen if we were not able to reenter the building for 3 weeks or 3 months?
- What would happen if a security breach was discovered and our customer database was compromised?
- What would happen if we discovered that our Web server had been hacked?
- What would happen if an earthquake (hurricane, tornado, flood) destroyed this building and many of our employees' homes in this area?
- What would happen if a major snow storm made it impossible for employees to get to work for a week or two?
- What would happen if a chemical spill from a nearby plant or railroad forced us to evacuate this building for a week? A month? 6 months?
- What would happen if electricity to this site were cut or unavailable for half a day, 1 day, 1 week, 1 month?
- What would happen if our high-speed connection to the Internet were to go out for half a day, 1 day, 1 week, 1 month?
- What would happen if a bomb went off in this building and we could not get back into it, ever?

- What would we do if major transportation routes (air, rail, road, sea) were shut down or disrupted?
- What would we do if key people were killed, injured, or missing?

As you can see, these questions elicit information because they create “what if” scenarios to which team planners have to respond. It gets people thinking in very concrete terms and you, as project manager, can help step them through this process. Again, since there may be aspects to the BC/DR planning process that do not fall under your direction or management, you may not be responsible for managing this process. However, whether you’re heading this up or simply participating as part of the team, you can bring your skills and expertise to the team process and help step people through this process. By envisioning “what would happen if,” you can help craft a realistic view of what the next steps would be. Immediately, people will begin thinking about what they would do without a server or without an application or without the resources at their desks—and this helps you begin to determine what the technological priorities and needs are for your BC/DR plan. Also keep in mind that fire has historically been the number one “disaster” to hit businesses, so start with the smaller, more localized potential problems and expand from there. It does no good to be fully prepared for a hurricane if you don’t have a plan for the common problems business face like power and cooling failures.

FUNCTIONAL REQUIREMENTS

Once the business requirements are developed, you can begin to craft the functional requirements. Functional requirements state what is needed, not necessarily the technology that will fulfill that need. For example, the sales department might say, “We’ll need a way to contact our customers. If the Internet connection and e-mail are down, will we have phones? If we have phones, we can call customers but how will we get their phone numbers?” The functional requirement might be to always have access to the most current customer contact information. For example, some small businesses might keep a printed copy of their customer list at their attorney’s office, which has branches in four cities other than the one in which you’re located. Although this might seem extremely low-tech, the only requirement is that the solution meets the needs of the organization. This can include the need to have low-tech, low-cost solutions available to the most common business disruption scenarios. Only you and your company can determine what’s most appropriate. The functional requirements describe what functions or features must be available. When you delve into the technical requirements, you can define the technological counterparts to the functional requirements.

When asking and answering the questions listed earlier in the business requirements section, listen to the answers carefully. Chances are good the functional requirements will start forming there. Your planning team will say, for example, “If our servers are down, we’d need a way to contact our customers.” This is a

business and a functional requirement. The business requirement is that customer contact is a vital aspect of the business; the functional requirement is that there needs to be some method for accessing current customer contact information in the event of a server outage. If the team ponders the question, “What if our entire server room caught on fire and was destroyed? What would you do without the tools you currently use to do your job?”, you’re likely to begin to understand that they might be able to get by without the billing system as long as they had a printout of the current status of accounts payable and accounts receivable, but they would not be able to continue business operations in the near-term at all without the main application server being up. That’s good information. You now know that the main application server functions are critical, and the billing system functions are important but not critical.

As you work through these scenarios, you may want to create a method of ranking these requirements so that you can gain agreement with the team of subject matter experts as to the relative importance of these requirements. You’ll have to listen carefully if you’re in charge of this process because people may describe one priority and then assert another. Using the billing system example, when you ask about what they would do in a particular situation, they may indicate that they could get by without the billing system because if they had current data, they could keep track manually; even though that might be a major task, it would be doable. However, if you then move to a ranking system and indicate the main application server function would be mission-critical but the billing system would not be, you might get some disagreement. You may need to manage the situation by helping people understand the point of the ranking system—which is to determine what you’d need within hours of a disruption versus what you’d need within days or weeks of a disruption. **Table 3.1** provides a few suggestions for ranking systems that you might find helpful, but feel free to create whatever works best for your organization that will lead to clarity and agreement.

The Sample One ranking system is fairly self-explanatory. The ranking is related to how critical a system is to the ongoing company operations. The Sample Two system uses commonly used word to describe priorities. Sample Three uses the color system, similar to the threat level system the U.S. Department of Homeland Security uses. Sample Four is obviously a simple priority ranking system using numbers. Sample Five is an example of a customized list you might create to indicate that anything related to revenue generation is the most important priority; anything related to

Table 3.1 Sample Ranking Systems

Sample One	Sample Two	Sample Three	Sample Four	Sample Five
Mission-Critical	Very High	Red	One	Revenue
Critical	High	Orange	Two	Support
Important	Normal	Yellow	Three	Maintenance
Support	Low	Green	Four	Other

supporting business operations and revenue is second. Tasks that maintain business operations come in third and the “Other” category is the catch-all. You can create any ranking system that is appropriate for your organization but spend some time defining the categories you choose to use so that you will know where the boundaries are for each category. This will help everyone have a shared understanding of the categories and will help everyone to consistently rate and rank priorities as a team.

TECHNICAL REQUIREMENTS

The technical requirements define how the business and functional requirements will be met. As the IT professional on the team, you will have the unique vantage point of understanding how these current business and functional requirements currently are being met with technology. As stated earlier, it’s entirely possible that some or many of your business and functional requirements for BC/DR planning are being met with current technology strategies. As you review the business and functional requirements, you can begin assessing how close or far your technology is from the desired state. In most cases, what you’ll find is that your technology solutions in place meet some but not all of your BC/DR requirements. This is essentially a gap analysis that tells you where your technology meets business and technology requirements for BC/DR and where it partially or completely misses the mark. As you can see from [Figure 3.5](#), you can graphically represent the key elements to help the team understand how near or far it is from the desired state (at a conceptual level) and then begin the process of prioritizing. In some cases, you first may choose to remediate small gaps so there is 100% confidence in that element rather than tackle a larger gap. In other cases, you may decide that the larger gaps are more critical and should be addressed first. The approach you take will depend entirely on your company, its current state of readiness, and many other internal factors. There is no right or wrong approach as long as you take action (once the plan is in place) to work in a thoughtful and incremental manner.

Technical requirements are important for reasons stated earlier, but they are also important because these will form the foundation of specific tasks related to defining

	In place	In progress	Planning	Future
Server high availability		█		
Local, scheduled backups	█	█		
Application data matrix (Tier 1, 2, n)			█	
Secure, off-site backups	█	█		
Emergency IT response team				█

FIGURE 3.5

Graphically representing current state.

the required technological solutions so you can go out to bid for these products or services; so you know what would need to be replaced; so you know what resources you'll need at a remote/off-site data center, and so on. When it's all said and done, you should have a complete list at the end that defines server types, server capabilities (number of processors, speed, RAM, disk space, network connections, etc.), applications, application requirements, application configuration needs, user configuration needs, and more. If this is currently part of your standard IT operations, then you may have all the configuration and technical needs documented already. If this is the case, you'll need to make sure everything is up to date and accounts for any new or changed technology implementations (current or upcoming). Most importantly, you'll have to determine where and in what format these data should be stored so that they are available to you in the event the server room, building, or location is destroyed or inaccessible.

As you can see, your BC/DR planning process ideally will help you make better use of existing technological solutions and help you implement new ones to meet your needs. You may discover through this process that one or more of your existing solutions is a perfect fit for your BC/DR needs. You may discover that some existing solutions are only being partially utilized or that they can be utilized in new and different ways. Finally, you may discover large gaps in your BC/DR technology readiness, and this should give you the information (and ideally, the organizational support) you need to implement the right solutions for your company.

As you can see, developing the business, functional, and technical requirements is all inter-related and none happens in a vacuum. As you develop your BC/DR plans, you should continually assess your current practices, processes and capabilities. In some cases, you'll find that what's already in place will work perfectly with your "best case" BC/DR plans. In other cases, you'll find that you want to modify existing processes and methods slightly to address your optimal BC/DR requirements. In still other cases, you'll find areas of the business (and technology) that is critical to ongoing operations that are completely exposed. This is the good news—the BC/DR planning process should help you assess these areas from the top down (business, functional, technical) and from the bottom-up (technical) and determine the status of your current business operations as it related to BC/DR. From a known state, you can make intelligent choices about how much work you need to do to provide the level of readiness required for your business.

BUSINESS CONTINUITY AND DISASTER RECOVERY PROJECT PLAN

Those of you familiar with project planning know that the project plan itself will be comprised of several major elements. The first element includes the various project definitions, which we've covered at length in this chapter. The project parameters (scope, budget, schedule, quality) should be defined; the project requirements must be delineated, so they fall within the project's parameters. Once the project definition

stage is complete, you create your WBS. As you know, the WBS defines all the major and minor tasks of the project that, when taken as a whole, describe the total amount of work in the project, or the project scope. The WBS we're using as the framework for this book and for our BC/DR plan is as follows:

1. Project Definition
2. Risk Assessment
3. Business Impact Analysis
4. Risk Mitigation Strategies
5. Plan Development
6. Emergency Preparation
7. Training, Testing, Auditing
8. Plan Maintenance

We introduced this visual aid at the beginning of the book and again at the outset of this chapter. We'll continue to reference our progress in this book according to this framework, as shown in [Figure 3.6](#). You'll see this figure throughout the book to provide a visual reference for where we are and what's coming up next.

Project definition, risk assessment

We've discussed project definition at length in this chapter, and we've also linked it to the risk assessment to be discussed in detail in [Chapter 4](#). The risk assessment is the phase in which all potential risks to the business are listed and then evaluated both for likelihood of occurrence and impact in the event of an occurrence. As a company and as a project team, you'll need to create a cut-off point so that risks that fall below the line are not addressed. This is one way the scope (and as a result, the budget and schedule) of the project is managed. We'll look at how to perform this phase of project work in the next chapter.

Business impact analysis

Business impact analysis, covered in detail in [Chapter 5](#), looks at how the business would be impacted if the major risks were to occur. In order to make this process productive, it occurs after the risk assessment so that only the risks that fall above the cutoff point, or above the risk line, are addressed. This, too, contributes to your ability to manage the scope, budget, and schedule of the project.



FIGURE 3.6

Business continuity and disaster recovery project plan progress.

Risk mitigation strategies

Tying the risks with the business impact analysis together yields your BC/DR priorities. Clearly, you want to address only risks that have a high likelihood of occurrence and a medium to high impact should they occur. If a risk has a low risk of occurrence and it would have a low impact on your business, you may choose to not plan for that particular risk. Every company has to make that call individually—there is no single right answer, though there are real-world limitations to the value of planning too far down the risk/impact ladder. It probably isn't of any benefit to spend 2 weeks and 300 staff hours planning for something that probably won't happen, and if it did happen, would impact only 16 of your company's 1400 employees and none of your company's top 100 clients. In [Chapter 6](#), we'll look at how to develop strategies to manage the risk including ideas on how to reduce, avoid, and transfer risk.

Plan development

Once you've assessed your risk and the impact of those risks, and developed strategies for mitigating those risks, you'll need to start working on putting those strategies into action. That means developing a set of tasks that will deliver the required results. Plan development will include creating the project plan's WBS tasks related to actual BC/DR activities (as opposed to plan activities) as well as all owners, deliverables, and success criteria. We'll look at this in [Chapter 7](#) in detail.

Emergency preparation

Part of every BC/DR project plan should be the actual emergency preparations that a company should undertake, and we'll look at this in detail in [Chapter 8](#). If your job is limited to IT-related functions, you might find that your role here is limited. Emergency preparations include the specific steps to take in the immediate aftermath of a disaster and the definition of when business continuity activities should begin. Though this might be outside the scope of your responsibilities or authority, we'll cover the basics so you can be a knowledgeable contributor to the overall BC/DR planning process. If your job as the project manager for this BC/DR project includes all aspects of BC/DR planning, then this section will help you rally the resources you need to create an effective emergency response plan.

Training, testing, auditing

[Chapter 9](#) covers the tasks you'll need to include in your BC/DR project plan related to training staff for emergency response and for implementing the BC/DR plan should that be necessary. Testing is something all IT professionals are familiar with, and this takes on significance when you look at testing from the BC/DR perspective. Finally, you'll need to audit and assess strategies after you've trained staff and tested the plan. This is part of the iterative process you'll use throughout the project management process. It is here where you discover key gaps or broken processes; it is

here you have the opportunity to fix these gaps, errors, and omissions so that your BC/DR plan is as solid as possible within the given constraints of the organization.

Plan maintenance

As we've discussed, an out-of-date plan is sometimes worse than no plan at all because it allows staff across the organization to make assumptions about BC/DR readiness that may simply be wrong. If your plan was crafted several years ago, there's a high likelihood it is no longer current. If you have a plan that you believe may be relatively current, you can short-track some of your planning processes by reviewing the plan against the steps delineated throughout this book. For example, you may choose to perform the risk assessment and business impact analysis with fresh eyes then compare the results to the plan you have. If there are significant gaps or disconnects, you may choose to scrap the old plan altogether or modify, update, and test the existing plan. The choice is yours. Whichever path you choose, whether you have an existing plan or are creating one for the first time, you should build in tasks that allow the plan to be periodically reviewed and updated. In [Chapter 10](#), we'll discuss some of the methods companies use to do this so that you can create a maintenance plan for your BC/DR plan that makes sense for the way you do business today and in the future.

REAL WORLD

Perfect World vs. Reality

Throughout this book, we'll discuss perfect-world scenarios as well as real-world realities. Project planning rarely follows the prescribed methods, timelines, and order we've discussed. It's useful to understand best practices and preferred methods so that you can strive to mirror those in your work. However, it's highly likely that there are one or more mitigating factors that come into play with your project planning process. To assume that things will follow the defined order and work out perfectly is to set yourself up for disappointment and failure. The goal should be to strive to follow the predefined processes and steps to the greatest degree possible and to diverge from those only with intent and conscious choice. Anytime you find yourself diverging from best practices, make sure you ask yourself if this is by accident, by choice, or by necessity. That should help keep your project on track while still giving you the flexibility to deal with the specifics of your organization. As long as you're aware that you're taking a side road or alternate path, you can still arrive at the same destination. It's when you close your eyes and hit the gas pedal that you're likely to get yourself (and your project) into trouble.

SUMMARY

Planning your BC/DR project is similar to other IT projects you've defined, developed, and managed in the past with the possible exception of the reach of the project. A BC/DR plan reaches into every corner of your organization and tests your assumptions about what you do, how you do it, and how important those things are to the viability of the company in the short- and long-term.

We looked at the elements that drive success in any IT project and looked at the specific factors that you'll need in order for your BC/DR project to be a success. Clearly, having executive support means that those further down the organizational ladder will be compelled or required to participate and to give this project the appropriate priority in the corporate scheme. Other success factors discussed include involving the right people early in the process, having an experienced project manager, clearly defining project objectives, requirements, and scope, as well as setting a shorter schedule with multiple milestones and using a well-defined project management process.

The project plan components are standard IT project plan components that should be incorporated into your planning process. We looked at the elements including project definition, forming the project team, organizing the project, planning the project, implementing the project, tracking project progress, and closing out the project. Although there should have been no surprises here, we did cover some of the more important elements in each of these categories related specifically to BC/DR project plans.

A business continuity and disaster recovery project plan requires that key contributors throughout the organization participate with you to identify the bottom-line needs of the organization. As an IT professional, there's simply no way you can know all you need to know about how business operates on a day-to-day basis to create an effective BC/DR plan without key contributors from your various business units or functional groups. Including people from facilities, accounting, legal, Human Resources, engineering, and others will be crucial to success, and with the information discussed in this chapter, you should now have a better idea of who needs to participate and what you can expect them to contribute.

Another important aspect of the BC/DR project plan is the definition of the project including the business, functional, and technical requirements. As you learned, this is likely to be an area that requires additional detail or refinement. Most companies find that it makes the most sense to create initial high-level definitions and then come back after the risk assessment and business impact analysis are complete to refine those definitions. The business requirements define what is needed to operate the business in the aftermath of a disaster (disaster recovery) and in the longer term (business continuity). The functional requirements delineate what is needed by way of functionality so that the business can get up and running as quickly as possible should a business disruption occur. Finally, the technical requirements, with which you may be best acquainted, determine exactly what the technical specifications are that will meet the requisite functional and business requirements.

Lastly, the BC/DR project plan elements are the elements specific to the BC/DR activities. We looked at the framework that will be used throughout this book as an example of one potential approach to the WBS for the project. This includes risk assessment; business impact analysis; risk mitigation strategy development; plan development; emergency preparedness; training, testing, and auditing; and plan maintenance. Each area will be discussed at length in the upcoming chapters.

KEY CONCEPTS

Elements of project success

- There are numerous well-known, time-tested success factors that contribute to the likelihood that your IT project will be a success. Executive support is always at or near the top of success factors for an IT project.
- User involvement is key to success because any IT project that does not ultimately meet user needs will likely be seen as a failure. User involvement must be well managed to ensure it remains focused and productive.
- An experienced project manager is another success factor, which makes sense.
- Anyone who's had to manage a project with all the challenges that come with it is likely to be more successful in subsequent projects.
- Clearly defined project parameters (scope, budget, schedule, quality) as well as project definition and requirements are also key to success. The more detail you develop to describe what you're trying to accomplish and how you'll accomplish it, the more likely you are to hit the target.
- Shorter project schedules contribute to project success. In some cases, it might make sense to break down various parts of your project into sub-projects.
- Projects with more milestones also tend to be more successful because milestones help keep you focused on deliverables. Milestones are checkpoints, and the more often you check your progress against plan, the more likely you are to be able to make small changes early that help you stay on track.
- Having well-defined project processes also contribute to project success for fairly obvious reasons. If the team knows what to expect and how to go about accomplishing and reporting project progress, the project has a better chance of moving forward. If you get bogged down in convoluted, illogical, or unnecessary project processes, your team will find ways to circumvent the processes or fail to complete project deliverables on time (or at all).

Project plan components

- The BC/DR planning process follows standard project management steps. The components used are ones you are likely familiar with, especially if you are an experienced project manager.
- Project definition serves to define what work needs to be accomplished. The definition includes the project parameters (scope, budget, schedule, quality); project objectives; and the business, functional, and technical requirements.
- Forming the project team is unique in a BC/DR project plan because the people that need to be involved with the project will likely come from every corner of your organization. Involving the right people at the right time will boost the chances of success for your BC/DR project.

- Project organization includes defining how the project will be run from team meetings to task status updates to overall project progress reporting. It also includes key processes such as change management and escalations. Having a well-organized project improves the project's chance for success by providing standardized, easy-to-use processes for the team.
- Project planning includes creating a WBS that, when complete, defines the scope of the project and meets the project's requirements and objectives. A well-crafted WBS includes tasks, dependencies, timelines, milestones, and success criteria, among other things.
- Project implementation is where the “rubber meets the road” and is where all the planning efforts take effect. Once the project is underway, change must be actively managed and project progress must be actively tracked and managed.
- Project tracking consists of all metrics you, your team, and your project sponsor have agreed to with regard to project progress. This may mean tracking time, costs, labor hours, percent complete, and other metrics that help bring the project to a successful conclusion.
- Project close out includes all tasks required to bring the project to an end and shut things down methodically. It typically includes reviewing change requests, project deliverables, and lessons learned.

Key contributors and responsibilities

- Key contributors in a BC/DR project plan may differ from key contributors you've worked with in the past.
- BC/DR activities require the coordinated efforts of key people throughout the company from facilities management to security to Human Resources to finance and accounting.
- Identifying the key contributors to your plan and what areas they will be responsible for in the BC/DR planning process will help ensure you have the people you need on the team to create a solid, workable BC/DR plan.

Project definition

- Project parameters define the scope, budget, schedule, and quality of the project. There is an interrelationship among these parameters. If you choose to increase the scope, you must also increase the schedule or budget. If you reduce the budget, you must increase the schedule, reduce the quality, and/or reduce the scope of the project.
- Understanding the relative flexibility of the project parameters helps you make decisions in line with the business requirements. For example, if budget is fixed, it is least flexible. Therefore, you will have to modify your schedule, scope, or quality if things change later on.

- The business requirements for the project must be understood before the project can get underway. Business requirements may be modified or revised after the risk assessment and business impact analysis is completed.
- Functional requirements for the project indicate what functions or abilities must be present in order to continue business operations after a major (or minor) business disruption. The functional requirements indicate what must be present or available, not how those functions will be made available.
- Functional requirements may be revised or modified after the risk assessment and business impact analysis phases of the project work have been completed. Information may come to light that suggests (or requires) your functional requirements be modified to better suit the company's needs.
- Technical requirements can be established only after the business and functional requirements have been developed. However, it is also true that your organization already has many technical solutions in place (or in progress) related to BC/DR.
- Your current (or in progress) technical capabilities should be taken into consideration as you assess business and functional requirements. There will be areas of complete alignment, areas that overlap, and areas where you discover large gaps.
- The BC/DR planning process will help you utilize existing solutions more effectively as well as address any gaps or future needs.

Business continuity and disaster recovery plan

- The BC/DR plan will follow a standard project management framework and rely upon standard project management processes.
- The BC/DR plan, at this highest level, should have these sections (or work phases): definition, planning, and organizing; risk assessment; business impact analysis; risk mitigation strategy development; plan development, emergency preparedness; testing, training, and auditing; and plan maintenance.
- Risk assessment and business impact analysis may induce changes to the business, functional, or technical requirements for the project.
- The plan development should include the development of the WBS including tasks, dependencies, task owners, success criteria, and milestones.

References

Curtis J. The importance of a great project manager., <http://quotient.net/blog/2012/6/25/the-importance-of-a-great-project-manager/>; 2012 [Retrieved May 26, 2013], from Quotient—Integrated Solutions.

Snedaker S. *How to cheat at IT project management*. 1st ed. Rockland, MA: Syngress Publishing, Inc.; 2005.

This page intentionally left blank

Business Continuity and Disaster Recovery in Energy/Utilities

IN THIS CHAPTER

- Introduction
- Real-life BC/DR challenges at ABC Energy Corporation
- Practical BC/DR solutions devised by ABC IS Department staff
- Benefits of integrating BC/DR planning activities into IT Governance
- Risk mitigation and recovery procedure best practices
- BC/DR testing best practices
- Summary
- Key concepts

INTRODUCTION

This chapter examines the challenges and accomplishments of an electrical utility's disaster recovery and business continuity planning efforts from 2005 to 2012. It is meant to serve as a real-world example of how the IT employees of a mid-sized company have responded to evolving business continuity threats and actual IT disaster recovery incidents. It is important to note that this chapter does not attempt to present a perfect solution or a solution which necessarily applies uniformly to all mid-size companies or all utility or critical infrastructure providers. However, we do believe there are some important lessons learned which can apply to any mid- or large-sized company. We thought it would be beneficial to showcase real-world obstacles to successful DR/BC planning and how they shaped both failures and successes at an actual company. Highlighted in this chapter are small things IT staff can do now to move the dial in a big way, in terms of business continuity and disaster recovery (BC/DR) process improvement. Specifically, this chapter focuses on these key areas:

- Integrating BC/DR activities into your IT Governance or IT project processes
- Improving BC/DR risk mitigation and recovery strategies
- Improving BC/DR testing

For the purposes of this chapter, the electric utility in question, herein referred to as ABC Energy (or ABC), shall remain anonymous in order to allow for a full accounting of the facts and, therefore, a more relatable chapter. ABC Energy, for the purposes of this chapter, is a purely fictional name and is not related to any organization or firm that shares the same name.

It is first helpful to understand that ABC is, in fact, a regulated, publicly traded electric and gas utility that generates over \$1B in revenue each year, employs close to 2000 employees, and serves geographically dispersed communities in one part of the United States. This chapter begins with a very embarrassing truth facing most companies. Like many companies, ABC, a company which is very adept at restoration of critical utility infrastructure, has never established, maintained, or tested a formal companywide BC/DR project or plan which accounts for all of its critical business processes and IT assets. However, many critical elements of successful BC/DR planning have interwoven themselves into its operations at the departmental level over the years, and the company's Risk Management group has begun coordinating companywide discussions to develop such a process and plan in the face of increasing threats to its IT assets.

There are many reasons BC/DR has pushed its way to the forefront of business operations in recent years. First, IT security threats are much greater today than they ever were in the past, and like most companies, ABC has had to deal with reportable IT security incidents that have resulted in limited loss of operations and limited financial damage. Second, ABC, again like most companies, has seen a steady increase in demand for IT services and has experienced a growing number of isolated disasters, both natural and human caused, where recovery of otherwise obscure IT assets and data was crucial to the continuity of different critical business processes. Third, an increasing set of government regulations now stipulate certain BC/DR planning activities must occur if the company does not want to incur large fines and a tarnished reputation; in some operational areas of the company, ABC Energy can incur up to \$1M in fines per day per violation.

It is important to note that information presented in this chapter is the direct result of IT staff, with limited resources, working over the better part of a decade to make incremental improvements when and where they could. They didn't attempt to tackle everything at once, nor did they have perfect processes to work from at the very beginning. They did, however, continually look for opportunities to make substantive improvements when new challenges or obstacles arose. By looking at every obstacle as an opportunity for process improvement, they fundamentally changed their way of doing business for the better. Whether they were recovering from unplanned operational outages and holding postmortem meetings with clients or sitting down with clients to discuss new IT initiatives, they took the opportunity to review, revise, and improve BC/DR planning along the way. Many of the BC/DR improvements they made were, in fact, created and implemented by mid- and low-level IT employees, working in tandem with different IS teams, as part of their daily operational tasks. They recognized, early on, that BC/DR planning is an ongoing process, and they began incorporating year-over-year BC/DR improvements into annual staff goals.

In the early days, they had to change their thinking in order to improve. Instead of wringing their hands or pointing the finger at some other part of the company for not leading the charge, they began to methodically tackle BC/DR by asking relevant questions and incorporating process improvement techniques in daily operational

activities. This chapter demonstrates how ABC first got a better handle on BC/DR requirements, then recovery and risk mitigation strategies, and then testing, in that order. This order is important for several reasons. First, it is impossible to develop effective recovery and risk mitigation strategies without first understanding business requirements. If you simply assume all IT assets are equally important in a disaster, you will find you don't have the time or money to do what is necessary. Moreover, you don't know the best place to start or what to tackle next unless you get a better picture of the requirements. Although the IT staff, attempting to do the best they could, had implemented some recovery and risk mitigation tools and processes, it didn't know what it should recover first, what the relative recovery times were for most applications, or what exact pieces needed to be in place for recovery of individual applications should a disaster strike. Second, the IT staff realized it was short-sighted to test recovery or risk mitigation strategies if you don't first understand whether these strategies match expectations. Therefore, the only right way is to start with requirements. But, how can IT staff force the business to define BC/DR requirements if no comprehensive BC/DR project exists? Let's find out.

INTEGRATING BC/DR REQUIREMENTS INTO IT GOVERNANCE

Although ABC has not yet completed a companywide risk assessment and business impact analysis (BIA), inclusive of all of its critical IT assets, it has developed several related processes and plans, within the IS Department, which are a means to this end. In addition, some business areas do have their own written BC/DR plans. However, many, if not most, do not fully account for IT asset recovery in such plans. Of all the initiatives undertaken by the company which have positively contributed to BC/DR planning efforts, establishing a mature IT Governance process was probably the most important.

IT Governance began at ABC before the majority of government regulations affecting IT Security and BC/DR were even put into effect. In essence, successful IT Governance ensures that formal processes to prevent wasteful spending and mitigate risk are in place when the business wants to buy new software, upgrade existing software or otherwise expand its IT services. ABC's IT Governance process is not 100% inclusive of every functional area, but it has matured over many years and has brought more and more IT initiatives across the business under its guidance. At its core, IT Governance provides a set of rules for discretionary funding of IT projects. If the business needs funding for IT projects, then it must go through the Governance process to obtain executive approval and the required funding. However, not all parts of the business must secure discretionary IT funding from the IT Governance process. Many operational areas are still immune to IT Governance, and they are able to place IT dollars into their annual budgets outside the IT Governance process. This, too, has changed over the years, as more scrutiny of IT dollars in department budgets has surfaced, and expanding government regulations have created more centralized IT security policies and procedures around IT assets and processes.

BC/DR requirements definition

So, how does IT Governance help BC/DR planning? For one, it ensures both formal IT project requirements definition and release processes are in place. These processes have been leveraged by the IT staff at ABC in order to improve BC/DR planning activities. For example, many business questions which are typically answered by a formal companywide Risk Assessment and BIA process are able to be asked during the early requirements gathering phase of each new IT project. IT project stakeholders are asked to document answers to these questions within a formal, signed Requirements document, before IT resources are provisioned. Based on completeness of the Requirements document, IT staff may ask for a meeting to engage with the vendor and business operational staff to ask follow-up questions and document responses. *The important lesson here is that any IT shop can begin to incorporate risk assessment and BIA activities into existing operations, even if a formal BC/DR project hasn't been approved yet.* By piggy-backing on existing IT project activities at your own company, you can easily begin to gather relevant data that will help you improve your company's overall BC/DR intelligence. It doesn't have to be an all or nothing approach, as ABC has learned. You can identify narrowly scoped, modest improvements within your control and begin to implement these improvements immediately.

The IT Requirements document at ABC records relevant BC/DR data (among many other technical and functional requirements), such as:

- Vendor information, including version, sales, and support contact information;
- Data conservators (i.e., business users who “own” the underlying business data and are responsible for approving access);
- All production, development, test, or QA environments;
- IT interfaces and/or integration points (i.e., uplevel and downlevel IT dependencies);
- Any business process inputs and outputs;
- Times of normal and peak use;
- Number of users by geographic location;
- Periodic outage windows for planned maintenance (such as security patching and operating system reboots);
- Monitoring and alerting requirements for unplanned outages (Who should be notified via e-mail or SMS, and during what times?);
- Recovery time objective (RTO);
- Recovery point objective (RPO);
- Productivity losses (by hour, day, week, and month) due to unavailability of the IT application or service;
- Nonproductivity financial losses (by hour, day, week, and month) due to unavailability of the IT application or service;
- Business continuity processes should, the IT application or service, be indefinitely unavailable (e.g., What would you do if your application was unavailable indefinitely for any reason?); and
- Safety, regulatory, security, financial, or other operational constraints or implications.

These BC/DR functional requirements are fundamentally critical to BC/DR planning activities at ABC, and gathering these requirements is interwoven into the early technical requirements phase of an IT project before initial design and cost estimation are completed. All levels of the IS Department, from the Project Management Office (PMO) to the Business Analysts to the IT Operations staff, are encouraged to sit with clients and have face-to-face discussions to help them understand the impact BC/DR requirements has on their business continuity. This conversation averages about an hour or so per application and often leads to a greater mutual understanding of capabilities between IT and the business.

In some instances, the Requirements document may group two or more related applications (e.g., Automatic Call Distribution and Integrated Voice Response for the Call Center) as a single service, even though separate software and data sets are involved. In this case, one Requirements document is all that is needed and the questions in the Requirements document simply delineate the different applications and responses by application, even though the business may consider this a single IT “service” from a BC/DR perspective (i.e., the two applications are meant to work together).

In one face-to-face meeting with the Payroll Department, who was participating in an HR/Payroll application upgrade, Payroll staff told IS staff that if the application was unavailable in a disaster, they could simply call the bank and ask them to repeat the same direct deposits that had occurred in the previous payroll cycle. For the small number that got paper checks, they would simply ask the bank to cut checks, if need be, based on prior paystubs or bank records held by those employees. In essence, they did not need immediate access to internal IT systems in order to continue payroll in the event of a disaster. This is the type of information that is critical to service level and BC/DR planning, and it only came to light fully when IS staff sat down with the business when they wanted to do a new IT project.

The Requirements document, inclusive of the BC/DR information above, is required to be signed by all impacted company Managers/Directors, both from the business area and the IS Department, before an IT Project can proceed beyond the planning and design phase to the approval and funding phase. Regardless of whether every IT initiative comes to ABC's IS staff with a completed Requirements document in hand, IT Operations and IT Security staff require a completed, signed Requirements document before any infrastructure is provisioned or access requests handled. In all cases, the IT Operations and IT Security groups request a seat at the table when business requirements or potential solutions are being discussed in the early stages of an IT Project. Even if the business has already purchased the software and/or scheduled an outside vendor, these groups insist on review and acceptance of BC/DR requirements prior to fulfilling any request for resources (human or technology). In this manner, they act as the BC/DR requirements police and can direct traffic in order to head off IT projects getting released without proper BC/DR requirements definition up front.

IT service level definition

Based on the responses recorded in the Requirements document, each IT application or service is slotted into a formal, tiered corporate IT service level matrix. Tier 1

applications have the shortest RTO and the highest availability goals, whereas Tier 4 applications have the longest RTO and lowest availability goals. All applications which don't require Tier 4 service level objectives default to the bottom tier, Tier 5, and are not enumerated specifically in the corporate IT service level matrix. The matrix simply lists Tier 5 applications as any application not specifically mentioned as a Tier 1-4 application. Therefore, the service level matrix is only updated when a Tier 1-4 application goes through its release phase to production or is decommissioned. Of the roughly 200 applications housed or dependent on data center resources, the vast majority of applications are slotted as Tier 5 applications with the largest RTO and lowest availability goals. Availability is measured as the percentage of cumulative uptime in any given calendar year, minus planned maintenance windows, whereas RTO is measured as the maximum time required to restore the IT application/service and associated data should an unplanned outage occur for any reason. RTO is largely subjective but is based on both productivity and other financial loss recorded in the Requirements document. The IS Department discusses the affect that RTO and other requirements have on the cost of the project, so the business is educated on how small differences in requirements may lead to very large differences in project cost. Nearly 85% of all applications have an RTO of several days up to a month. This allows the IS Department to identify which applications are more critical to the business and plan for IT DR activities accordingly.

Application recovery procedures

In addition to the Requirements document, ABC develops a separate BC/DR planning document, prior or during the Release phase of the IT project, called the Application Recovery Statement (or ARS). The primary objective of the ARS is to document the step-by-step procedures to recover the application or IT service in a disaster recovery scenario. Similar to the Requirements document, the IT Operations staff is available to sit down with anyone completing an ARS in order to help them understand how their answers will impact a recovery operation. The ARS is comprised of two main parts. The first part of the ARS records all required dependencies that must be available before specific application or service recovery steps can proceed. Documented dependencies may include required:

- Network infrastructure, such as which networks and data centers by location must be available;
- Client infrastructure, such as minimum number of workstations by location and/or any thin clients or virtual PCs (i.e., virtual desktop infrastructure);
- Server infrastructure (i.e., which server(s)/data volume(s) need to be recovered);
- Database infrastructure (i.e., which database(s) need to be recovered);
- Mobile infrastructure services, such as BlackBerry Enterprise Server;
- Network drives/files (e.g., G:\, H:\, etc.); and

- Other back-end infrastructure services, if applicable, such as Active Directory, terminal/thin client servers, paging/e-mail/fax servers, Internet access, FTP access, remote access, network printing, etc.

The ARS has checklists for many common infrastructure dependencies and allows the person filling out the document to simply check what is needed in order to make the process less cumbersome.

The second part of the ARS asks the analyst or business support person to answer questions about the actual recovery, including:

- Overview of recovery concepts;
- Detailed, step-by-step recovery procedures;
- Interfaces, integration, and synchronization with other applications or data sets;
- Business continuity procedures (What will the business be doing while the application is being recovered or if the application is down for an indefinite period of time?); and
- Any additional information that may be helpful in a disaster, such as location of any paper records, electronic media storage, persons, etc., which could aid recovery.

The ARS instructions ask that the author take into consideration that, in an actual disaster, the individuals performing the recovery may not be familiar with the application. In addition, the ARS is revisited throughout the lifecycle of the application, including:

- Immediately before the application goes live;
- When the application goes through a major upgrade;
- When information contained in the document changes for any reason; and
- At least once every calendar year.

Similar to the Requirements document, the ARS is required to be signed by every impacted company Manager/Director before final access control changes are made and the application is released into Production.

Summary of integrating BC/DR requirements into IT governance

Regardless of whether a formal IT Governance process exists at your company, ABC demonstrates how BC/DR requirements, IT service level definition, and effective application recovery procedures can be integrated into normal IT operational tasks in order to improve recovery strategies and BC/DR outcomes for business clients. By taking a bottom-up approach to BC/DR planning where business needs intersect with daily IT operations, absent a formal top-down BC/DR project, ABC IT staff have seized the opportunity to make ongoing, incremental process improvements during the different phases of the Software (or System) Development Lifecycle. By continually improving written BC/DR documentation and asking for formal business area

approval before applications go into production, they have made BC/DR planning discussions a normal part of business operations and affected positive change.

For more information on performing a risk assessment and BIA, and determining BC/DR requirements, continue reading [Chapters 4](#) and [5](#) in this book.

IMPROVING BC/DR RECOVERY AND RISK MITIGATION STRATEGIES

Once definition of BC/DR requirements/service levels and application recovery documentation started to improve at ABC, the IT staff was able to craft better functional designs for the supporting IT infrastructure and ongoing risk mitigation activities, such as security patching, backup, and periodic recovery testing. Disaster recovery and risk mitigation strategies go hand in hand when working to improve BC/DR planning. Disaster recovery strategies focus on the use of technology, process, and people to meet service level objectives in terms of RTO, RPO, and so on, in the event of a disaster. Risk mitigation strategies focus on avoiding or limiting the effect of identified threats should they materialize. Threats such as IT security threats, hardware failure, power failure, floods, or fire are rather well known, occur more frequently, in general, and are likely to affect nearly every company at some point; however, their impact is often isolated to a small group of IT assets, individual networks, or parts of a building. Threats such as widespread natural disasters (e.g., hurricanes, tornados, and earthquakes) have a greater likelihood depending on geographic location and can cause widespread damage across neighboring geographic regions and multiple company assets.

In the absence of a formal risk analysis and ranking of all identified threats to the company's operations, the IT staff at ABC made a calculated choice to focus their attention on the more common threats to IT assets, such as IT security threats, hardware failures, threats to individual data centers and buildings, and, ironically, even power failures. The following recovery and risk mitigation strategies are not meant to be complete or necessarily demonstrate what all companies can or should do, but they are highlighted in this chapter in order to demonstrate how one group of talented IT professionals has drastically improved their company's BC/DR planning efforts by acting within their own sphere of influence. Please keep in mind there are many common risk mitigations or recovery best practices not listed here, which may or may not be in place at your company, including things like monitoring and logging of events, physical access controls, personnel training, etc. The following examples were chosen because they may be overlooked, may not be common practices today at your company, or may offer a new way of leveraging existing processes at your company to improve BC/DR planning.

Ensuring access to BC/DR documentation in a disaster

In the aftermath of a disaster, the first thing you will need is information necessary to begin recovery. This information is typically defined in a formal BC/DR plan

document. Absent a formal document, ABC IT staff knew it was critical to have a central location for BC/DR and other operational documentation they were creating on a daily basis, at a minimum; one that could be backed up securely and was readily available off-site. ABC IT staff also realized that a review and update of this documentation should occur regularly to ensure it was current, with the most opportune time being the implementation of infrastructure changes required to accommodate new IT projects.

To this end, IT Operations staff worked with IT Security staff to create a checklist of items for the IS Project Management Office and Business Relationship Management teams for inclusion during the Release phase of each new IT project. Before an application goes live, disaster recovery documentation gets created or updated, and stored in a central location at the same time backup procedures and access control changes are implemented. IT DR documentation stored in a central location includes:

- Requirements documents;
- ARSs;
- Physical and logical network and system design documents;
- IT Service Level Matrix;
- Incident Response/Crisis Communication Plan, including call out trees and teleconference phone numbers;
- Network, system and database backup, and restore procedures;
- System and database inventory lists;
- Master IT Vendor Contact List, including vendor sales and support contact information;
- Encrypted, password-protected master password databases;
- IT physical asset database (exported copy);
- IT Security audit database (exported copy);
- IT Service Management database (exported copy).

In order to ensure all IT DR information is available to those who need it in a real disaster, multiple copies are made and stored at different locations. First, all IT DR documentation is maintained centrally on a secure production network file share and periodically replicated off-site. This off-site copy is also archived to tape for 30 days, and the tapes are rotated out each week in a secure, fireproof vault. (Alternatively, it could just as easily be replicated to a secure, encrypted location in the Cloud, if you don't use tape for archival purposes.) Second, the entire Disaster Recovery folder is burned to DVDs as well as copied to remote USB drives on each of the data center command center PCs each month by IT Help Desk staff. A copy of the monthly DVD is given to three different IS Managers to take home with them; old DVDs are securely shredded. The IT project Release phase includes a checklist of the above BC/DR documentation that must be created or updated before IT Security will provision or otherwise change access or authorization to an application released to Production. This enforcement mechanism ensures BC/DR planning is integrated into the on-boarding process for new software.

TIP**Use New IT Projects to Begin BC/DR Planning Documentation**

If you don't know where to start with BC/DR process improvement, you don't have executive sponsorship for a companywide BC/DR project or your BC/DR documentation is incomplete, simply begin improvements with the next IT project you are asked to support. Involve your IT Operations and/or IT Security team and use the BC/DR documentation list from ABC as a starting point to begin to document answers to BC/DR questions as part of the IT project plan. Or, if no formal IT project plan exists, document answers to BC/DR questions as part of your infrastructure provisioning (i.e., server build) or access control change processes.

Change approval board and technical change review committees

ABC has a formal Corporate IS Change Management process and Corporate IS Change Approval Board (CAB) in order to control the impact of changes on IT service levels and ensure changes adhere to IS standards. In addition, specific operational IT networks which are partially or wholly managed or supported by corporate IS staff, such as the Energy Management System network, the Physical Security network, the Facilities network, and the Generation networks, have separate cross-functional Technical Change Review Committees where all proposed IT changes are documented in advance and discussed and approved by all stakeholders outside the Corporate IS CAB meetings. Although each company is different, ABC cannot stress enough the importance of establishing and maintaining a formal change review process, including periodic meetings with affected stakeholders, for every IT network managed by the company. In essence, if you don't control change, you can't plan for BC/DR.

In order to keep BC/DR documentation current and to ensure continuous improvement of BC/DR processes, ABC has integrated BC/DR into its formal change control mechanisms. Whenever a change is approved and executed, ABC assesses whether DR documentation needs to be updated as a result of the change. The change request document or form provides a simple checklist and asks the change requester to evaluate which DR documentation, if any, will need to be updated after the proposed change is approved and completed. The change requester's supervisor or the IT asset owner, who approves the change, is responsible for ensuring applicable disaster recovery documentation is updated accordingly before the change is closed. For example, if a change involves upgrading an existing software application to a new version, the ARS is updated to reflect the location of the new installation files and, if applicable, the new server name, location, etc. At weekly change control meetings, closed change request records are reviewed for required updates to any DR documentation.

ABC's change control meetings also ensure integration of BC/DR risk mitigation best practices into daily IT operations. For example, if an unplanned outage occurs for any reason, a separate problem ticket is opened and root cause analysis, lessons learned, and any planned improvements (i.e., future planned changes) will be discussed during weekly CAB meetings until the problem is closed out, thus mitigating

the risk of reoccurrence of the unplanned outage. Depending on the severity or cause of the unplanned outage, the CAB may recommend a separate, *ad hoc* “postmortem” meeting be set up with all stakeholders after recovery and problem resolution is complete, in order to discuss root cause analysis, planned preventative measures, and incorporate lessons learned into BC/DR planning and documentation.

CRITICAL CONCEPT

Use Change Control to Enable Continuous BC/DR Process Improvement

One of the most important things you can do immediately to improve BC/DR outcomes at your company is begin to formally integrate BC/DR processes into your change control procedures by (1) ensuring your change request process includes an assessment of whether BC/DR documentation needs to be updated (or created) and (2) ensuring your change control meetings have standing agenda items to discuss unplanned incidents or outages and assign relevant BC/DR action items (such as the need for a separate postmortem meeting with all stakeholders to discuss BC/DR planning improvements).

Security control testing

For certain IT assets deemed critical to safety, health, company operations, or which fall under certain government regulations, an added level of testing, specific to security controls, is performed with each and every planned significant change, such as the installation of a new hardware asset, new software, or security patches. Tripwire, a security baseline and monitoring tool, is used to document security baselines before and after the significant change is made in a test environment, prior to the change being approved for the production IT asset. In this manner, unanticipated changes to established security baselines for the particular IT asset in question can be discussed with the vendor or otherwise evaluated by the IT operational area prior to the actual production change being approved. For such changes which are approved to proceed, security baselines are either updated with an explanation of the justification or mitigating procedural or technological controls are documented.

CRITICAL CONCEPT

IT Security: Cost vs. Benefit

It is clear that the IS Department at ABC has invested a substantial amount of time and money into its IT security practices to ensure a rather mature BC/DR risk mitigation strategy with regard to IT security threats. However, they didn't get there overnight. More importantly, they know they are never going to reach some allusive goal with respect to their BC/DR planning efforts. Rather, they have committed themselves to continually changing and refining their practices based on real-world challenges and opportunities. Instead of blaming or pointing the finger, they have engaged. Instead of giving up on the seemingly impossible, they have made small, gradual steps forward with the business by their side. By establishing formal change control and incident response processes, they are able to *improve their BC/DR planning*.

Continued

CRITICAL CONCEPT—cont'd

over time. The goal, regardless of your size, industry, available resources, risk profile, etc., should be *continuous improvement over time*, and nothing more. In order to do this, you simply need to establish processes and procedures, by which, you can formally examine, evaluate, and address each unforeseen incident as it happens, documenting and incorporating your findings into your operations as you progress. It's as simple as that. Don't think you have to develop a perfect strategy before you begin. Simply begin with what you have now, and make the time to discuss, document, and refine as you go along.

Separation of duties

The risk of internal sabotage is often overlooked as a significant risk to a company, but all companies should treat this threat seriously since the impact is so great, even if the likelihood isn't. Before a new IT project is released to Production, the IT Security team requires separation of duties related to ongoing support be documented. ABC maintains separate password databases for Network, Systems (servers and storage), Infrastructure Applications (e-mail, mobile, wireless), IT Security, and the each of the different application support teams, in order to mitigate risk of internal sabotage by a lone employee. Moreover, systems' administrators and IT Security, both of whom have a high level of rights across all supported networks, have two user accounts, one used for day-to-day user activities and an administrator-level account used to perform operational tasks requiring elevated privileges.

Centralized security vulnerability assessment

In order for an organization to understand, and properly plan for and manage, the security risks to their IT assets, they must have up-to-date information on real-time security vulnerabilities by platform. Therefore, it is critical that IT staff incorporate real-time security vulnerability information reporting by vendor platform as part of their ongoing maintenance activities.

To this end, ABC uses a centralized security patch assessment hosted service known as Secunia Vulnerability Intelligence Manager. All IT asset types by vendor, across the company, are loaded into the tool and weekly reports are generated for the different IT operational areas. IT asset types, by vendor and platform, can be requested to be included in the Secunia vulnerability database if they don't already exist. IT operational areas generally must assess reported vulnerabilities within 30 days of the Secunia report, and assessment tasks are discussed weekly as part of the Change Management processes discussed earlier. ABC also subscribes to the SANS Institute Consensus Security Alert service in order to obtain up-to-date information about critical zero-day security exploits. Zero-day exploits that are identified as critical are assessed and managed separately, through *ad hoc* CAB meetings, for all involved stakeholders.

Vulnerability assessment results are loaded into the tool in order to track known vulnerabilities across all IT assets. If an identified vulnerability is remediated

through a change, e.g., a security patch is applied or an unneeded service port is disabled, the associated change ticket number is noted, and the status is set to “resolved.” Otherwise, any mitigating procedural or technological controls are documented in the tool and the status is set to “accepted.”

Although there is an ongoing cost for this service, ABC realized that integrating centralized vulnerability assessment into its change control procedures has helped educate all IT operational areas on the importance of continually mitigating security risks to IT assets as part of normal business operations. In addition, ABC recognizes the cost of not having a formal, centralized vulnerability assessment process is far greater than in the past, since the likelihood of a security threat materializing is always growing as demand for IT services grows.

IT network vulnerability assessment

In addition to understanding current vulnerabilities by vendor and platform, a second (and equally important) piece to maintaining a low security threat profile for networked IT assets is to have information about how these assets are seen on the network by unauthorized users and how they respond to network requests on open physical and logical ports. To this end, it is critical for any organization involved in risk mitigation activities to periodically scan the network and produce actionable reports for high, medium, and low network vulnerabilities so that ongoing remediation can occur through established change control processes.

For all IT networks across the company at ABC, internal and external network vulnerability assessments are planned and scheduled on a periodic basis. In addition, network vulnerability scans are required to be performed by outside audit firms on a periodic basis for certain networks with critical IT assets subject to government regulations. Moreover, when new servers are installed and prior to applications being released to production, individual asset vulnerability scans, using the Nmapse Rapid7 and Nessus vulnerability assessment tools, will be scheduled by IT Security. All identified vulnerabilities are categorized as high, medium, and low, and status of all remediation efforts is tracked centrally. In order to minimize risk to critical operational IT assets, such as generation control networks, arrangement is made to do the scanning in failover mode (if clustered) or do the scanning when generation units are undergoing maintenance or otherwise off-line.

In addition to periodic scans, formal quarterly release processes for major IT applications incorporate changes required to remediate critical vulnerabilities into their release schedule. In addition, when an application goes through a major upgrade or release, remediation of high and medium scan results is incorporated within the IT project as a distinct effort. In all cases, monthly updates are required to be documented in the centralized tracking tool and progress on all open and closed items, regardless of threat assessment, is summarized and reported monthly to all stakeholders and their executives by IT Security.

Security control baselines and change detection

In addition to real-time vulnerability information (by platform) and ongoing assessment of network vulnerabilities, IT staff must be able to determine unexpected gaps in the security controls implemented on their IT assets, such as the introduction of unplanned network ports and services or unplanned changes to permissions and rights on a server.

As was discussed in the previous section, new IT systems going into Production are scanned with the Nmapse Rapid7 vulnerability scanning engine to determine known network vulnerabilities. As part of the Release Management phase of the IT project, identified vulnerabilities are analyzed against approved security control baseline standards and exceptions are documented with compensating administrative, network, and/or physical controls. Security control baseline standards may vary between operational networks or different classifications of assets. For example, all cyber assets which fall under NERC CIP (North American Electric Reliability Corporation's Critical Infrastructure Protection) Reliability Standards have to have a wide range of prescribed security controls in place, whereas non-CIP devices may only require security controls which mitigate or fully remediate vulnerabilities with a high threat assessment. If vulnerabilities are identified outside of approved security configurations, they are either remediated prior to being placed in Production or exceptions are documented and approved by IT Security in coordination with IT operational groups. In addition, security control standards are reviewed and often updated with new information during quarterly review meetings with IT Security.

In addition, as part of the lifecycle management of IT assets, Tripwire, a configuration change detection tool, is also installed on critical IT assets and used to detect, gather, and report on real-time, historical changes to approved local security configurations. IT asset owners receive periodic Tripwire reports via e-mail and are asked to correlate approved change records to any detected changes to established security baselines or standards, such as new service ports being opened up or changes to internal user accounts, rights or access control settings. Status of detected changes is recorded in the tool, and any exceptions or open items are reviewed at periodic change control meetings.

Data center and network

Based on what we've discussed so far, it is clear ABC has spent a considerable amount of time and energy over the past 8 years improving security risk mitigation strategies for their IT assets. In addition to security risk mitigation, other risk mitigation activities were undertaken in parallel to help improve recovery operations in addition to other service levels. Since all critical IT services depend on reliable and protected data center and network assets, they began with improvements to these core infrastructure assets, incorporating BC/DR best practices as they progressed. First, they implemented a data center and network upgrade project in order to

(1) enable server virtualization, (2) enable a converged shared storage infrastructure, and (3) improve recovery objectives based on their most stringent RTO requirements—30 minutes for their Outage Management System (OMS).

Today, they operate dual production data centers outside of flood zones in the same city as their headquarters, 10 miles apart and connected by 10 Gbps redundant fiber loops. Both data centers employ redundant A and B power supplies, with UPS and diesel generator power backup systems to power both the internal network, servers, and environmental systems, such as chilled cooling or sump pumps, in case of loss of building power. Enough diesel fuel is kept at each site to run the generators for several days, if need be. All networking gear is standardized on a single vendor, Cisco, and both core and distribution routers and switches are dual aggregated, each with dual power supplies connected to both A and B data center power feeds. Both 1 and 10 Gbps connectivity is provided, depending on requirements. By designing full redundancy into their network and environmental systems, they ensure that the loss of a single data center node will not cause a network outage.

In addition, they operate an FM-200 dry fire suppression, subfloor leak detection, and preaction sprinkler systems in their primary data centers. The FM-200 dry fire suppression system is waterless and protects expensive IT equipment by leaving no residue or deposits upon discharge; the discharge can be removed from an area with simple ventilation. If dry fire suppression fails to put out the fire within a certain amount of time, preaction sprinkler systems will trigger. Under the 18" subfloors, leak detection is also in place with sump pumps should ground water be detected.

Moreover, ABC segments operational networks from each other and employs firewalls and IDS/IPS (Intrusion Detection System/Intrusion Prevention System) technology between networks in order to further mitigate risk.

ABC's WAN infrastructure connects buildings in some 20 different geographic locations spread over an approximate 350 mile radius. In addition to the dual production HQ data centers, ABC has smaller remote data centers or server closets, as well as a separate co-location facility over 100 miles from HQ. These smaller remote locations house limited production capacity for remote operational areas, and a few house remote off-site backups for critical HQ systems and data. The co-location facility provides WAN connectivity to remote areas and can be used to house production capacity in the event it is needed.

Compute and data

Not so long ago, servers were purposely built for nearly every piece of application software, the two were configured to work with each other and were inextricably linked once put into production, and the term “bare metal recovery” was part of the lexicon of standard IT disaster recovery operations. As a result, restoration of the software and data, or IT service, always depended upon additional plans, procedures, and costs associated with restoration of the server hardware, operating system, and individually configured network interfaces. As a result, recovery operations for IT infrastructure had to be designed more specifically for each and every application

and took additional time and resources. In addition, the cost of the infrastructure design was much higher if continuous data protection (e.g., mirrored hot sites), spare parts/redundant server hardware, or server clustering software was required for high-availability applications. Today, virtualization technologies have obfuscated much of the underlying hardware to the point where recovery operations are dramatically less expensive and take much less time than they used to. ABC was an early adopter of such technologies and has nearly a decade under its belt in terms of how to best manage compute and data to achieve drastically improved BC/DR results.

As was stated earlier, ABC's most stringent RTO is 30 minutes; however, they currently operate with recovery times under 5 minutes for most applications in most unplanned outage scenarios. ABC does not implement full mirroring between its dual production data centers in order to achieve this performance, primarily because virtualization technologies cost much less and produce better than required performance *based on documented requirements*. Instead, they physically separate Production (Prod) systems from Development (Dev), Test or Quality Assurance (QA) systems. All production systems are split between the two data centers. If one data center houses Prod, the other houses the Dev, Test, and/or QA instances for that particular application or service. They then backup these systems and data to the alternate data center bidirectionally. In addition, they maintain a reserve of additional compute and storage capacity at each data center in the event an entire data center is lost to a disaster, and they need to recover the most critical systems and data within 24 hours (i.e., Tier 1 and 2 applications, as defined in their Service Level Matrix). Backups of remote systems and data to one of the HQ data centers occur at regularly scheduled intervals and at off-peak times over slower WAN links.

ABC was an early adopter of server virtualization, in part due to its significant BC/DR and cost benefits. Today, it has a “virtualization first” policy; all new server instances are virtualized, regardless of application vendor support, unless requirements or contractual obligations dictate otherwise. For example, if a server requires a special communication adapter or there are exceptional performance requirements, a physical server will be used instead. From a support standpoint, moving from a virtual server to a physical server (P2V), if need be for specific troubleshooting circumstances, is easily accomplished with Novell’s PlateSpin tool. Today, VMWare ESX and VCenter technologies are employed to virtualize nearly 100% of Microsoft Windows instances using commodity Dell rack mount or blade server hardware. In addition, all Oracle Sun Solaris server instances are virtualized zones using Solaris’ ZFS file system on shared physical Oracle Sun Sparc servers.

VMWare allows for virtual server instances to be housed on shared enterprise storage using any of a number of storage protocols, including file-based protocols such as NFS. ABC uses NFS over 10 Gbps Ethernet extensively to serve up nearly all virtual server instances to clients on shared NetApp storage systems. By doing so, each virtual server instance is stored as a single VMDK file on a shared enterprise storage volume. Since each server is essentially a network file, ABC’s BC/DR recovery strategy has improved significantly for several reasons. First, files are much

easier to manage than block-based fiber channel LUNs, which require full restoration on available storage (and significantly more time) before data inside can be recovered. Second, ABC uses the built-in data protection technologies of the shared NetApp storage to snapshot the volumes housing the VMDK file, locally, and then replicate the snapshots to off-site storage periodically using NetApp's SnapMirror technology. Snapshots are essentially very fast, point-in-time backups of the storage volume housing the virtual server instances. Snapshot operations have virtually no effect on server performance, and no server-based backup software is required to be purchased or managed. To restore a virtual server instance from backup disk media, one simply connects to the snapshot or remote mirrored snapshot and either connects to the VMDK file in order to boot the virtual server or peek inside to extract volume-level folder and files using a free tool such as UFS Explorer.

In addition, VMWare employs two primary technologies, VMotion and HA, which build on the concept of a “server as a file” and further enhance disaster recovery capabilities. VMWare server VMotion and storage VMotion allow server instances to move seamlessly between disparate server and storage hardware, without taking an outage on the server itself. VMWare HA (high availability) detects if virtual servers are unresponsive for any reason and automatically resurrects the server on an available ESX node using VMotion. Together, these two technologies allow for virtually no server down time for planned maintenance, and near seamless automatic server recovery without human intervention in the case of most unplanned hardware failures.

CRITICAL CONCEPT

Server Virtualization and Shared Network-Attached Storage: Transformational for IT Disaster Recovery

The capabilities that server virtualization brings to BC/DR operations have been transformational for ABC. Instead of having to perform slow recovery from tape, having to reconstitute entire block-based LUNS on separate available storage, having to use cumbersome backup and recovery software to manage distinct backup jobs, or even having to deal with bare metal recovery of physical servers, ABC can recover virtual servers easily and reliably in minutes instead of hours or days. In addition, virtualization drastically improves availability and service levels by allowing ABC's IT staff to put physical ESX hosts (server hardware) in “maintenance mode” at any time to perform planned hardware maintenance without having to take down virtual server instances; VMWare simply VMotions the all virtual servers to another ESX host with available capacity, with no client impact, so the physical server can be powered off or rebooted at any time without incurring an outage. Moreover, server virtualization technology even enables automatic, scripted failover, and fallback processes so that ABC IT staff can provide self-service failover to DR sites for individual applications or sets of applications, as you will read about later in this chapter.

In the case of Oracle Sun Solaris, the ZFS file system is used to create virtual Zones which house each virtual “zoned” server. Tools such as NetApp's Open System SnapVault (OSSV) can then be used to snapshot the zone/server locally, while the server is live, on the same production storage volume, similar to virtual servers

managed by VMWare. OSSV can also be installed on physical server instances to create snapshots of entire physical server data volumes on shared storage, and it is generally licensed at little to no cost if you already license the NetApp hardware and replication software. Replication of historical snapshots to off-site storage (i.e., mirrored snapshots) occurs exactly the same way as with VMware virtual servers, via NetApp SnapMirror.

ABC's use of shared enterprise storage to house network files and virtual server files together, along with local historical backups of the data (i.e., snapshots), has transformed system-level backup and recovery operations entirely. By employing similar storage systems at each data center location, production and backup data can be seamlessly served up at the same time. By employing clusters of ESX or Solaris ZFS hosts connected to enterprise storage at each location with sufficient reserve compute capacity, restoration of virtual servers at off-site facilities is as simple as opening a file from within VMWare VCenter or Solaris. This is one reason why server virtualization is a huge enabler of private or public cloud computing for disaster recovery operations.

Virtualization also improves database recoverability. At ABC, databases are backed up to local server volumes using vendor backup toolsets, and a limited number of local backups are kept to minimize required volume sizes. Since these server volumes are contained within a single VMDK or Solaris zone, database backups can easily be recovered from "local" volumes once a snapshot is restored and the virtual server is started back up. There is no need to at ABC to manage separate backup jobs of databases over WAN links to separate off-site storage volumes.

Since reliability, availability, and recoverability of virtual servers are tied heavily to shared enterprise storage, and to a lesser extent, individual physical ESX or Solaris servers at ABC, it is important that significant fault tolerance be designed into their enterprise storage. All NetApp storage systems employed by ABC which house production servers and network files (as opposed to merely backup data) utilize a pair of clustered HA controllers, redundant fiber loops to each disk shelf and RAID DP disk groups. Clustered controllers (or heads) allow the system to automatically fail over from the primary head to a secondary head if any problems occur. In addition, redundant fiber loops ensure that all disks are presented to and accessible by either head. Moreover, the disks are arranged into fault tolerant RAID DP groups, allowing up to two disks in any RAID DP group to fail without losing access to the data volume. Spare disks on each system are available to reconstitute any RAID DP group on the fly, and phone home capability ensures that NetApp is automatically notified of any disk failure so that they can send out replacement disks to be received and replaced within 4-8 hours. For physical servers, such as VMWare ESX or Solaris hosts, boot partitions are mirrored in a RAID 0 disk configuration. Therefore, if one disk fails, the other disk is still read to and written from, allowing the hosted hypervisor or operating system to remain operable. All physical server and storage system network interfaces and power supplies are redundant, as well, with both A and B connections to different clustered distribution switches or different PDUs (power distribution units) within a data center rack.

Self-service application failover and fallback

By treating servers as network files, by storing these network files on enterprise storage volumes, and by using volume-level data protection technologies built into the enterprise storage systems, ABC has been able to set up automated, self-service failover, and fallback operations for specific business areas using common scripting tools. For example, ABC's Outage Management System (OMS) is a software application which, in combination with geospatial information system (GIS) overlay data, provides 24/7/365 Transmission & Distribution operations personnel with the ability to manage all electric outages throughout its service territory from a central location. The OMS application has the shortest RTO of any application on the corporate network, at 30 minutes, and it is critical that it be highly available during annually occurring storm seasons. The OMS application utilizes a back-end Oracle database for its real-time transactions and also relies on a copy of the GIS proprietary VMDS (Version Managed Data Store) database for its map data. Both databases must be online at the same time in order for the OMS application to work correctly.

In the old days, the OMS application ran on a Windows NT clustered physical server that was highly unreliable. Prior to a planned upgrade of the OMS software, IS staff convinced the business support staff to move to a virtual server environment for BC/DR improvements. The OMS application server hosts the application on its E:\drive and connects to both the Oracle and VMDS databases residing on a separate server. As part of the upgrade, the OMS application server was virtualized on VMWare and moved to a single NetApp production volume. The Oracle and VMDS databases were moved to another NetApp production volume.

Using NetApp's snapshot technology, snapshots were scheduled to be taken locally every 15 minutes on both the database volume and the application server's E:\ drive, and then replicated using SnapMirror out to a target NetApp system at the DR site. OMS IT support staff had previously requested a 15-minute RPO requirement for 24/7/365 operations. Initially, it wasn't known if taking a snapshot of a live database, without quiescing (or pausing) it first, would cause data integrity issues. However, OMS IT support staff communicated that database transaction logs could be manually employed, if need be, to rollback both databases to a previously stable state within the 15-minute backup window. In the event of any unplanned outage of production OMS, manual failover operations involved quiescing (or pausing) the data mirror, breaking the mirror, converting the target-mirrored volumes at the DR site to writeable production volumes, and then connecting the backup OMS virtual server's E:\drive to the target volume, before the application could be launched in failover mode at the target site. In order to fallback to the production data center once service restoration is complete, a similar manual process is followed. Although this manual failover process took IS staff significantly less than 30 minutes to execute, ABC does not maintain or staff an on-site 24/7/365 corporate network operations center, and it could take up to 30 minutes or more during nonbusiness hours for IS on-call staff to simply respond to phone call and be able to remotely connect to the network to perform the manual failover operation.

Based on this fairly straightforward and time-tested manual recovery failover and failback process, IS staff took each manual step and wrote a script to automate both the failover and failback procedures. They worked with OMS IT support staff to iteratively test the failover and failback process to ensure it met the business area's needs. Now, ABC's OMS IT support staff have separate failover and a failback scripts, which can be easily executed from their desktops. In the event of an unplanned outage to the primary OMS system, the failover script is launched, failover occurs in a matter of a few minutes, and OMS operators simply launch a separate icon on their desktop to run OMS from the DR site. This technique, enabled by advances in virtualization on shared enterprise storage, has since been employed at ABC to provide additional self-service failover and failback for other 24/7/365 software applications, such as other critical work management systems, without IT staff intervention.

Industrial control systems

Whereas the corporate physical security and facilities networks at ABC are highly virtualized and, therefore, derive the benefits of virtualization for BC/DR operations on a regular basis, other operational networks, such as ABC's Distributed Control System (DCS) for generation control and Supervisory Control and Data Acquisition (SCADA) system for EMS control, vary in their use of virtualization and BC/DR operations. Networks such as these are known as industrial control system (ICS) networks, and the lion's share of vendors in this space are much more traditional when it comes to network/system design, configuration, and support. Initially, ICS had little resemblance to IT systems in that ICSs were isolated systems running proprietary control protocols using specialized hardware and software. Widely available, low-cost Internet Protocol devices are now replacing proprietary solutions, which increases the possibility of cyber security vulnerabilities and incidents. Hardware and software design and support for ICS networks are typically outsourced entirely to a single vendor, and companies such as ABC rely heavily on specific vendors for ongoing support of these systems, as do most energy and utility companies. Risk is typically higher with such networks, as well, since many ICS processes are continuous in nature and unexpected outages of systems that control industrial processes are not acceptable. For an ICS, human safety and fault tolerance to prevent loss of life or endangerment of public health or confidence, regulatory compliance, loss of equipment, loss of intellectual property, or lost or damaged products are the primary concerns.

Unfortunately, BC/DR is often an afterthought in terms of how these vendor support contracts are written. Moreover, since ICS systems rarely fall under the purview of a corporate IT department or are supported by personnel without specialized IT skill sets, users of these systems are typically the last to participate in mature change control, IT DR planning or other industry-standard IT security or service management processes. Ironically, however, the companies they work for serve to benefit more from such processes.

As a result of this unfortunate reality, government regulation of ICS systems has increased dramatically over the past decade in the United States. At ABC and most other electric utility providers throughout the United States, NERC CIP Reliability Standards, implemented and enforced by the U.S. Department of Energy's Federal Energy Regulatory Commission starting in 2007, now mandate that such ICS networks must have written and auditable disaster recovery plans (DRPs), including roles and responsibilities of responders and required actions in response to events or conditions of varying duration and severity that would activate the recovery plan. In addition, backup and recovery procedures, along with annual exercises of recovery plans and testing of backup media, are now required. Moreover, updates to recovery plans are also mandated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident, and updates must be communicated to personnel responsible for the activation and implementation of the recovery plan within 30 calendar days of the change being completed.

ICS components or networks such as the EMS SCADA and generation DCS systems, which are considered by ABC to be critical, have HA requirements. One method of achieving HA is through the use of redundancy. Additionally, if a component fails, it should fail in a manner that does not generate unnecessary traffic on the ICS, or does not cause another problem elsewhere, such as a cascading event. In addition, the control system should have the ability to execute an appropriate fail-safe process upon the loss of communications with the ICS or the loss of the ICS itself. In the case of the EMS SCADA system, ABC has defined "loss of communications" to be 1 minute without communication. In the event of loss of communication on the primary EMS SCADA system, ABC maintains an Emergency Operations Center (EOC) with a fully redundant SCADA network, and all EMS SCADA system operators and support personnel have a 30-minute window after "loss of communication" to resume normal operations at the EOC. ABC EMS SCADA support personnel also maintain procedures for operating the SCADA system in manual mode with all external electronic connections severed until secure conditions can be restored.

Since high reliability of ICS systems is an important method of risk avoidance at ABC, the EMS SCADA system, for example, employs redundant A and B hosts in production, with an off-line spare available at the primary site. A third C host at the EOC ensures that emergency SCADA operations can continue at the EOC until the primary site is restored. In addition to maintaining redundant hosts, backups are performed using the "backup-in-depth" approach, with layers of backups (e.g., local, facility, and disaster) that are time sequenced such that rapid recent local backups are available for immediate use and secure backups are available to recover from a massive security incident. A mixture of backup/restore approaches and storage methods, including both disk-to-disk and disk-to-tape backup, is used to ensure that backups are rigorously produced, securely stored, and appropriately accessible for restoration.

Today, primarily due to the introduction of NERC CIP Reliability Standards since 2007, EMS SCADA and generation DCS support personnel participate in a

variety of cross-functional processes along with IS Department personnel at ABC. Each network has its own cross-functional technical change review committee that meets periodically. In addition, all operational IT networks participate in a weekly NERC CIP change control meeting and an annual cross-functional NERC CIP Recovery Plan exercise.

TIP**Risk Management and Contingency Planning for ICSs**

A comprehensive resource for risk management and contingency planning for ICS networks can be found in NIST special publication 800-82, *Guide to ICSs Security: Supervisory Control and Data Acquisition (SCADA) systems, DCS, and other control system configurations such as Programmable Logic Controllers (PLC)* (found online at: <http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf>). This publication provides thorough planning guidance for protecting ICS networks, including how to protect individual ICS components from exploitation, maintain ICS functionality during adverse conditions, and restore the ICS system after an incident (Stouffer et al., 2011).

Summary of improving BC/DR recovery and risk mitigation strategies

ABC has spent nearly a decade investing in and improving its risk mitigation and recovery strategies to ensure BC/DR solutions meet or exceed documented BC/DR requirements for critical systems. ABC approached both security risk mitigation and operational DR improvements simultaneously, using business functional requirements and regulatory requirements as the starting point. IT staff improved the company's BC/DR capability gradually, without a formal enterprise-wide BC/DR project, by focusing on incremental improvements and incorporating BC/DR best practices within its existing change control processes.

In terms of security risk mitigation, IT staff at ABC implemented a standardized change control process, a central CAB and technical change review committees for each critical operational network. It enforces separation of duties through standard IT project Release processes. In order to develop a comprehensive understanding of changes to security threats, it implemented a centralized vulnerability information tool and performs periodic network vulnerability scans and change detection for critical assets. In addition, it produces and revises standard security configuration baselines based on the type and version of operating system platform in use and changing information on current threats. Moreover, it enforces testing of security configuration baselines through existing change control procedures in order to further mitigate risk.

In terms of recovery operations, IT staff at ABC implemented core data center and network improvements first, followed by shared enterprise storage and server virtualization technologies to meet compute and data resource recovery objectives while minimizing operational costs. It standardized and consolidated its infrastructure hardware and vendors. Furthermore, it leveraged its virtualized compute infrastructure on shared storage to implement self-service failover and fallback operations for critical applications with stringent RTO and RPO requirements.

For its ICSs, such as its generation control systems and EMS SCADA system, ABC established policies and procedures in order to be in compliance with NERC CIP Reliability Standards. Furthermore, it implemented cross-functional technical change review committees and annual cross-functional disaster recovery exercises to share best practices across IT operational areas and reap the benefits of continual process improvement.

More information on Risk Mitigation can be found in [Chapter 6](#) of this book. In addition, further discussion of Emergency Response and Recovery operations can be found in [Chapter 8](#).

IMPROVING BC/DR TESTING

With significant improvements in IT disaster recovery and risk mitigation strategies now in place, ABC has evolved and improved their BC/DR testing over the years. Even though ABC acknowledges there is always opportunity for improvement, they have rightly embraced the concept of BC/DR planning as an ongoing continuous improvement process. Testing the right things, on a regular, periodic basis, has resulted in successive, documented lessons learned for all involved, and as a result, BC/DR planning has gradually improved over time.

Recovery from actual incidents: Postmortems and documenting lessons learned

ABC has experienced several BC/DR incidents of varying duration and severity; however, none were caused by a widespread natural disaster or loss of electricity for weeks or more. Several years ago, a torrential rainstorm flooded the basement of ABC's service center building at one of its main campuses, which housed old, manual electric relay equipment for its primary generation site in town. As a result, four generation units tripped and went off-line for several days, taking out building power to their old production data center as well. Diesel generators were brought in to supply power to the building and the data center while field crews worked to bring in power from across the street and other crews worked on restoring the electric relays housed in the flooded building. Water had to be pumped out of the basement after the storm subsided, and the entire basement had to be air dried before the relay gear could be repaired and generation brought back online.

The entire incident started over the weekend, so the impact for most employees and many departments was minimal. However, the impact to the company's bottom line, with generation off-line, was significant. During the relay restoration work, crews needed access to a little-known application database to help them rebuild the relay infrastructure. Few IS staff had ever heard of the application, but relay repair staff swore it ran in the data center; apparently, it was accessed very infrequently. So, for hours, IS staff frantically tried to locate documentation on this application to see what production server it was housed on, where the backup files were kept, etc., in order to restore the database so that the relay repair work could continue.

Although IS staff eventually got the database restored, it stopped the repair work for several hours and those few additional hours of downtime cost ABC quite a bit of money. This incident remains a very important lesson for ABC in terms of BC/DR planning, one they all remember to this day.

Most DR incidents involving IT outages at ABC are rarely this dramatic. However, ABC, like most companies, has certainly experienced its fair share of isolated, unplanned IT outages. Actual incidents over the years have ranged from isolated physical server outages running the EMS SCADA system (caused by unmirrored local disks that failed), to ESX servers on the corporate network purple screening due to OEM firmware bugs, to enterprise storage system panics where head failover didn't occur as designed and a good chunk of production virtual servers went down temporarily (until VMWare HA kicked in), to environmental failures in the data center taking down redundant power and several systems along with it (systems whose redundant power supplies were both accidentally connected to one power source).

Actual incidents which cause unplanned outages and impact IT service levels at ABC are tracked through weekly change control meetings. Separate incident tickets are created and closed after service restoration, and problem tickets are used to track root cause analysis. Often problem tickets will spawn one or more additional changes required to apply a long-term fix or to mitigate the likelihood of a similar future incident resulting in a service outage. Depending on the severity, impact, or duration of the outage, separate *ad hoc* postmortem meetings will be scheduled with all stakeholders.

These postmortem meetings serve several purposes. First, they provide a forum for the relevant IT support staffs to explain root cause and discuss how incident management processes were handled, including stakeholder communication, recovery procedures, response time, outside vendor support (if applicable), and the like. Second, meeting minutes document what worked well and what could be improved in terms of people, process, or technology. Third, lessons learned are documented, and incident response plans, crisis communication plans, DRPs, and/or recovery procedures are updated accordingly. Successive postmortem meetings may be scheduled after further analysis and additional preventative changes are completed.

All IS supervisory staff at ABC understand the importance of postmortem meetings to continuous process improvement and as a means of regularly testing written BC/DR documentation based on recovery from actual incidents. Postmortems always incorporate a review of written BC/DR documentation in order to incorporate lessons learned. Staff are trained to view postmortems as learning opportunities for everyone involved, and care is taken to explore the facts objectively, work as a team on follow-up action items, and not place blame on individuals or groups for things that went wrong.

Scheduled BC/DR tests

In addition to testing BC/DR documentation based on recovery from actual incidents, ABC also schedules several planned testing activities each year. These planned tests are meant to provide you with a sample of the kinds of operational

BC/DR testing required of an electric/gas utility such as ABC, including what is documented during testing and how testing is critical to demonstrating how ABC is engaged in the continual process of BC/DR planning. Planned testing which is specified in a BC/DR plan may originate from multiple sources, including outside regulations which specifically prescribe certain BC/DR tests occur periodically, to testing of internal IT/audit controls designed to address risk-based assessments required of regulations. Since reliability (vs. recovery) of IT services is also a critical component of risk mitigation, ABC also performs reliability testing of redundant systems. It is important to note that ongoing testing of a written information security plan document, to include some level of incident response and disaster recovery testing, is now required of nearly every company in the United States, not just big companies or those involved with critical infrastructure. More information on legal and regulatory requirements can be found in [Chapter 2](#).

Corporate data center redundancy testing

ABC schedules production data center redundancy tests to occur once each year. Although this is not a regulatory requirement, internal controls dictate that each of the two production data centers is subject to the annual testing, every other year. During these annual tests, redundant systems are tested, including power, network, and storage clustered controllers. A test plan is developed in advance which specify what specific step-by-step tasks will occur and what the expected observation or result should be after each step. The test plan also has a section to document what actually occurred after each specific action is taken so that actual result can be compared with expected result. Testing often causes some disparities between expected and actual results, and sometimes it is necessary to perform service recovery on isolated systems during the test. All stakeholders, including support vendors (e.g., storage, network, etc.), are notified in advance that a planned outage is not expected, but may occur.

Multiple IT operational teams participate in the annual data center testing, including IT Operations, IT Security, application support team on call staff, the EMS team, Facilities, etc. so that each team can understand all lessons learned. A single person is designated to document test plan observations, incidents, recovery actions taken the day of the test, and any follow-up action items. After testing is completed and all monitoring systems, support staff and 24/7/365 business areas report normal operations, successive follow-up meetings are scheduled until all resulting action items are completed. All test documentation is stored and can be referenced for the next annual test.

During the power part of the test, either A and B power are cut to the entire data center, separately, while environmental, network, and systems monitoring tools are observed. Response from UPS, ATS, and backup generator systems is observed after the power is cut. The backup generator is run for 20 minutes to ensure power and environmental stability under generator power. A (or B) power is then restored and the generator is turned off after the ATS switches back to the correct power source (if applicable). After all environmental systems show normal operations, the Network part of the test can begin.

During the network part of the test, a set of switch stacks, representing at least 50% of the entire data center network inventory, is identified for clustered fault tolerance testing. During this part of the test, all power to one redundant node on each of the identified switch stacks is physically pulled in order to test network redundancy. Dual power is then restored to each node after all observations, fixes and follow-up action items are documented. After all monitoring systems show full network restoration, the last part of the test, enterprise storage head failover testing, can begin.

During the storage part of the test, power is pulled to each of the primary controllers on each production storage system, one at a time, to test automatic cluster failover. Again, observations are observed and recorded, along with any follow-up action items. Storage system logs are exported and saved for future discovery, should problems arise. After successful head failover is completed, a giveback operation is performed in order to restore control to the primary head.

As a result of these extensive annual data center redundancy tests, improper system configurations have been corrected, along with hardware and network connectivity mistakes. In addition, improvements have been made to build and provisioning processes to prevent future human-caused error. As a result, ABC has experienced significantly fewer unplanned outages year-over-year as a result of implementing these annual tests.

EMS SCADA EOC testing

ABC is also required to test its EMS SCADA EOC each year under NERC Reliability Standard EOP-008, Plans for Loss of Control Center Functionality. Requirements specify that a contingency plan be developed to include the following:

- The contingency plan shall not rely on data or voice communication from the primary control facility to be viable.
- The plan shall include procedures and responsibilities for providing basic tie line control and procedures and for maintaining the status of all inter-area schedules, such that there is an hourly accounting of all schedules.
- The contingency plan must address monitoring and control of critical transmission facilities, generation control, voltage control, time and frequency control, control of critical substation devices, and logging of significant power system events. The plan shall list the critical facilities.
- The plan shall include procedures and responsibilities for maintaining basic voice communication capabilities with other areas.
- The plan shall include procedures and responsibilities for conducting periodic tests, at least annually, to ensure viability of the plan.
- The plan shall include procedures and responsibilities for providing annual training to ensure that operating personnel are able to implement the contingency plans.
- The plan shall be reviewed and updated annually.
- Interim provisions must be included if it is expected to take more than 1 hour to implement the contingency plan for loss of primary control facility.

As part of the required annual plan test requirement, a simulated outage occurs and all EMS operations personnel physically move to the EOC with the goal of reestablishing operations within 1 hour. Full testing includes all IT hardware and software, either located at the EOC or required for isolated EOC operations, including staff workstations (EOC and Corporate), desk phones, closed-circuit wireless radio communications, logins and user profiles, access to required documents, printing, external communication links, and testing of EMS SCADA and other necessary operations applications, such as OMS and Real-Time Scheduling. Documentation outlining the test must be developed and maintained as demonstration to auditors of the annual requirement.

SOx 404 application recovery testing

As a public company with a market capitalization over \$75M, ABC must comply with Section 404 of the federal Sarbanes-Oxley (SOx) Act Section 404—Management Assessment of Internal Controls. In essence, SOx Section 404 (SOx 404) requires covered entities perform a top-down risk assessment in order to produce a set of internal controls to adequately address the risk of material misstatement for financial reporting. Since most companies use IT software and data to produce such financial reports, this software and data typically fall under a company's SOx 404 IT controls. If the production software and data are involved in an operational disaster scenario, companies generally have to demonstrate that recovery procedures are in place to ensure loss or unauthorized changes to the data do not take place and lead to material misstatement of financial reports. Overall, a formal written DRP which includes these recovery procedures is generally required for all SOx 404 covered entities.

As part of ABC's documented internal SOx 404 corporate IT controls, data recovery tests for financial applications are performed annually, and the recovered data are validated by comparing it to production data in order to ensure accuracy. During these annual tests, an alternating 50% of all SOx 404 applications are identified for testing every other year. For each half of SOx 404 applications identified in a particular year, a recovery test form is completed which documents:

- Date recovery test completed
- Recovery test participants
- Purpose and systems/application recovered
- Summary of recovery process, referencing established backup and recovery plans, and/or disaster recovery test plans that exist
- Explanation of validation process and results, including screen shots or other documented evidence of successful validation
- Follow-up items completed, such as DRP updates, recovery procedure updates, etc.
- Signatures by both staff who performed the recovery test and the Data Conservators (i.e., data owners) for the data in question

These recovery test forms are required to be kept for 5 years, and samples are supplied to ABC's Internal Audit department each year as part of annual IT control audit procedures.

NERC CIP-009 recovery testing

NERC CIP Reliability Standards require ABC to perform a number of BC/DR tests and documentation reviews each year under *Standard CIP-009—Recovery Plans for Critical Cyber Assets*. Cyber assets are defined as IT assets which communicate via routable protocols in order to control (noncyber) Critical Assets required to operate the Bulk Electric System. Specifically, ABC is required to:

- Annually review recovery plan(s) for Critical Cyber Assets, which (1) specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s), and (2) include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets; for example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.;
- Exercise the recovery plan at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident;
- Update recovery plan(s), as part of its change control procedures, to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates must be communicated to personnel responsible for the activation and implementation of recovery plan(s) within 30 calendar days of the change being completed;
- Annually test information essential to recovery that is stored on backup media to ensure that the information is available; test can be performed off-site.

For both the recovery plan exercise and backup media test, ABC holds annual meetings with cross-functional CIP operational areas to complete standard forms which demonstrate the annual exercises/tests occurred. For each CIP network, different Critical Cyber Assets are identified each year for testing. If any actual incidents occurred during the year which caused the Cyber Asset to have an unplanned outage, ABC documents actual recovery steps and ensures any lessons learned are incorporated into the existing recovery plan or associated asset recovery procedures. Otherwise, a tabletop exercise will be scheduled so that participants walk through a fictional incident and document roles, responsibilities, and tasks involved in a simulated recovery operation. Roles may include both internal staff and outside vendors, consultants, or other support staff. Acceptance (or validation) criteria, used to determine successful restoration, are documented. Procedures used to determine if acceptance criteria were met are documented. Evidence demonstrating acceptance criteria, such as screen shots, are inserted. Corrective actions, based on outcomes, are also documented. Finally, the recovery exercise is signed by all participants,

approved by management, both in advance of the exercise and upon completion, and archived for 3 years.

For the annual backup media test, ABC identifies different CIP Cyber Assets within each CIP operational area each year. For this set of Cyber Assets, a form is completed documenting test objective, acceptance criteria, initial conditions (i.e., state of the Cyber Asset prior to testing), sequence of events, duration, expected response, participants and evaluators, emergency termination conditions, test results (e.g., screen shots showing evidence of restored data from restored backup media, etc.), validation that termination criteria were met (i.e., Was the test successful or not?), corrective action needed (if the test wasn't successful), and any lessons learned.

If corrective action is needed, a corrective action plan is documented elsewhere on the form. Once again, management approves at two stages: after plan completion (before testing begins) and after acceptance criteria are documented (including any corrective action plan). Acceptance criteria can range from being able to read/restore configuration files for hardened devices, such as network switches or programmable logic controllers (PLCs), to the ability to read/restore system and data volume backup files/catalog for a database, application, or other type of server.

Enterprise business continuity testing

ABC has also begun tabletop companywide BC testing. It's first such test was set up as a recurring monthly meeting being led by the Risk Management department, with participation from the IS Department, Internal Audit, and business area management. ABC's objective in performing a tabletop BC test is to document and evaluate how the company would respond to a specific, limited disaster scenario so that it can begin to flesh out information that would go into a companywide BC/DR Plan. ABC's goal is to use these tabletop BC tests to interview company leadership, gather practical information, and continue process improvement. For its first BC test, participants started with a small isolated scenario, identifying a chemical spill at a nearby operations site as the fictional disaster to evaluate. As of the writing of the book, ABC said their first meeting was very "eye-opening."

Summary of scheduled BC/DR testing

In summary, it is clear BC/DR testing at ABC is not an afterthought. It is part and parcel of their operations and proof that they integrate ongoing BC/DR planning into their day-to-day operations. It is not simply enough to have a written plan. ABC proves the plan is working by documenting ongoing testing. By holding postmortem meetings after incidents occur, along with planned scheduled tests, and by documenting outcomes and lessons learned, ABC not only meets its regulatory requirements, but, more importantly, it evaluates and mitigates its ongoing risk and continuously reduces its exposure to significant loss from a disaster. For more information on testing, training, and auditing BC/DR plans, visit [Chapter 9](#) in this book.

SUMMARY OF BEST PRACTICES AND KEY CONCEPTS

In this chapter, we looked at how one company operating in the energy/utility sector, ABC, has approached BC/DR planning through (1) integrating BC/DR requirements into IT Governance, (2) improving BC/DR risk mitigation and recovery strategies, and (3) improving BC/DR testing.

The discussion was not an exhaustive review of all BC/DR planning activities described in this book (or in use by ABC), but simply a starting point and a discussion of key initiatives at ABC which moved the BC/DR planning dial in a big way. The takeaway from this is that BC/DR planning efforts can (and should) be integrated into your daily operations regardless of whether or not you have executive support for a formal BC/DR project plan.

Key best practices we discussed were:

1. In the absence of a formal BC/DR plan or policies, ask about BC/DR requirements when new projects or request for new IT resources is made, and document results in a formal BC/DR requirements document.
2. Ensure BC/DR requirements, separation of duties, and step-by-step application recovery procedures are fully documented before new IT infrastructure goes into production.
3. Determine a process for establishing service level tiers, to include availability objectives and RTOs, for applications based on documented business disaster recovery requirements.
4. Centralize BC/DR disaster recovery documentation, back it up off-site, and give it to key IT personnel to take home with them on DVD or flash drive media.
5. Use existing (or establish) change control process to make risk mitigation improvements, such as security control testing, security control baselines, security control change detection, and postmortem incident reviews.
6. Improve reliability for critical data center, network, enterprise storage, or other shared infrastructure by designing for fault tolerance.
7. Employ server virtualization and a shared storage infrastructure, where possible, to improve risk mitigation and recovery outcomes.
8. Establish formal procedures for both network and server infrastructure vulnerability assessments, both as part of infrastructure build procedures and during periodic network vulnerability assessment testing.
9. Integrate BC/DR testing activities into your day-to-day operations, including formal incident postmortem meetings and regularly scheduled redundancy and recovery testing.

References

Stouffer K, Falco J, Scarfone K. Guide to Industrial Control Systems (ICS) Security. Gaithersburg, MD, USA, <http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf>; 2011 [Retrieved May 25, 2013].

Risk Assessment

4

IN THIS CHAPTER

- Risk management basics
- Risk assessment components
- Threat assessment methodology
- Vulnerability assessment
- Summary
- Key concepts

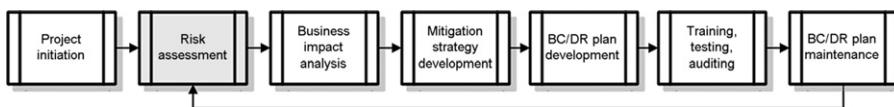
INTRODUCTION

In this chapter, we're going to discuss the concept and practical application of risk management. We'll look at the broad business perspective, the practical business continuity and disaster recovery planning perspective, and the IT-centric perspective. We'll look at risk *management* to understand the overall process then delve into the risk assessment process. This is where the first phase of project work begins.

Creating a business continuity plan unique to your operation is critical for your success. Each organization will handle potential threats and associated risks differently. Each company will have to take into account the location, industry, organizational culture, company structure, departments, work units, management approach, and strategic objectives. Each of these elements impacts how your organization responds to threats. For that reason, a very important step in this process is performing the risk assessment. IT risk assessments can also support a variety of company-wide risk management activities including:

- Development of an IT infrastructure architecture
- Development of an IT security architecture
- Definition of interface requirements for IT functions (how IT interconnects to other business areas or functions)
- Implementation and maintenance of security solutions

As you can see in [Figure 4.1](#), we've completed the basic project initiation steps (see [Chapter 3](#)) and we're moving into risk management. Clearly, we can't create a viable BC/DR plan until we know which specific threats the company faces. Every company faces numerous common threats such as the potential for a server failure or power outage; but each company also faces numerous threats that are either unique to

**FIGURE 4.1**

Business continuity and disaster recovery project progress.

the organization or unique in the potential impact. Throughout this chapter, we'll discuss risk management from a BC/DR perspective, but there may be risks your business faces that are not mentioned. In [Chapter 1](#), we provided a list of potential threats to be addressed, but the list is not exhaustive and you'll need to look at your own business with other knowledgeable members of your company to determine what risks you'll need to assess. We'll cover many of those threats in more detail in this chapter. It should serve to prompt you to think about these events in light of business continuity and disaster recovery planning processes.

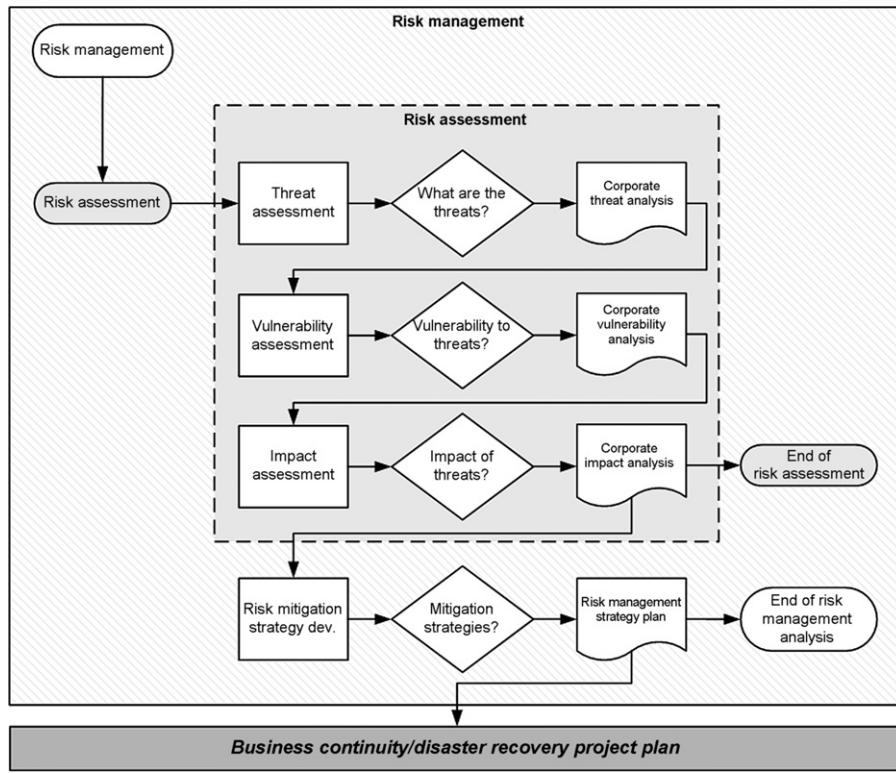
One of the common objections to BC/DR planning is that there are just too many things that could go wrong to plan for them all. That's partially correct—there are thousands of things that *can* go wrong, but fewer things that actually are *likely* to go wrong. You should certainly create a plan for things that are *likely* to go wrong. However, even things that are *unlikely* to occur should be reviewed and accounted for due to their potential impact.

Let's use driving to work as an example. There are hundreds, if not thousands, of threats to you as you drive to work each day, but you still took some basic precautions to reduce, remove, or avoid certain risks. So, while it's not likely you'll get in an accident driving to work, you planned ahead to reduce your risk. First, you probably took a driver's education class when you were learning to drive, so you could learn the basic rules of the road. That's risk reduction. Second, you probably obey traffic controls such as stop signs and signal lights. That's another risk reduction strategy. Third, you probably have car insurance so that if something does go wrong, you won't face exorbitant costs related to repairing the car. That's a risk transference strategy. Still, it doesn't prevent someone from plowing through a red light or losing control of their car going 75 miles per hour on the highway. So, you've done what you can to reduce your risks and you also realize there are risks that you can do nothing about. The only way to take your risk profile to zero would be never to go in a motorized vehicle anywhere and never to go near roadways containing motorized vehicles. That's not a very practical solution. It may be effective, but it is neither feasible (for most) nor desirable as a risk mitigation strategy. Just because you can't manage all the risks involved with driving a car, it doesn't stop you from getting in your car and driving to and from work 5 days a week. You can't control all the risks, but most people will still do what they can, within reason, to limit their risks—like take a driver's education course, follow traffic laws, and buy insurance. So, it makes sense to try to address the risks we can in business, recognizing there will be risks we do not or cannot address.

We'll also discuss risk concepts including *avoidance*, *reduction*, *acceptance*, and *transference* of risk. These are four general methods that can be used to manage risk, and we'll discuss how these apply to your BC/DR planning process. We'll look at the risks to your company and to your IT operations to help you determine which are acceptable, which must be mitigated (reduced or avoided), and which can be transferred, all within the constraints unique to your company. Risk management must fit within the financial and time constraints of the company to be viable; in other words, they must be reasonable. When you finish reading and absorbing this chapter, you'll have information you can use to go back to your executive team to gain support for your BC/DR project if you've been unable to gain that thus far.

RISK MANAGEMENT BASICS

Risk management is a general topic that looks at how all risks are managed across the enterprise. The number and type of risks companies face in today's world are many and varied. For example, companies face risks to the value of their company through gyrations in the stock market, they face shareholder lawsuits for mismanagement of the company, and they also face risks based on currency fluctuations in an international trading environment. These are just three risks companies face with regard to the value of the company. The value of the company impacts its ability to raise additional capital, the interest rates it receives on loans, and the rating of any bonds the company may try to issue (or has issued). This is just one type of risk management focused on financial risks to publicly traded companies. Let's look at some other types of risks. There are risks associated with union contracts, labor agreements, or outsourcing agreements. There are risks associated with products such as product tampering, product malfunction, product contamination, or product failure. These are risks companies face related specifically to the products they make or sell. There are risks to loss of life associated with utility companies, healthcare companies, and certain industries. We're not going to delineate every possible risk a company could face nor are we going to have an in-depth discussion of risk management here. However, it should be clear to you that risk management is a large undertaking at any company. There are risks beyond business continuity and disaster recovery that your company is likely aware of and has probably already addressed. There are three key aspects to any risk assessment methodology, which we'll cover in this chapter. First is the risk assessment process—how you go about performing the assessment. Next is the assessment approach—will you opt for a quantitative, qualitative, or semiquantitative approach? Each approach has an appropriate use, but you'll need to select an approach and use it consistently. Finally, your analysis approach will need to be determined. Do you want to look at your risk from a threat orientation, an asset/impact orientation, or a vulnerability orientation? You could use all three or a combination, but selecting, documenting, and then using a consistent method is important if you want to end up with a reliable plan.

**FIGURE 4.2**

Four basic risk management steps.

Let's begin with looking at the risk management process visually. [Figure 4.2](#) contains a flowchart that indicates the four basic steps in risk management:

- Threat assessment
- Vulnerability assessment
- Impact assessment
- Risk mitigation strategy development

We're going to focus on threat and vulnerability assessment later in this chapter. In the next chapter, we'll discuss the impact assessment process in more detail, though we will mention it throughout this chapter as appropriate. In [Chapter 6](#), we'll discuss risk mitigation strategy development in detail, but again, we'll also touch upon it as we discuss threat and vulnerability assessments in this chapter. As you can tell, these four areas are intertwined and it's difficult to discuss one aspect without also touching upon the others. However, we'll save our in-depth discussions of impact assessment and mitigation strategies for later chapters.

We've used shading in [Figure 4.2](#) to indicate the general boundaries of risk assessment versus risk management. However, we're far less concerned with the boundaries than the actual work products. In each of the phases, there is an assessment and an analysis that should result in a report or written document. This helps you move from one phase to the next in an orderly and coherent manner. You can also use these phases as part of your Work Breakdown Structure to delineate tasks, deliverables, timelines, and deadlines. Let's begin with a brief look at each of these four areas just to be clear about definitions and boundaries.

REAL WORLD

Risk Management Certification

If you're interested in risk management, there are numerous opportunities for professional growth through education and certification. One such certification is the Certified in Risk and Information Systems Control from ISACA ([ISACA CRISC, 2013](#)). Formerly known as the Information Systems Audit and Control Association, ISACA now goes by its acronym only. The SANS Institute also provides a course in Risk Management and a certification track (Global Information Assurance Certification; [GIAC, 2013](#)). There are also numerous other non-IT risk management certifications available. They range from general business risk management to very specialized financial and insurance risk management functions. If you're interested in risk management, it will serve as an excellent foundation for career growth in your IT career.

Risk management process

The process of managing risk includes assessing potential and also analyzing the trade-offs or opportunity cost. Imagine a company that says we need to make sure our systems *never* go down. The potential for systems to go down occasionally is very high; most systems go down for one reason or another from time to time. The cost of those system outages varies, usually in direct correlation to the time the system is down and whether the downtime is planned or unplanned. If the system is down for 10 minutes while it's rebooted due to an emergency patch installation, the cost may be negligible. If the system goes down for days because the database is corrupted by a hacker and restoring back to the previously validated database data experiences a few problems, the cost is much higher. Now, let's offset that with the opportunity costs. If we spend \$5000 on various systems to keep that server up and running, that's \$5000 we *couldn't* spend on something else, such as marketing materials, advertising, or employee wages. In addition, there's the cost of the downtime versus the cost of the solution. What does 1 hour of downtime for that server cost your company in lost sales, lost productivity, lost reputation, or lost consumer confidence? That's the opportunity cost of downtime.

The point is not to get into a detailed financial discussion regarding business costs but to understand that for every activity that occurs, some other activity cannot occur. For every dollar spent doing something, that dollar cannot be spent doing something else. Clearly, if you have \$50 left at the end of the week, you can only spend that \$50 once. If you choose to spend that \$50 on dinner and on the movies, you cannot also spend that \$50 on the latest electronic gadget. Every choice made excludes other

choices not selected. Understanding opportunity costs within the risk management process is important because you can't manage every risk to zero. In some cases, it simply can't be brought that low; in other cases, the opportunity cost of doing so is disproportionate to the benefit. These assessments require some level of qualitative assessment (an assessment made without hard data, a value judgment). Understanding all aspects of the decision-making process will help you and your team to make better decisions based on the unique requirements and constraints of your company.

Two other useful concepts in this process are *magnitude* and *frequency*. For example, an earthquake's impact to business operations would have a high magnitude, meaning the impact would be extreme. However, in many places, even those prone to earthquakes, the frequency is relatively low. California does experience fairly regular earthquakes, but the frequency of large earthquakes that impact business operations is relatively low.

Finally, each threat and potential mitigation strategy has a *cost* and a *benefit*. As we discuss various threats later in this chapter, we'll look at costs—in dollar figures and in the cost to human life and business operations. There's also the benefit of the mitigation, which ideally should more than offset the cost of the event. Let's look at a concrete example. The cost of installing fire suppression systems in a building may be \$15,000. Typically, fire suppression systems cost about \$5.00 per square foot; specialty fire suppression systems may run as high as \$10.00 per square foot. Compare the total cost of installation with the cost of a major fire in terms of (1) building damage, (2) equipment damage (desks, computers, carpet, decorations, files, records, inventory), (3) IT equipment damage, and (4) human injury and death. \$15,000 looks like an excellent investment because the cost of installing the system is far lower than the benefit it provides by way of risk reduction. These are the kinds of assessments you'll need to complete for your BC/DR plan. Let's look at each of the phases briefly, so you understand the framework for the entire risk assessment process.

Threat assessment

We've used the words "risk" and "threat" several times, almost interchangeably. Although this is correct in a general context, it's not quite accurate in a specific risk management context. *Business risk* is defined as:

The process of identifying, controlling, and eliminating or minimizing uncertain events that may affect businesses. It includes risk analysis, cost benefit analysis, selection, implementation, and testing of selected strategies, and maintenance of those strategies over time.

The key words here are *identifying, controlling, eliminating, or minimizing uncertain events*. Risk management is about trying to manage uncertainty. We can't ever completely remove all risk all the time, but we can find ways to reduce or eliminate many risks. The process of risk management is one of determining which risks should be addressed and how they should be addressed.

A more IT-centric view of risk management was defined by Joan S. Hash in the Computer Security Division of the Information Technology Laboratory at the National Institute of Standards and Technology (<http://www.itl.nist.gov/lab/bulletns/bltnfeb02.htm>):

Risk is the net negative impact of the exercise of a vulnerability, considering both the probability and the impact of occurrence. Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. The objective of performing risk management is to enable the organization to accomplish its mission(s) (1) by better securing the IT systems that store, process, or transmit organizational information; (2) by enabling management to make well-informed risk management decisions to justify the expenditures that are part of an IT budget; and (3) by assisting management in authorizing (or accrediting) their IT systems on the basis of the supporting documentation resulting from the performance of risk management. Risk management encompasses three processes: risk assessment, risk mitigation, and evaluation and assessment. (Hash, 2002).

Both business risk and IT-specific risk must be addressed using the same methodology; only the details will differ. We can use the following equation to define risk as well:

$$\text{Risk} = \text{Threat} + (\text{Vulnerability} + \text{Likelihood}) + \text{Impact}$$

Thus, risk could be viewed as the combination of the threat itself, the specific vulnerability, the likelihood of that vulnerability being exploited, and the relative or absolute impact of that threat on the organization or system. Vulnerability and likelihood are shown together in parentheses simply to indicate that some people prefer to assess these in one pass or as one value. Looked at another way, a vulnerability may exist in an operating system, but if you're running that operating system behind a firewall, the likelihood of that vulnerability impacting your systems may be low to zero. So, you can see the difference between vulnerability and likelihood and how you might assess these elements. Whatever approach you use, it is acceptable as long as you account for both factors in your equation. Although this might seem like splitting hairs, it's important to define these various elements so that we can discuss them at the level of detail needed to perform a thorough and meaningful risk assessment. We'll discuss *threats* and *threat sources* in depth later in this chapter.

Vulnerability assessment

The *vulnerability assessment* analyzes how vulnerable, susceptible, and exposed a business or system is to a particular threat. It should include an assessment of how *vulnerable* a particular system is to a threat as well as the *likelihood* of that threat occurring. The likelihood portion of the assessment can be a part of the vulnerability assessment, though you could also break it out as a separate process if desired. As long as your risk assessment includes vulnerability and likelihood assessments,

you should be in good shape. Clearly, it is useful to know that a system is *vulnerable* to a threat that has a 90% *chance* of occurring, a 50% *chance* of occurring, or a 1% *chance* of occurring. The vulnerability and the likelihood of the event are closely related, and the results are used as inputs to the impact assessment. Certainly, a server that is outside the firewall is far more vulnerable to external attacks than a server that is inside the firewall. This is an example of relative vulnerability as both servers are vulnerable but one more so than the other. How likely is it that either server will be attacked? Probably 100% for the server outside the firewall and perhaps 30% for the server inside the firewall in today's attack-laden environment. As you can see, creating relative assessments for vulnerability and likelihood results in different risk profiles for the two servers. We'll look at this in greater detail a bit later in this chapter.

Impact assessment

The *impact assessment* analyzes how great or small the impact of a threat occurrence will be on the business or system. An earthquake has an enormous impact on a business that is in or near the epicenter of the quake; it has a lesser impact on businesses further from the epicenter; it may have a slight impact on other companies around the country if infrastructure fails or if key suppliers or vendors are located in the region impacted by the earthquake. Therefore, impact varies based on numerous factors. Clearly, a fire contained to the lunchroom has a much lower impact than a fire that engulfs the entire building. We'll look at the impact of various threats in detail not only in [Chapter 5](#) but also in conjunction with our discussion of the risk assessment process throughout the remainder of this chapter.

Risk mitigation strategy development

We mentioned four distinct strategy types of risk mitigation earlier in this chapter. You can *reduce*, *avoid*, *accept*, or *transfer* risks. Each strategy comes with an associated cost. It's far more expensive in many cases to completely avoid a risk than it is to reduce the impact of the risk. Most businesses are more likely to build in state-of-the art fire suppression systems rather than construct a building with absolutely no flammable materials. The cost of building a completely fireproof building is far higher than installing a high-quality fire system. However, each company has to make that assessment. There are certainly situations in which building a fireproof facility is not only cost-effective, it may be the only viable option for a particular type of company.

Some risks are worth accepting. As we discussed in the introduction of this chapter, we all accept risks in our everyday lives. We drive cars, we cross busy intersections on foot, we eat unhealthy food, we buy high-risk stocks. These are all risk-laden activities but we accept these risks. We may find ways to reduce our risk such as obeying traffic signals when driving and crossing streets; we may limit our intake of junk food to some extent; or we may put 25% of our investment funds in a savings account. These are all attempts to reduce risk, but there is also an element of acceptance. It's like saying, "I'll accept 35% of this risk," meaning I'll obey traffic signals

but I'll still drive my car. You've accepted that even if you obey traffic laws, there's still a chance, albeit a smaller one, that you could end up in an accident.

Risk mitigation strategy development is the process of deciding which risks you should address and in what manner. The inputs to this are the risk assessment analysis or reports that delineate which threats exist, how vulnerable your systems are, and how likely the threat is to occur as well as the impact of these occurrences on your business. The compilation of these data will help drive sound business decisions because you'll be able to look at your entire risk profile and decide how to proceed. Since there are rarely perfect solutions in business, your job during this phase is to make intelligent decisions and trade-offs in light of the data collected. We'll discuss this in detail in [Chapter 6](#). For now, let's turn our attention to the risk assessment components.

PEOPLE, PROCESS, TECHNOLOGY, AND INFRASTRUCTURE IN RISK MANAGEMENT

Earlier in the book, we introduced the framework of “people, process, and technology,” as a framework that works well for IT projects. However, for business continuity and disaster recovery planning, a fourth category needs to be included: *infrastructure*. Although infrastructure is included in the technology category, there’s a tendency to look at technology from a hardware point of view—how many servers, how many spindles of storage, and how many desktops. To ensure that we also look at the underlying infrastructure, we’ve added that as a fourth element. You can bundle it back into technology if you want, but this way it will be clearly visible and on your radar as we proceed through our planning. As IT professionals, it’s relatively easy to look at technology and assess the various risks. It’s a bit more difficult to assess the risks to people and the processes they use to run the businesses, but it is part of normal IT project planning in most cases. Assessing the infrastructure, however, might be a bit out of the ordinary for IT planning, which is why we expanded our model to specifically include it. In BC/DR planning, the infrastructure, which includes the building and facilities of the company, the utilities to the building, and the external infrastructure such as transportation and utilities, must also be assessed. Let’s look at these four components using the earlier power outage example.

People

If the power goes out in the building, how likely is it that people will be able to get anything done? Many offices have no windows, so they’d be working with emergency lights that illuminate only exits and major hallways, for example. People will be distracted, they’ll be gathering around people’s desks discussing the outage, not focused on work. If the outage is from a storm outside, they may be concerned about getting home safely from work that day or the status of power at their own homes.

People respond in a variety of ways to small and large events. How the people in your company respond will be based on numerous factors including the kinds of work they perform, the types of people your company hires, and more. For example, if your company hires experienced medical personnel, they may respond well to emergencies. If you hire interns right out of high school, they will likely respond differently to emergencies. Looking at the employee population and understanding how they are likely to respond to small and large business disruptions will help in your planning. It also helps to look at the range of employees you have and the locations in which they work. Just stepping back and looking at your company's personnel from a disaster planning perspective can give you insights into how people might respond to an emergency and factors you may need to consider in your planning.

Process

What about the processes? Let's assume the power to the building is out. It doesn't matter if the server room has emergency power or not, does it? Users' desktop computers aren't available, and the software they use to get their jobs done is unavailable. If the company has any processes still done by people without technology, those processes can proceed but sooner or later, those processes will require computer data as input or output. In many cases, then, continuing with those few processes that are not dependent upon technology (or electricity in general) will cause systems to get out of sync. If materials are off-loaded from an incoming delivery truck and placed in inventory and paper inventory sheets, keep track of materials, quantities, and locations, which may help the delivery truck get back on the road, but it causes a problem on the other end. Now, there is inventory in stock that is not included in the last computer inventory count. Will that paperwork ever end up being input or will it take a cycle count in 3 months to discover the problem? This is a small example of how all business processes are impacted by this single threat, a power outage, even if the process isn't directly impacted by the threat.

Technology

Clearly, technology is the heart of operations in many companies today, especially those located in industrialized nations. Without technology, most things just come to a grinding halt. It's almost hard to understand the impact of technology on our lives until you're forced to do without. If the power's ever gone out in your home, even for a few hours, you suddenly realize you can't get on the Internet to get news, you can't update your stock portfolio online or on your desktop, you can't watch TV, you can't make a pot of coffee, you can't tell what time it is, you can't recharge your cell phone, and on and on. Yes, you can use your tablet if it has cell phone service activated on it, but that might be about it. Most people find their normal lives just come to a halt. We're at a loss because we've become so accustomed to having uninterrupted power $24 \times 7 \times 365$. Clearly, people living in areas where electrical service is less reliable are more aware of the impact, but they also have developed risk mitigation

strategies—they may have generators, battery backups, or solar power to their homes in order to offset that risk, for example, or they have simply designed their operations around these facts.

The important concept here is that technology is needed so that the *people* in the company can use the *processes* defined to conduct business. Technology, by itself, is a pervasive business tool, but it is most often useless without the context of people and process. As we continue our discussion of risk assessment, keep that fact foremost in mind. It will help as you look at risks to remember that there are four elements to be addressed with every risk: people, process, technology, and infrastructure. By incorporating this four-pronged view of risk, you can help reduce the chance that your plan will have any significant gaps.

Infrastructure

Infrastructure is sometimes included in the technology segment of “people, process, and technology,” but it’s useful in BC/DR planning to address it as a discrete category. Most IT professionals understand the term infrastructure from an IT standpoint, but from an organizational standpoint, it refers to things such as the building and facilities, the utilities coming into the building, and the external infrastructure such as public transportation, public utilities, communication services, and any other local, state, or national resources pertinent to your business. Corporate infrastructure typically is managed by the facilities manager or by someone assigned those duties, whether in finance, operations, or human resources. External infrastructure typically is managed, owned, controlled, or regulated by the local, state, or federal government. Within a BC/DR risk assessment, the risk to the company’s infrastructure from various threat sources must be evaluated and assessed. Risks to the external infrastructure must also be understood, though mitigation strategies will clearly differ for resources you control or own versus those you do not. In a natural disaster or serious external event, there are usually disruptions to external infrastructure components that have far-reaching effects, which are often underestimated in the planning stages. It’s difficult to realistically assess what will happen if a major freeway collapses or a nearby chemical plant explodes. Your business will have to rely upon local officials, including fire, police, and emergency medical staff, to address the external events. Your business will also need contingency plans with regard to your business operations in such an event.

IT-SPECIFIC RISK MANAGEMENT

Risk management across the business enterprise is a wide and varied topic, as you’ve seen. IT-specific risk management is a subset of overall business risk management. That said, there are some very unique risks in IT that exist nowhere else in the enterprise. These include developing technical, physical, administrative, and management standards and processes for protecting the confidentiality, integrity, and availability

(CIA) of information across the enterprise. IT risk management must balance the organizational needs for technology (especially availability) with current technological capabilities and costs. Just about every risk can be mitigated with large expenditures, but the objective of risk management is to reduce risks in the most cost-effective manner possible. If money were no object, risk management would take on a whole different function.

Keep in mind that most medium-to-large organizations have a formalized risk management program that encompasses more than just IT. Unfortunately, it is not uncommon for those enterprise-wide programs to overlook or minimize key elements of IT risk management. Many risk management programs for large companies were developed decades ago and have not been updated to include current IT risks and associated management or mitigation strategies. As a result, you may find that your company gives little attention to mission-critical IT risk management functions. Part of your job as an IT leader is to ensure that the organization understands IT risks and supports efforts to mitigate those risks.

For example, your finance department may be aware of risks related to credit cards, but they may not be well-versed with regulations for Payment Card Industry (PCI) security compliance. Though your company may accept credit cards only occasionally or in only a few locations, you are required to maintain compliance with PCI. Alternatively, they may be aware of the need to be PCI compliant but have no idea how to achieve that objective. These are all elements of IT risk management that extend beyond the walls of the IT department and which have broader organizational implications.

TIP**National Institute of Standards and Technology Resources**

The U.S. Department of Commerce has a division called the National Institute of Standards and Technology, often just referred to as NIST (rhymes with mist). This federal resource is chock full of information on technology from risk assessments to managing access control lists to managing cloud-based security. If you're looking for reliable guidelines on managing information security, this is a great resource. You can begin at this URL and delve into topics that catch your attention: <http://csrc.nist.gov/publications/index.html>. Admittedly, you can go down a wormhole on this site, as there are so many different topics to explore, but if you're going to get lost online, this is a great place to do so ([National Institutes of Standard and Technology, 2013](#)).

IT Risk management objectives

Clearly, the greatest risk to IT is the data stored on and traveling across IT equipment. There are three needs with regard to electronic data: CIA (we discuss these three concepts in greater detail later in this chapter). Maintaining these three elements is the objective of IT risk management at its highest level.

More specifically, the objectives of IT risk management are to enable the company to achieve its strategic objectives by:

- Securing IT systems more fully
- Enabling management to make well-informed decisions with regard to the purchase and implementation of IT systems
- Enabling management to authorize (accredit) the IT systems on the basis of supporting documentation that results from the IT risk management activities

The system development lifecycle model

From these three objectives, you can see that IT risk management is a subset of overall risk management because the IT systems must enable the company to achieve its objectives in a secure and cost-effective manner. IT risk management ideally is incorporated completely into a company's system development lifecycle (SDLC) activities, which have five phases (the names for the steps may vary slightly depending on whether you're focused on the lifecycle of software development or hardware and application implementation):

1. Analysis/requirements
2. Design/acquisition
3. Development/implementation
4. Integration and testing/operations or maintenance
5. Disposal

In some cases, a system may be in several stages simultaneously. Regardless of the phase (or the terminology), the methodology for risk management is the same. As with project management, risk management is an iterative process. As you can see from the data in [Table 4.1](#), the phases and phase characteristics track closely with overall risk management and BC/DR planning activities ([Stoneburner et al., 2002](#)). For example, phase 1 is an assessment of risks and the development of requirements. Phase 2 is the development or acquisition.

REAL WORLD

SDLC Vs. Agile Methodologies

It's worth noting here that the SDLC framework, while still employed throughout hundreds of thousands of organizations worldwide, is slowly being replaced or supplemented by the Agile methodology. The SDLC waterfall approach is founded in predictable process, which drives quality results albeit more slowly than its more nimble cousin, Agile. On the other hand, Agile focuses on adapting rapidly to almost ever-changing requirements to drive quality results more quickly. Regardless of the methodology you choose, IT risk management should be incorporated into your process.

There are many excellent resources on IT risk management, and rather than go into more detail on the subject here, we'll direct you to these resources:

1. The U.S. NIST publications are available on the Internet at <http://csrc.nist.gov/publications>, including Special Publication Special Publication 800-30

Table 4.1 SDLC Phases

SDLC Phases	Phase Characteristics	Support from Risk Management Activities
Phase 1—Initiation	The need for an IT system is expressed, and the purpose and scope of the IT system is documented	Identified risks are used to support the development of the system requirements, including security requirements and a security concept of operations (strategy)
Phase 2—Development or acquisition	The IT system is designed, purchased, programmed, developed, or otherwise constructed	The risks identified during this phase can be used to support the security analyses of the IT system that may lead to architecture and design trade-offs during system development
Phase 3—Implementation	The system security features should be configured, enabled, tested, and verified	The risk management process supports the assessment of the system implementation against its requirements and within its modeled operational environment. Decisions regarding risks identified must be made prior to system operation
Phase 4—Operation or maintenance	The system performs its functions. Typically, the system is being modified on an ongoing basis through the addition of hardware and software and by changes to organizational processes, policies, and procedures	Risk management activities are performed for periodic system reauthorization (or reaccreditation) or whenever major changes are made to an IT system in its operational, production environment (e.g., new system interfaces)
Phase 5—Disposal	This phase may involve the disposition of information, hardware, and software. Activities may include moving, archiving, discarding, or destroying information and sanitizing the hardware and software	Risk management activities are performed for system components that will be disposed of or replaced to ensure that the hardware and software are properly disposed of, that residual data are appropriately handled, and that system migration is conducted in a secure and systematic manner

Source: Stoneburner G, Goguen A, Feringa A. NIST Special Publication 800-30, "Risk Management Guide for Information Technology Systems." Recommendations of the National Institute of Standards and Technology; July 2002, p. 5.

Revision 1, “Guide for Conducting Risk Assessments” ([National Institutes of Standards and Technology, 2012](#)).

2. Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE). OCTAVE provides best practices for evaluating IT security. It was developed by the Computer Emergency Response Team at Carnegie Mellon University. [www.cert.org/octave](#) ([Carnegie Mellon Computer Emergency Response Team, 2013](#)).
3. Control Objectives for Information Technology was developed by IT auditors, and it provides a framework for assessing IT security, developing performance metrics, and monitoring performance over time. [www.isaca.org/cobit.htm](#) ([ISACA, 2013](#)).
4. Common Criteria (International Standards Organization, ISO) 17799. These criteria represent the international standard for testing IT security systems.

Information about the criteria can be found at [www.commoncriteria.org](#), and a copy of the criteria can be purchased from ISO at [www.iso.org](#) ([International Organization for Standardization, 2013](#)).

Other helpful Web sites include:

- Computer Security Institute: [www.gocsi.com](#) ([Computer Security Institute, 2013](#))
- SANS Institute: [www.sans.org](#) ([SANS Institute, 2013](#))
- Center for Internet Security: [www.cisecurity.org](#) ([Center for Internet Security, 2013](#))
- Computer Emergency Response Team: [www.cert.org](#) ([Carnegie Mellon Computer Emergency Response Team, 2013](#))
- NIST: [www.nist.gov](#) ([National Institutes of Standard and Technology, 2013](#))
- Computer Security Resource Center: <http://csrc.nist.gov> ([National Institutes of Standard and Technology, 2013](#))
- ISACA: <http://www.isaca.org> ([ISACA, 2013](#))

The IT risk assessment process intersects with business continuity and disaster recovery planning risk assessment in that we need to evaluate the various risks (including, but not limited to, security) to the company and the IT systems in the larger risk arena. However, the goals are the same: to enable businesses to meet their strategic objectives. Clearly, being in business after a disaster or major business disruption is an objective of every organization.

Identifying risk for IT systems includes two major components: systems and operating environment. The systems data include but is not limited to:

- Hardware (servers, storage, network core, routers, firewalls, desktops, printers, telephones)
- Software (OS and applications)
- System interfaces (internal, external connection points)
- People who support the IT systems
- Users who use the IT systems
- Data, information, and records
- Processes performed by the IT systems

- System's value or importance to the organization (system criticality)
- System and data sensitivity (confidential, trade secret, medical data, etc.)

The operating environment data can include:

- The functional requirements of the IT system
- The technical requirements of the system
- Users of the system
- Security policies (company policies, industry, regulatory, governmental requirements)
- Security architecture (to assess vulnerability to cyber threats)
- Level of protection needed for CIA
- Current network topology, network diagrams
- System interfaces, information flow diagrams
- Data storage protection
- Technical controls (added security products, identification requirements, access requirements, audits, encryption methods, etc.)
- Physical controls (access control, monitoring, etc.)
- Organizational controls (policies and procedures defining acceptable methods and behaviors)
- Operational controls (backup policies and procedures, personnel security, system maintenance, off-site storage, or computing capabilities, etc.)
- Environmental controls (power, temperature, humidity)

These items are included to give you additional insights into the areas you'll need to investigate throughout your risk assessment phase. Some items may not be relevant to you, and you can delete them from your list. You and your team may have other items not listed that you want to include. It's better to be inclusive at this juncture. You can always pare down your list later, but if you trim it down too early in the process you may miss critical threats, threat sources, and vulnerabilities.

RISK ASSESSMENT COMPONENTS

The risk assessment process is shown in the shaded area in [Figure 4.2](#) earlier. There are three distinct steps defined in the preceding section. So, let's begin with a discussion of *threats* and *threat sources*. If you look up the definition of threat and threat source, you'll see pretty much the same or very similar definitions. In this book, we're likely to use the two terms interchangeably as well. However, it is worth noting the distinction just to help clarify the risk assessment process.

A power outage threatens just about every business. The threat, then, is a power outage. However, the threat source is where the power outage comes from. For example, power outages can occur when ice storms break power lines, when transformers are struck by lightning or when substations or the power grid itself experience some major failure of the power infrastructure. These are all *threat sources*—where the

threat actually comes from. Does this matter? Well, in general discussions of threats, it's often not very useful to discuss a threat source separate from the threat. Most of the time, we simply discuss a power outage. However, in BC/DR planning, understanding the *threats* and *threat sources* can help you uncover potential risks to your company or IT systems about which you were previously unaware. If we discuss a power outage in a general manner, you might think about power going out to the server room or even power going out to the building. If you fail to consider the possibility of power going out because a train derails and wipes out a nearby substation, have you adequately addressed the threat? That's a judgment call in many cases. The likelihood of a train derailing and wiping out a nearby substation has got to be pretty low on the likelihood scale, unless, of course, there are 90 trains per day, and the substation is adjacent to the tracks.

REAL WORLD

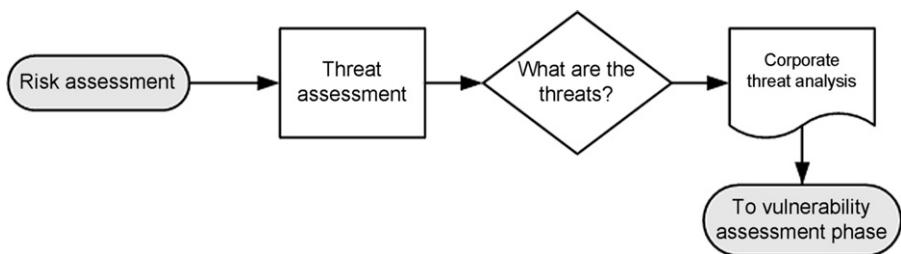
Threat Sources Change the Game

It's worth noting here that some threat sources are important to evaluate independent from threats. A power outage in the data center is an excellent example. The cause of the power outage will drive numerous other assessments. When looking at what is likely to occur in your area, threat sources can be crucial. For example, if power is out because of a powerful hurricane hitting the entire region, you have to have different plans in place than an area where power might go down but in a more localized fashion. If your company is located in areas where hurricanes, tropical storms, or earthquakes routinely occur, you're much more likely to have identified several threat sources related to power going out than companies in other areas of the country. Keep this in mind as you differentiate *threats* from *threat sources* because in some instances, threat sources change the entire landscape of your assessment.

As you can see from this one example, there is no one set of threats that will fit every company. In the following sections, we're going to discuss threats and threat sources, but it is certainly not going to be a comprehensive list. We'll get you started in this assessment, and you'll need to add details unique to your company and your geographic location(s).

Figure 4.3 shows the steps in the threat assessment segment. This is a subsection of Figure 4.1 shown earlier.

The risk assessment begins with the assessment of all potential threats and an analysis of those threats. The output from this phase is the input to the vulnerability assessment phase. Some companies may choose to look thoroughly at each threat and create a full assessment of each threat (such as threat, vulnerability, and impact for power outage or flood). However, it's advisable to create a detailed threat assessment first. If you get caught up in the details of looking at a specific threat before all threats have been delineated, you may waste time and resources planning for the wrong things. You may only be able to see the relative risk of various threats once the entire list has been created. Be sure to keep this in mind and focus on generating a comprehensive threat assessment before moving into the vulnerability assessment phase. Otherwise, you risk rework, errors, and gaps in your final BC/DR plan.

**FIGURE 4.3**

Threat assessment subprocess.

Information gathering methods

There are numerous methods you can use to gather data about your company's risks. Some of the methods are described briefly in this section. If you have preferred methods or a process unique to your company, feel free to use those as well.

- 1. Questionnaires.** Standardized questionnaires can elicit data from specific groups or individuals. Questionnaires can help limit input and feedback to those areas most useful.
- 2. Interviews.** Interviews with subject matter experts can be extremely helpful in uncovering needed information. This process is particularly helpful when you have subject matter experts who cannot or should not participate on the BC/DR team but whose input is vital. Interviews can be conducted using the questionnaire instrument to help direct and focus the interview. However, sometimes a more freeform interview can yield more information.
Questionnaires often contain unintentional biases and allowing an interviewee to discuss the topic without the constraints of a questionnaire can often yield data that might otherwise have been missed.
- 3. Document reviews.** Reviewing corporate and organizational documents can help identify threats, threat sources, and vulnerabilities. These documents may also be extremely helpful in understanding the company's current critical processes and functions so that systems can be properly prioritized later in the process.
- 4. Research.** Internal and external research can be extremely helpful and often is needed to round out the data collected. Your team can gather reams of data on the frequency and likelihood of storms, earthquakes, or other natural events from a variety of governmental resources (many of which are referenced throughout this chapter). Your team can also gather data from local fire departments, police departments, and other local organizations. Finally, there may be a lot of data about past business disruptions or events archived within the company that may be helpful in understanding threats, threat sources, and vulnerabilities to things such as break-ins, thefts, utility outages, process failures, or cyber crimes to name just a few.

These four methods should yield the data that you need to use as input to your assessment. However, it should be clear that these four methods could also yield reams of data, some (or much) of which might be useless or off-target. Before launching into your threat assessment, you should decide how to limit your data gathering efforts so that relevant data are most likely to be gathered. Review your questionnaires and interview questions to be sure they are focused and targeted on risk assessment for business continuity and disaster recovery planning. Limit your review of documents and research to those items specifically related to BC/DR. Although this might sound obvious, it is sometimes overlooked in the desire to avoid gaps or omissions in the planning process. Information overload happens quickly, so be sure to clearly define what data you're collecting so you don't end up sifting through reams of irrelevant information.

Natural and environmental threats

We've chosen to divide threats into natural threats—those caused by natural phenomenon and found in the environment—and human threats—those caused by humans either intentionally (including terrorism) or accidentally. Natural or environmental threats occur everywhere, but there are certain geological boundaries that determine whether you're more likely to experience a tornado or a hurricane, an electrical storm or an ice storm. We'll review some of the major threats and discuss business considerations. We'll also point you to a few resources that might be of interest or assistance to you and your team as you perform your risk assessment. The information contained in the following sections is intended to expand your understanding of these threats as well as to spark thoughts on how these events may relate to your business operations. Read it thoroughly or skim through it, but be sure to review so you don't miss any threats that might impact you and your IT shop at some point in the future.

Before we delve into the details of various natural and environmental threats, let's remember that these threats impact *people, process, technology, and infrastructure*. Though you'll undoubtedly take a very IT-centric view of these threats, you should also ask how these threats will impact the people, processes, technologies, and infrastructure of your business.

Fire

We've listed fire first because it is the most common disaster businesses have to deal with. Each year in the United States, fire causes thousands of deaths and injuries and costs billions of dollars in property damage. Fires are caused by a wide range of events (threat sources vary), some of which are intentional, some accidental, and some environmental. Intentional fires come under the banner of arson and we'll discuss arson a bit later (and arson, itself, can be classified as "intentional" or "terrorism" depending on other factors).

Fires cause injury and death to people, but fires also cause damage to buildings, systems, and corporate records. If your firm does not already have a fire response

plan in place, you should start your fire threat assessment by setting up a meeting with your local fire department representatives. It is important to understand what can and cannot be expected from the fire department in terms of fire and emergency response in your area. While it may really be outside the scope of your job in IT, it may someday impact your department, so if you don't have a plan in place, start by creating one for the IT department. It's helpful to have the fire department do a walk through to help you identify and remove (or reduce) fire risks. In some cases, this type of walk through is required by law before a business can occupy a commercial building. However, many times, it is not required or things within the facility may have changed significantly since the inspection. Be prepared for the fire inspection to yield negative results. This may impact business operations in the near term. For example, if there is a serious and imminent fire danger in your building due to improperly stored chemicals, the fire department may require the building be evacuated and locked until proper fire protections and practices are in place. If you suspect there are significant fire hazards in your facility, you should speak to senior management about it to get the situation resolved as quickly as possible. However, if you feel the danger is that serious, don't wait for a meeting to occur, take appropriate remedial action.

Clearly, most companies do not have conflagrations waiting to happen, so you will usually get solid recommendations from your fire inspector or perhaps a few minor violations to correct. You'll learn a lot about how fires start and how they should be contained by talking with your local fire crew. You can also find out how to develop fire drills and safe fire evacuation procedures, if those are not already in place.

If you're in a small company, you may also wish to contact your insurance carrier (or have the appropriate person in your company do so) to learn about fire prevention and protection measures that make sense for the type of business you're operating. They clearly have a vested interest in preventing fires since the fewer fires you have, the more money they make. Insurance companies will typically provide information resources and, sometimes, free training to assist you in fire prevention and containment.

REAL WORLD

Insurance as Risk Mitigation

We'll cover this in more detail later, but having hazard insurance is a widely used and effective risk mitigation strategy. It's also often required by law. Purchasing appropriate levels and types of insurance transfers the *financial* risk to another entity, but it never transfers *responsibility*.

Most companies develop and practice fire drills and clearly post evacuation routes throughout the building. These practices *may* reduce the company's potential liability in the event of a fire with injury or death, but more importantly, they *will* reduce the likelihood of injury or death. Evacuation maps should be posted clearly,

and everyone should know the shortest route outside and the closest exits. Larger facilities may also assign crew leaders responsible for making sure their area is evacuated and taking a head count once outside. If you have fire equipment such as automatic fire doors, sprinkler systems, or fire extinguishers, make sure managers and supervisors are familiar with these systems and their use. You may choose to conduct training on emergency equipment such as fire extinguishers so that people have hands-on experience prior to a real emergency. If the first time someone attempts to use a fire extinguisher is during an actual fire, they may be unable to read or process step-by-step instructions. If they've run through it a few times in nonemergency situations, they have a better chance of using the fire extinguisher effectively during the emergency. Talk with your insurance company and local fire department to learn how to prevent, contain, and manage fires in the workplace.

With regard to IT systems, you should certainly see about having chemical fire suppression systems installed in your server rooms, though most current building codes will address this issue adequately. Servers that are sprayed with water from overhead sprinklers may have a higher risk of water damage than fire damage. Those of you occupying older buildings should consult with your facilities manager or fire inspector about what type(s) of fire suppression (if any) exists in your building and, more specifically, in your server room(s).

TIP**Assessing the Entire Landscape**

The cause of fires can be internal or external to the company. Several natural hazards can spark fires. Electrical storms, tornadoes, earthquakes, and drought can all cause fires to flare, so when you begin looking at fire as a potential threat to your company, also be sure to look at all potential threat sources. If you plan for an electrical fire in the building but neglect to address the potential for wildfires sparked by lightning storms or drought or the possibility that adjacent buildings may start a fire, you will have an incomplete risk assessment and leave your company vulnerable to those threat sources.

Floods

Floods are characterized by relatively high water flow that spills over the natural or artificial banks of a stream or waterway or that submerges land not normally below water level. External floods, like fires, can be caused by a variety of factors. Just to reinforce definitions used earlier, floods can be considered a threat, but the threat sources are many. Floods can be caused by:

- Heavy winter or summer rains
- Melting snow
- Swollen rivers (from rain, snow melt, broken dams, etc.)
- Broken levees or dams
- Tropical storms bringing water inland beyond normal levels
- Tsunamis (which can cause flooding of large areas after the initial wave hits)

- Extremely high tides (typically caused by tsunamis, hurricanes, and powerful storms)
- Broken water mains

Depending on your location, you may be able to identify additional flood threat sources. Floods are the most common of all natural disasters, so there's a good chance your company will have to deal with flooding at some point in time. Floods can impact the building, the equipment (desks, chairs, file cabinets, computers), records (paper and electronic documents of all kinds), and people (drowning, injury, shock, etc.). Floods can also cause power outages and destabilization of the infrastructure. For example, a flood can cause landslides or the ground beneath the building to shift or sink, causing a serious failure of the building structure (or serious risk of failure). Landslides of surrounding areas can occur when the ground becomes too saturated. Landslides and other ground shifts (called *subsidence*) can not only impact your building but also disrupt the transportation infrastructure, including airports, railroads, and roadways. Flooding can also cause buildings to become uninhabitable. Doors, walls, floors, and ceilings can warp or split. Dangerous and noxious mold of various types can proliferate in the right conditions.

In the United States, the federal and state governments have various agencies that provide information about the nature, severity, and frequency of natural disasters in various geographic locations along with information on preventing (when possible) or mitigating the impact of these events. They often provide excellent emergency management resources and, in some cases, free or low-cost training.

In many instances, buildings located in flood plains were built before modern flood plains were defined. In other cases, buildings are built and areas later become flood plains. Regardless, it's important to understand where the flood plains are in your area (if any) and how they might impact your business. This is most important for small and medium companies that may have moved into a leased facility. If you are not the owner of the building, you may not be fully aware of the flood risks in the area. Unfortunately, not all landlords are honest, and you might have inadvertently placed your business in harm's way. You might not discover it until your insurance carrier contacts you about flood insurance requirements or until you experience a loss and discover you have no flood insurance or that your insurance was voided due to your location in a flood plain.

As with fires, it's a good idea to understand the best routes out from the building and away from the area in the event of a flood. If you're going to shut down early due to heavy storms in the area, it's also useful to let employees know in advance which roads, bridges, under- or overpasses are closed and which routes out are best.

If you are subject to flooding, you can look at standards set by the National Flood Insurance Program, part of the Federal Emergency Management Agency, at <http://www.fema.gov/business/nfip/> (Federal Emergency Management Agency, 2013). Another helpful part of that Web site is the emergency response and recovery

area, <http://www.fema.gov/response-recovery> (Federal Emergency Management Agency, 2013).

The risk of flooding to your IT components follows the general flooding risks. Desktops, laptops, routers, switches, hubs, printers, and cabling are all subject to failure if exposed to water, whether the power on those devices is on or off at the time. In some cases, you might evaluate whether it makes sense to flood-proof your server room, though in most cases, the answer is likely to be no. If the rest of the building is underwater, paying to seal a server room may not be a good investment, but only you and your team can make that assessment. We'll look at business impact analysis (BIA) and risk mitigation strategies (and associated costs) in upcoming chapters.

Emergency lighting systems are useful in many types of emergencies—from fire to flood to power outages, so we'll list them once here as an item “strongly suggested” for a variety of emergencies. Does emergency lighting reduce your risk of these various threats? No, but it does reduce the overall risk of injury and death of your employees. The cost of installing these systems is relatively small, and if they prevent one serious injury or one death, it will have been an excellent investment. This is an example of the cost/benefit being extremely favorable—small cost, large benefit.

REAL WORLD

Never Assume . . .

Years ago, I had a client in Arizona who built a brand new facility and placed the computer room on the bottom floor. In looking at the floor plans, I noticed the bottom floor was below grade (below street level). I asked about the likelihood or potential for flooding and was told not to worry about it. The area never flooded; there were sump pumps built into the plan in the unlikely event of flooding. Fast forward about 2 years. There were unusually heavy summer rains, and the entire area surrounding this building was under a foot of water. As it turns out, the sump pumps didn't work, and the computer room was sitting in a couple of feet of really dirty water. Needless to say, the computer equipment was ruined, the company was unable to process any data at all, and they had to pay hefty fees to expedite replacement equipment to get them back up and running once the room dried out. The company survived that outage, but just barely. In retrospect, would they have built the computer room on the main level? It's impossible to say. They clearly accepted (or ignored) the risk of flooding. They clearly absorbed the cost of remediation (or their insurance company did) when it occurred. Was that a good business decision or a bad one? Only the management of that company can tell us. However, the takeaway is this: check your assumptions about what *can* and *cannot* occur and be very clear about what level of risk you are *really* assuming.

Severe winter storms

Much of the Midwestern and northern states in the United States experienced the severe winter storm dubbed “Nemo” in early 2013, and the southern and southeastern states often experience devastating tornadoes and hurricanes including Katrina and

Sandy (discussed in a later section). Severe weather is a fact of life and if scientists are correct, it appears the globe is in for more severe weather in the coming decades. Severe winter storms include substantial snow fall, strong winds, freezing rain, ice, and often freezing or subzero temperatures.

During heavy storms, people often can't get to or from work or they get stuck *en route*. Once at work, they may worry about their homes and families and be less productive. Driveways, sidewalks, and entries may become blocked or slippery and pose a hazard to people and vehicles. Technology can be affected by winter weather in the event that technology is exposed to the elements such as outdoor pumps, electronics, or mechanical devices that freeze and do not function.

Severe winter weather can disrupt a business by preventing it from opening for days at a time because no one can physically get to the building, employees, and customers alike. In some cases, employees may be able to work from home if systems in the building are still functioning. Unlike loss of power or loss of cooling, even if the heat in the building goes out, the servers and other IT equipment will continue to function normally and may enable some portion of the business to continue. For example, if you have Web servers, they may keep serving up Web pages, taking online orders, and tracking online orders, even if no product is leaving the warehouse. In other businesses, you may still be able to process data, develop software, deliver utilities, or manage manufacturing functions in other locations even if you can't access your own building.

In addition, extremely cold temperatures can cause pipes to burst, which can cause a variety of problems. The pipes that burst are typically those carrying water, but other pipes can burst potentially causing an environmental hazard (though this is less common). Freezing pipes can cause flooding, so the threat may be flooding but the threat source is a winter storm, something you might not immediately think about.

Heavy snow and/or ice can build up on roofs and walls, causing structural damage and collapse. In cases of very heavy snow, people may be unable to remove the snow (steep roofs or large areas such as warehouses) or there may simply be nowhere to shovel the snow, as was the case in upstate New York in February 2007 when parts of the area were dealing with over 12 feet of snow. (By way of comparison, though the storm named Nemo that hit February 2013 in the United States dumped 2-3 feet of snow on the northeast, it ranked just 16th in all time storm snowfall.)

If your company is located in a place where there is snow, ice, and cold temperatures, you may want to consider keeping supplies in the building in the event employees are unable to leave. This should include food, water, blankets, emergency medical supplies, batteries, radios, and possibly battery-powered televisions. Depending on the nature of your business, the location, and the climate, emergency power generators and portable heaters might be warranted. You should also arrange for snow and ice removal from driveways, parking lots, and sidewalks. Remember to clear snow and ice from emergency areas such as doorways, electrical boxes (main circuit panels, for example), and fire hydrants.

REAL WORLD**Winter Weather Warnings**

On March 3, 2007, the St. Cloud Times (Minnesota) reported that a warehouse roof had collapsed after heavy snow, the second such collapse in that storm. It also reported 911 vehicles off the road, 411 car crashes in a 12-hour period (6:30 PM to 6:30 AM), and 99 spin outs. Airline flights in and out of the area were delayed or canceled. And here's something you might not think about—the fire department was asking people to dig out hydrants in case of fire. When it's 20° below zero, fire is usually a welcomed thought, but if your house or company is on fire, you hope the fire department can find the hydrant before the building is consumed in flames. This is a great example of a risk that you might not think about beforehand but is obvious once it's pointed out.

One final word on winter storms—don't assume that just because you're located in a warm climate that you don't need to plan for winter storms. If you use suppliers, vendors, or contractors located in cold climates, they could be impacted by winter weather and that, in turn, could affect your business operations. Winter storms do sometimes impact warm climates, as well. Are they worth planning for? Probably not, but that's for you to decide.

Electrical storms

Electrical storms can occur any time of the year and in any climate, though they're most likely to be found during hot, humid summer months in the United States. There are an estimated 25 million lightning flashes in the United States each year. About 300 people are injured and an average of 66 people are killed each year in the United States due to lightning strikes. Lightning kills more people per year than tornados, on average, though they occur one or two at a time and are therefore less visible to the public than the death of, say, 60 people in a single tornado. Lightning can cause power outages, fires, damage to buildings, falling debris (trees, poles, etc.), and injury or death to people (and animals). High winds sometimes accompany electrical storms, and these can contribute to flying or falling debris, power outages (lines blown down or struck by falling debris), and structural damage to buildings as well.

REAL WORLD**The Positive and Negative Sides to Electrical Storms**

According to the National Oceanic & Atmospheric Administration (NOAA), a department within the U.S. Department of Commerce, lightning originates in certain types of clouds in the region of snow crystals, snow, and ice pellets. The motion of the storm causes the snow crystals to become positively charged and the snow and ice pellets to become negatively charged. The positively charged particles rise within the storm, while the negatively charged particles remain in the middle to lower portion of the storm. This difference of electrical potential can cause cloud-to-cloud lightning. In some cases, the negatively charged particles toward the bottom of the cloud create positive charges to form on the ground and in the immediate vicinity of the cloud. This increases the likelihood of cloud-to-ground lightning strikes. Not all lightning originates from the bottom of the cloud, however. When it originates from the top of cirrus anvil clouds, the lightning is called positive lightning. For more on lightning, electrical storms, and other weather phenomena, visit the NOAA's Web site at <http://www.noaa.gov/index.html>.

Electrical storms can cause power outages, but they also can cause power spikes, surges, and dips. Clearly, power that is too high or too low can damage a wide range of electrical equipment, including all IT equipment. During electrical storms, power to buildings may fluctuate. We're all aware of the damage a power surge can do to electrical equipment, but extended low power (brownout) can also damage electrical equipment. Many companies invest in uninterrupted power supplies (UPS) to provide either battery backup to equipment, which typically provides just enough power to allow for an orderly shutdown of equipment. Batteries must be tested regularly and replaced and a process for doing so should be part of your BC/DR plan, if you have battery backup. UPS systems can also provide failover power, which provides ongoing power for some extended period of time when equipment loses power. Usually, these systems rely on backup power generators that run on diesel or other fuel, so be sure that fuel is checked for backup power systems on a periodic basis. Checking the readiness of UPS systems should be part of normal IT operations processes, and a process for ensuring disaster readiness should also be incorporated.

Many UPS systems provide power conditioning as well. This serves to keep the power from surging too high or dropping too low. If you have these systems in place, you are already familiar with them. If you do not have them in place, a bit of research will help you determine the best solutions for your firm based on the variety of unique conditions and constraints. Clearly, you can spend a little or you can spend a lot—the benefits typically do track with the costs, but you'll have to make some intelligent trade-offs based on your company's needs.

TIP**Building Business Continuity and Disaster Recovery (BC/DR) into Everyday Tasks**

In [Chapter 3](#), we discussed the challenges some IT managers have with actually getting their organizational leaders to support and fund BC/DR activities. We mentioned the opportunity to add BC/DR activities into your standard operating procedures as a way to begin to provide some measure of protection for your firm. Let's use UPS systems as an example. We know that having UPS systems in place for core infrastructure is critical. Depending on how your facility is configured, having UPS systems in place to run core equipment (core network and e-mail, for example) during a brief power outage might make sense. If your building has backup generators, using UPS power to smoothly transition from normal to emergency power can mean the difference between continuous operations and an uncontrolled, very risky shutdown and restart. One strategy would be to add the cost of a UPS to each server or storage unit you purchase. Pretty soon, you'll have power backup options built into your infrastructure without having to get a specific project approved to do so. This is not sneaky or underhanded, this is how business runs. Of course, if you are strictly forbidden to spend funds related to BC/DR (and that would be a very strange circumstance indeed), then this is a way to incrementally improve your environment and protect the company's critical IT assets.

Drought

You might not think drought has anything to do with you or your company, but you might be surprised by some of the statistics. For instance, drought has a greater impact than any other natural hazard, and its costs in the United States alone are estimated to be between \$6 billion and \$8 billion annually. That impact probably doesn't directly touch most IT shops, but if you're in an industry that is highly reliant on water, it will definitely impact you.

According to the National Drought Mitigation Center at the University of Nebraska in Lincoln (UNL):

Drought produces a complex web of impacts that spans many sectors of the economy and reaches well beyond the area experiencing physical drought. This complexity exists because water is integral to our ability to produce goods and provide services. Impacts are commonly referred to as direct or indirect. Reduced crop, rangeland, and forest productivity; increased fire hazard; reduced water levels; increased livestock and wildlife mortality rates; and damage to wildlife and fish habitat are a few examples of direct impacts (National Drought Mitigation Center, 2013).

The impacts are environmental, social, and economic and can be widespread. Droughts impact businesses in a variety of ways, but many are long-term effects hard to predict or quantify. For example, areas experiencing prolonged drought may find populations shifting out of the area in search of employment or new opportunities. Natural population shifts (those not driven by drought or other natural hazards) can also impact water availability. The shift in the U.S. population toward the western and southwestern states including southern California, Nevada, Colorado, Arizona, and New Mexico, among them, has put enormous stress on water resources in those areas. So, while there may or may not be drought conditions in some areas, there are water resource problems in many areas that can have the same long-term impact as drought.

Clearly, if your company's business activities involve the use of or reliance on water as a resource, you need to look at local, state, and national plans for drought mitigation. Some of the indirect impacts of drought can affect a wider range of businesses beyond those that rely on forests, streams, and lakes, according to the Drought Mitigation Center at UNL:

Many economic impacts occur in agriculture and related sectors, including forestry and fisheries, because of the reliance of these sectors on surface and subsurface water supplies. In addition to obvious losses in yields in both crop and livestock production, drought is associated with increases in insect infestations, plant disease, and wind erosion. Droughts also bring increased problems with insects and diseases to forests and reduce growth. The incidence of forest and range fires increases substantially during extended droughts, which in turn places both human and wildlife populations at higher levels of risk (National Drought Mitigation Center, 2013).

Earthquake

The U.S. Geological Survey defines earthquakes in this way: “Ground shaking caused by the sudden release of accumulated strain by an abrupt shift of rock along a fracture in the Earth or by volcanic or magmatic activity, or other sudden stress changes in the Earth.” (U.S. Geological Survey, 2013)

Most people who live in earthquake-prone regions are well aware of that fact. They feel tremors from time to time and either have lived through minor or major earthquakes or have heard stories from those who have. However, you might be surprised to know how often small earthquakes occur. Figure 4.4 shows an earthquake map from the U.S. Geological Survey Web site taken in 2007. This is the historical view of earthquake activity for the United States (for a real-time map view, visit <http://earthquake.usgs.gov/earthquakes/map/>; U.S. Geological Survey, 2007). Clearly, earthquakes of small magnitudes happen frequently in many locations, and there’s no need to plan for those. However, it is vital to plan for disaster recovery in areas where large magnitude earthquakes are not uncommon. Parts of California

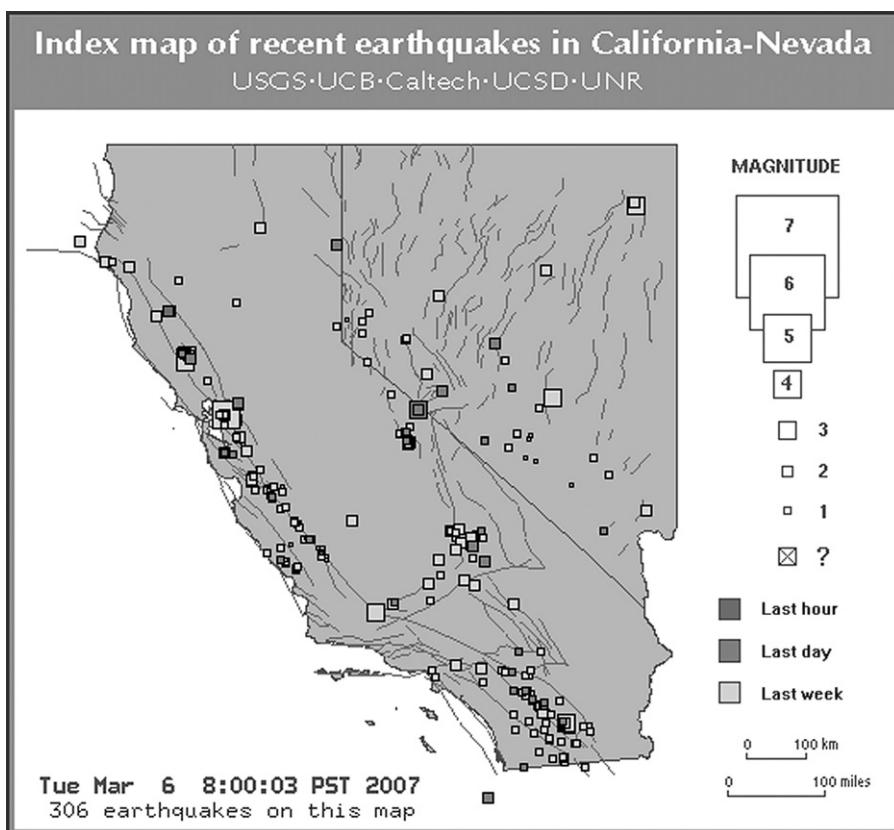


FIGURE 4.4

U.S. Geological Survey seismicity map.

and the Pacific Rim are most prone to large earthquakes, and companies in these areas no doubt have ample disaster planning. However, the extent to which IT is involved varies by industry and by company, so don't assume that IT is covered in your organization's plans unless you know specifically that it is.

Damage from a single earthquake can cause in the hundreds of millions of dollars, though clearly the large earthquakes have a lower frequency of occurrence than the smaller ones that cause little or no damage. That said, scientists estimate that there is more than a 60% chance of a damaging earthquake striking the San Francisco Bay Area of California before 2035 ([U.S. Geological Survey, 2005](#)).

Earthquakes can cause damage and have an indirect impact far from the epicenter of the quake. As witnessed in 2004, undersea earthquakes off the coast of Sumatra, Indonesia triggered a tsunami killing 230,000 people in Thailand. This is not the type of event you can ever fully plan for, but understanding your proximity to geographic risks can help you devise plans to address even these enormous events.

Although you may have earthquake preparedness plans in place if you live in an earthquake-prone region, you should review your preparedness in light of the most current data available for your area. There may be new regulations regarding building safety, hazardous material handling, and others that may impact your business. Though you may be aware of many of these, a quick review of the latest information and regulations related to your area and your firm can help reduce your legal risks even if they can't change your earthquake risks. If your company is not located in an earthquake region, you should still assess the potential for a large earthquake in your area and determine whether creating a preparedness plan for such an event would make sense. Also keep in mind that your business operations can be severely impacted by an earthquake that occurs elsewhere. Key Internet infrastructure and communication sites could be disrupted, causing Internet traffic to slow or stop. Communications and power infrastructure can fail, causing disruptions far beyond the immediate impact area. Supply lines, shipping routes, roadways, manufacturers, importers/exporters, suppliers, and vendors may all be impacted by an earthquake, so your preparedness needs to extend past the walls of your building and include an assessment of the risk your key business relationships face. We'll discuss this in more detail in [Chapter 5](#), but it's good to keep this in mind as you review these various threats. You'll continually need to "scan the horizon" to see how any of these threat sources might directly or indirectly impact your business operations.

TIP**Likelihood Vs. Impact**

Earthquakes are a good example of the need to balance the potential for a disaster with the frequency and impact of that disaster. An earthquake could be classified as a threat; the threat sources could be defined as shifting ground (subsidence), fire, gas leaks, explosions, infrastructure damage, building damage, structural failure (collapsing buildings, roadways, bridges), human injury and death, to name the most common of them. There are residual or longer-term threat sources from earthquake including disease outbreak, water shortages, water

Continued

TIP—cont'd

contamination, food shortages, food contamination, and even civil unrest. For more on earthquake maps, occurrence patterns and more, visit the U.S. Geological Survey's Web site at <http://earthquake.usgs.gov/hazards/about/basics.php>. There is an abundance of information on earthquake data from around the United States and around the world on this site. There are useful articles on earthquake preparedness that might be useful to those of you in earthquake-prone areas. Even if you've lived in an earthquake zone all your life, you will probably still learn a few helpful facts from a visit to the site.

Tornados

A tornado is a revolving column of dry air that occurs over land (unlike hurricanes, which originate over water and can spawn tornados). Tornados have been observed on every continent on the earth except for Antarctica, though the most tornados occur in the United States. Tornados are found most often in the central part of the United States, but hurricanes also can cause tornados in southern and eastern states as well. Wind speeds typically do not exceed 110 miles per hour, though some tornados have been observed with wind speeds in excess of 300 miles per hour, were more than 1 mile across, and traveled over a dozen miles on the ground.

Tornado damage usually is limited to the direct path of the storm, but the path of the storm is often extremely unpredictable. Like those who live in earthquake regions, most people know if they live in a tornado-prone area and have taken standard precautions. Tornados can disrupt businesses through physical damage to the facility, but it often has an even greater impact on the employees of a business whose homes may be destroyed or severely damaged by a storm that did not hit the business location. Employees will be worried about friends, neighbors, and family; they may lose their home or they may see their neighbor's home destroyed, causing severe emotional stress and trauma. People may be injured or killed, and emergency services may not be able to reach the victims in a timely manner or at all. Tornados can also destroy needed infrastructure including telephone poles, power poles, power stations, roadways, and even emergency services (the fire house or hospital could be in the direct path of a tornado, for example). Tornados, like earthquakes, hurricanes, and many other natural disasters, can damage the infrastructure to the degree that emergency service providers are unable to reach your location for hours, days, or weeks.

Emergency preparedness information is widely available, and you should be sure the information you have on how to prepare for and respond to a tornado is up to date. Again, keep an eye on the horizon and determine if any of your key business partners, suppliers, vendors, or customers is located in areas subject to tornados.

Hurricanes/typhoons/cyclones

Hurricanes are defined as “severe cyclones, or revolving storms, originating over the equatorial regions of the Earth, accompanied by torrential rain, lightning, and winds with a speed greater than 74 miles per hour” (U.S. Geological Survey, 2013). Of course, a revolving storm with winds of 65 miles per hour will also be devastating,

even if it is not officially classified as a hurricane. In the United States, we've grown accustomed to hearing about Category 3 or Category 4 storms. Hurricane Katrina was alternately classified as a Category 4 and Category 5 storm because the wind speed changed over time. Hurricane Sandy, which started out as a tropical cyclone, was classified as a Category 3 then downgraded to a Category 2 when it hit land. That didn't stop it from bringing commerce to a grinding halt for days after it hit in late October, 2012.

REAL WORLD

Superstorm Sandy

The storm dubbed Superstorm Sandy ultimately impacted 24 U.S. States, including the entire eastern seaboard and as far west as Wisconsin. The unusual storm surge hit New York City on October 29, 2012 causing flooding in streets, tunnels, and subway lines. Power was out in many parts of New York City and surrounding areas. Damage has been estimated at over \$50 billion USD. The question is this: If you were assessing potential disasters for an IT organization in Manhattan in 2012, would subway flooding have been on your radar? Probably not, but it is now. Is it likely to ever occur again? It's hard to say. Will you plan for something like this in the future? It will likely depend on your company, your industry, and the risks you identify through this process.

Regardless of the category or wind speed, hurricanes and tropical storms pose a significant threat to people and businesses (and more). Hurricanes bring destructive winds, torrential rain and flooding, storm surges of ocean water, and tornados. Hurricanes originate over warm ocean water but can travel across land and cause significant damage over coastal and inland areas. This was the case in several of the recent storms including Hurricanes Sandy, Katrina, Rita, and Wilma. More than half of the U.S. population lives within 50 miles of a coast, and this number is increasing every year. Many of these areas, especially the Atlantic and Gulf coast regions, are in the direct path of hurricanes.

TIP

A Storm by Any Other Name...

Cyclones, typhoons, and hurricanes are all the same weather phenomenon; the name changes with the geographic location. The term cyclone is used for many types of tropical storms but most typically is used for storms that originate in the southwestern Indian Ocean. Typhoons originate in the northwestern Pacific Ocean (Pacific Rim area), and hurricanes originate in the northeast Pacific or Atlantic Oceans. However, storms can cross various boundaries, so the actual terminology used is somewhat arbitrary. A tropical storm by any other name is just as devastating.

As with many other natural hazards, there is very little you can do to avoid the risk short of relocating to an area that is not subject to those kinds of risks. Unlike tornados that can be spawned without warning, most hurricanes are tracked long before

they hit land. Therefore, people often have the option of evacuating before the storm hits. As we saw with both Hurricane Sandy and Katrina, there were numerous problems with evacuation, including an underestimation of the strength of the storm, the inability of people to evacuate (gas shortages, traffic jams, etc.), or even the financial inability of people to make alternate arrangements (among other reasons). There is, of course, the problem with false alarms. The cost of evacuating, for individuals and businesses, is significant. Businesses have learned that they don't need to shut down for every hurricane that threatens their area, but that's a dangerous risk to take. If the speed, path, or strength of the storm is underestimated, lives can be lost. Therefore, your business leaders will need to assess the appropriate actions to take based on your company's type of business, location, and risk of hurricanes.

The cost to IT can be significant. Hurricanes bring high winds and rain, so power outages, flooding, and structural damage are the norm. If your building is destroyed by a hurricane, your IT resources are gone. How will you recover your operations in the face of total devastation? If you have a data center located elsewhere, you might recover far more quickly. If your backups were in a bank vault 2 miles away and the bank has been flattened, you might be out of luck. We'll look at the potential business impact of hurricanes in [Chapter 5](#).

Tsunamis

Tsunamis are defined as large destructive sea waves generated by earthquakes, volcanic eruptions, or large landslides. The tsunami that occurred in the Indian Ocean in December 2004 killed 230,000 people in 11 countries. It was a horrific example of the devastation a tsunami can cause. Though early warning systems do exist, they were not helpful in notifying people in the affected areas. Tsunamis have struck North America and the areas especially vulnerable are the five Pacific States—Hawaii, Alaska, Washington, Oregon, and California—and the U.S. Caribbean islands.

The United States has redoubled its efforts to improve early warning systems, and with the numerous communication channels now available to most people in the United States including TV, radio, the Internet, e-mail, instant messaging, land and cell phones, the likelihood of early warning is better than it was two decades ago. However, because 50% of the U.S. population lives within 50 miles of a coastline, there is also a good chance that evacuation routes would quickly become clogged if a metropolitan area such as Seattle or San Francisco needed to evacuate in advance of a tsunami warning. Therefore, it's vital for businesses in these areas to understand the potential risk and the mitigation strategies available to them. For more information on tsunamis, you can visit the National Oceanic and Atmospheric Administration Web site dedicated to tsunami research and information at <http://nctr.pmel.noaa.gov/>.

Volcanoes

Volcanoes are vents in the surface of the Earth through which magma and associated gases erupt. The shape of the volcano is made by the erupted material and typically forms a cone shape. Those living in volcano regions are well aware of the risks. Volcanoes, like other natural hazards, can occur with or without warning. However,

unlike hurricanes or tornados, volcanoes don't change locations. Though some inactive volcanoes may be forgotten or disregarded, they are known points in the Earth from which magma and gas can erupt. Planning for a volcanic eruption typically includes evacuation because the lava flow is unpredictable in its path and moves more quickly than most people realize. It is sometimes impossible to get out of the path of lava flow; sometimes it creeps slowly forward for days, and residents (and businesses) have time to collect their belongings and evacuate before watching the hot lava devour their house.

Businesses in volcanic areas should prepare evacuation plans and certainly be prepared for the possibilities that the building will be burned or covered by lava or that the ash that often accompanies an eruption could make the air and water hazardous. Ash particles are typically very fine and quickly clog filtration systems for water and air.

Avian Flu/pandemics

Let's start with some definitions. An *epidemic* is an outbreak of a contagious disease that spreads rapidly to a local population. A *pandemic* is defined as an epidemic that covers a very wide geographical area including entire regions, countries, or continents. According to the U.S. Centers for Disease Control (CDC), the Avian Flu does not *currently* pose a threat as either a potential epidemic or pandemic. However, the propensity of viruses to mutate creates some future risk of epidemic or pandemic outbreaks.

The Avian Flu (also called bird flu and referred by scientists as H1N1) has gotten a lot of press in recent years. The flu naturally occurs in bird populations, but in recent years, it has been seen in humans. Many wild birds carry the virus in their intestines but do not get sick from it. However, it is highly contagious, and domesticated birds are at high risk of contracting the virus, getting sick, and dying from it if they are exposed. There are numerous variations of the virus, and therefore, it is difficult to assess the risk to humans. Some strains have a low chance of infecting humans, others a much higher likelihood.

In the United States in 2012-2013, the flu outbreak across the nation had a significant impact on companies. While not always considered a "disaster" type of event, the cost of key employees being very ill and not able to work is a risk factor associated with flu outbreaks. According to the CDC ([Flu.gov, 2013](#)):

- A pandemic may come and go in waves, each of which can last from 6 to 8 weeks.
- An especially severe influenza pandemic could lead to high levels of illness, death, social disruption, and economic loss. Everyday life would be disrupted because so many people in so many places become seriously ill at the same time. Impacts can range from school and business closings to the interruption of basic services such as public transportation and food delivery.
- A substantial percentage of the world's population will require some form of medical care. Healthcare facilities can be overwhelmed, creating a shortage of

hospital staff, beds, ventilators, and other supplies. Surge capacity at nontraditional sites such as schools may need to be created to cope with demand.

- The need for vaccine is likely to outstrip supply, and the supply of antiviral drugs is also likely to be inadequate early in a pandemic. Difficult decisions will need to be made regarding who gets antiviral drugs and vaccines.
- Death rates are determined by four factors: the number of people who become infected, the virulence of the virus, the underlying characteristics and vulnerability of affected populations, and the availability and effectiveness of preventive measures.

Not a pretty picture, but as with all disaster planning, it's better to go in well armed with current and accurate information.

You might be arguing that if a pandemic hits, you'll have no control over the situation. Even though that may be true, you still have to provide some sort of contingency plans. Let's look at a possible scenario. Your company sells an enterprise-level software product. It's used at major corporations throughout the world. It seamlessly integrates into their messaging and communications applications, and they rely heavily on this application. Your largest client, a Fortune 100 company, comes to you and asks, "What plans do you have to support this product in the event of an H1N1 or other flu outbreak?" Here's a variation on the theme. Your company's vice president of Global Sales comes to you saying she is trying to close a deal with a Fortune 500 client that would mean tens of millions of dollars in revenue for the company. However, in order to close the deal, she needs the IT group's "Pandemic Readiness Plan" to allay concerns by the potential client about your company's ability to respond to global service and support needs in the event of an outbreak or other pandemic. Sound far-fetched? As more organisms adapt to current medications, the likelihood of an unchecked outbreak of some new flu variation is relatively high.

So, you might think that if the flu hit, you'd shut your doors until it blew over, but you may not be able to hide your head in the sand for long. The difficulty, of course, is that IT systems are not impacted by the flu—people and processes are. So, as the IT professional in the group, you have to figure out how you can provide the services required of you in the event that tens, hundreds, or even thousands of your staff are out sick, quarantined, or unable to report to work. In pandemics, there is a fairly high mortality rate, though it usually impacts the young, old, and infirm the hardest. Still, what if key staff die or are too ill to work for an extended period of time?

It seems callous to be worried about business in the face of death and serious illness, but businesses provide important services that are needed all the time. Shutting the doors may seem like the best option and for some companies, it might be, but you can't make that determination off the top of your head. If you run the IT department for a hospital, you have to keep the doors open and deal with the situation head on. In the BIA, we'll revisit this topic. As a threat, the Avian Flu or pandemic flu are just abstract concepts, but they are worth looking at in terms of your company's vulnerability to these events and the impact they might have on your company, your employees, your customers, your supply chain, and your community.

This section on natural and environmental hazards is not exhaustive, but it should give you a solid start in investigating the threats and threat sources your company might face. As you read through the various hazards, you may have thought of other threats not listed or you may have learned about threats you didn't think applied to your business. For example, not everyone would think about the risk of fire or flooding from an earthquake. If your company is located in a low-lying area and there is a dam or water containment system uphill, an earthquake can break the containment and send water downhill, flooding your building, street, or neighborhood. These kinds of examples point to the importance on doing research and being familiar with the surrounding area. You won't know that you need to plan for flooding if you don't know the reservoir is located just 3 miles away uphill from you or that you need to plan for wildfires because just over the crest of the hill is an open grassland. In the next section, we'll look at human-caused hazards and here too, you'll need to be aware of your surroundings. What does the company across the street or around the corner do? Do they work with hazardous materials or noxious chemicals? Could there be a biohazard or chemical spill in the area? Is there a railway that runs near your building or a major freeway? Is there a nuclear power plant in the region? Is nuclear waste transported on roads near your building? These are the kinds of things to consider as you read through the remainder of this chapter, as you develop your threat list and research potential hazards in your area.

Human threats

Human threats, like environmental or natural hazards, come in all sizes and shapes. Although we might like to distinguish between intentional and unintentional acts, that goes only to motive and intent, not impact and outcome. So, we'll look at these threats without regard to whether or not they're intentional except in a few cases. Terrorism is, by definition, intentional as is war, theft, and sabotage, to name a few. Other threats such as fire, chemical spills, or electronic data loss can be caused by intentional acts or human error. Remember the statistic cited earlier in the book—that 80% of data loss are human caused? It doesn't differentiate between intentional or accidental because the effect is the same. Let's go through some of these human-caused hazards in some detail. You may learn new facts that help you plan better or you may simply become aware of one or more threats you didn't previously know about.

Fire

Human-caused fires can be located inside or outside as in the case of improper wiring or unattended campfires. Fires are the most common business disaster, so regardless of what other planning you do, you should certainly ensure you have a solid fire recovery plan and you practice fire drills and fire procedures regularly.

Most commercial buildings have fire suppression systems; some buildings have fire doors to prevent fire from running uncontrolled through a building. Fire extinguishers, alarms, smoke detectors, and other fire equipment should be located

at strategic places throughout the building, should be well marked, and should be tested regularly to ensure proper functioning.

Arson is an intentionally set fire. The local fire department may investigate any fires in your building to determine the cause. Some insurance companies may prohibit payment of insurance claims in some circumstances, so be sure to have someone from finance or legal review your company's insurance policy, especially with regard to fire.

Theft, sabotage, and vandalism

Theft, sabotage, and vandalism are all intentional acts carried out by employees, tenant's employees (not associated with your company), former employees, and strangers. Many of these types of problems can be effectively thwarted by having security procedures in place. These include controlling access to the grounds, the buildings, and certainly to the inner offices, labs, server rooms, and other areas within the building that contain expensive, sensitive, or strategic materials. Most IT professionals understand that security begins with controlling and monitoring physical access and the same is true for your business as it is for IT equipment.

Theft can come in many different forms, some of which might not immediately come to mind, such as:

- Software piracy (are employees stealing software from the company or installing illegal software?)
- Counterfeiting (of currency or any other commodity of value, including company checks, ID badges, software, etc.)
- Theft of proprietary information (intellectual property, trade secrets, confidential data, etc.)
- Equipment theft (from office supplies to servers and everything in between)

You might think of some of these elements, but when you view them in light of BC/DR planning, you might find you need to take a few additional steps to address these. For example, you might have a plan for how you'd get your business backup and running after a fire, but what if someone came in and stole two critical servers? First, are the data safe? Second, how would you recover? Those are the kinds of considerations to include when you think about what could be stolen or damaged within the walls of your company. Keep in mind, too, that as with most computer fraud or theft, most company fraud or theft is perpetrated by those *inside* the company, not by mysterious outsiders.

If your facility is small, be sure to have a process in place for monitoring visitors or those entering the building such as strategically locating a receptionist or someone's office near the entry way. In some companies, this falls to the HR staff to manage. In larger facilities, you may need to have a more formal method of monitoring and controlling access such as visitor sign in, presentation of identification, and the issuance of a visitor badge. Many companies require cell phones and other digital devices to be left with the front desk so that photos or recordings cannot be made

while in the building. This prevents someone from stealing trade secrets or casing the property to determine the best way to burglarize the building during off-hours.

Any of these acts is intentional, and prevention is typically the best solution. However, should your business be vulnerable to theft, sabotage, or vandalism due to the location, the nature of the work you do, or the likelihood of having disgruntled employees or vendors, you should review your plans for preventing and recovering from these threats. However, since we're focusing on IT, we're going to cover theft, sabotage, and vandalism in the IT realm in just a bit.

Labor disputes

If your company includes union workers or your company interacts with another company that includes unions and union workers, there is a risk that labor disputes will disrupt business. Remember that you have to look at your company as well as at your key suppliers, vendors, contractors, outsourcers, and even customers. A major disruption in any of those areas could temporarily or permanently disrupt your business. For example, if you're a supplier to a large manufacturing company and that company represents 75% of your sales, what happens if they shut down for 6-8 months during a labor dispute? How will your company survive? Clearly, it's not desirable to have such a large portion of your revenue stream from a single source, but that's sometimes a business reality. Your executives may realize this puts your company at risk but the upside profit potential may be compelling. Therefore, as the BC/DR planning team, you need to assess this risk both internally and externally and determine both the likelihood and the impact a potential labor dispute would have on your business. Keep in mind, too, that there are various ways labor disputes can play out—from work slowdowns to strikes to sabotage. Each of these scenarios may have a slightly different impact on your company and your operations, and each should be assessed as a separate threat source.

Workplace violence

The unfortunate reality is that there is violence in the workplace. Whether from disgruntled former employees or unhappy current employees, violence can occur without warning. According to the U.S. Department of Labor's Occupational Health and Safety Administration (OSHA), homicide is the fourth leading cause of occupational injury in the United States. In 2010, the latest year for which data are currently available, there were 506 homicides out of 4547 fatal workplace injuries (Occupational Safety & Health Administration, 2013).

Before you start looking suspiciously at your coworkers, keep these facts in mind: 71% of workplace homicides are robbery related and only 9% are committed by coworkers. Although any person or company could experience workplace violence, the likelihood of violence increases with these factors:

- High interaction or exposure to the public
- Exchange of money or funds
- Working very late or very early, especially alone

- Guarding valuable assets or money
- Regularly dealing with volatile situations or violent people

Cab drivers, liquor store staff, late night convenience store staff, and safety officers (police and security guards) are occupations at the top of the risk list (Occupational Safety & Health Administration, 2013). If you believe your company's premises, location, or type of business may be at risk of workplace violence, you should certainly take preventive measures if you have not already. There are numerous resources available, from government Web sites to on-site training programs that can train your staff to prevent and address workplace violence effectively.

If we look at workplace violence from a business disruption point of view, a serious injury or death could result in the premises being sealed off as a crime scene for some period of time. Equipment such as computers or other needed items could be seized as part of the investigation. Employees will be impacted and productivity will suffer; good employees may choose to find employment elsewhere, and your reputation in the community, in your industry, or in the eyes of potential employees may suffer.

TIP

Workplace Violence Is a Serious Threat

If you're interested in learning more about preventing workplace violence, visit the OSHA Web site focused on that topic at www.osha.gov/SLTC/work-placeviolence/evaluation.html.

The U.S. Department of Health and Human Services, Centers for Disease Control and Prevention (CDC)'s National Institute for Occupational Safety and Health (NIOSH), has additional resources related to workplace safety, and you can download videos on preventing workplace violence by visiting this link: www.cdc.gov/niosh/docs/video/violence.html (U.S. Centers for Disease Control and Prevention, 2013).

Terrorism

The very nature of terrorism is that it cannot be planned for and sometimes cannot be prevented. Therefore, your assessment should include not the threat of terrorism but the threat sources that stem from it. This goes back to many of the issues we've already discussed—what if your power goes out or there's a chemical spill or an anthrax release? (We'll cover biohazards in an upcoming section). How will you address the results of terrorism? When you look at it this way, it seems to become a slightly more manageable topic. Ultimately, each company has to assess its vulnerability based on geographic location, the nature of its business, its international business connections, its political involvement, and more. If your company is vulnerable to terrorism, there's a good chance you have a strong team in place that has already addressed this. Nuclear power plants, power stations, airports, and others have developed contingency plans because of federal or state mandates to do so. If you believe your company should have a stronger plan to prevent or address a terrorist threat, you should involve high-level executives or managers in your company and discuss next

steps. There may be resources at the U.S. Department of Homeland Security that can be helpful to you or you may wish to consult with a private firm that specializes in this area to address the specific threat of a direct attack on your company.

However, most companies are not the target for such an attack, but may be in the area of an attack or may experience the result of an attack. Addressing the likely threat sources in your area that potentially could be targets for terrorists will help you devise a plan that will help address the aftermath of an attack, even if you don't know whether the incident was intentional or accidental.

The U.S. Department of Homeland Security has a wide variety of resources, including information on terrorism, on their Web site at www.dhs.gov/index.shtml (U.S. Department of Homeland Security, 2013).

Chemical or biological hazards

Chemical hazards are present in a variety of manufacturing environments, whether the chemicals are the *result* of the manufacturing process or are used *within* the manufacturing process. A biological hazard, often called a *biohazard*, is defined as a danger to humans or the environment resulting from biological agents or conditions. Both chemical and biological hazards can occur as the result of an accident, sabotage, or terrorism.

If your company is not involved with chemical or biological agents, you may still face risks in this regard. You need to look in your local area and determine what other types of companies exist. If a chemical plant is located 4 miles away, what is the risk to your operations? What if it's next door? Fifteen miles away? Your local and state agencies may regulate these types of companies, so there may be information that's easily available to you. Some research on local companies should also reveal the nature of work that your commercial and industrial neighbors do. If you run into trouble locating this information, you might be able to contact a friendly commercial leasing (real estate) agent. Commercial leasing agents often have their fingers on the pulse of the community and can tell you who your neighbors are and what type of work they do. Your local Chamber of Commerce may also be able to provide useful information. Keep in mind that you're more likely to encounter these kinds of hazards in a heavily industrialized area, so you can look at your location and determine where the industrial areas are in relation to your operations. Areas that are heavily residential with a bit of commercial building space are less likely to pose a threat of chemical or biological hazards.

If your company is involved with chemical or biological research or manufacturing, you no doubt have safety procedures in place with regard to these agents. However, you and your team might review your safety procedures with an eye toward BC/DR planning. What types of containment procedures are in place? What sort of evacuation procedures is practiced? What are the countermeasures or remedial activities that should take place if a spill, leak, or release occur? In some cases, your company's activities (or the chemicals and biohazards) may be closely regulated by government or industry and the procedures and requirements address these questions. However, you may need to take this information as input to your business continuity and

disaster recovery planning by asking how operations would be impacted by a chemical or biological hazard. Would you have to setup operations elsewhere? How long would it take to reoccupy the building, or would you have to permanently move? If the servers and other IT equipment were inaccessible due to contamination, what would you do? How would you resume operations? These are the kinds of questions you'll ask and answer as part of this process. For now, the key is to determine what, if any, risk you have to internal chemical or biological hazards? Remember, if your company works with hazardous materials, they may have planned well for handling a spill or release in terms of protecting life and property. They may not have thought about how such an event might impact business operations in terms of IT assets. Don't reinvent the wheel on this one, just review your company's plans and ensure IT needs are addressed within it.

We haven't addressed the risk of the release of these agents as part of sabotage or terrorism, but the result would be the same. If a chemical plant in the area were to be the victim of sabotage or a terror attack or just an accident by a careless employee, the net result to your firm is the same.

If a chemical or biological agent were to be released in your area as part of a terror attack, you would have to address the same types of issues such as whether the best course of action is to evacuate the building or to shelter-in-place. If you believe your company may be vulnerable to these types of threat sources, you may want to contact your local police and fire department for guidance on how to handle these types of incidents. The bottom line, however, is what data you need to develop a sound BC/DR plan that addresses the impact of this type of threat.

War

This type of threat clearly exists for many companies around the world. For U.S.-based companies, the risk is greatest for divisions of the company that may be located in areas of political or economic instability. Plans for shifting operations away from areas experiencing war, civil war, or civil unrest should be made in areas that are vulnerable. BC/DR plans should examine which areas of the company may be vulnerable and how they can be protected. Remember that not only would local operations in a war zone be disrupted but vital knowledge, equipment, or assets could be destroyed or stolen from the company. In addition, you'll need to consider the impact of losing that part of your IT operations. Are vital assets located there? Is substantial computer power, storage, or operational support staff there? What would happen to your IT organization should this location be closed? The BC/DR plan must look holistically at the people, process, technology, and infrastructure of the organization in areas vulnerable to war or civil unrest and assess the vulnerability to these various threats.

Cyber threats

We placed cyber threats last because it is a large and ever-changing topic. We'll cover some of the common threats in this section, but we recognize that they will shift and change quickly. The good news is that many, if not most, of these threat

sources are ones that you and your IT team are very familiar with, and as such, your BC/DR plan should be fairly easy to construct in this area. Most of these threat sources have to be assessed and addressed through normal IT operations and security assessments (and certifications), so you may already have all the data you need to include in your BC/DR plan.

The bottom line in IT is data security. Sure, a stolen server is a hassle to replace, a hacked Web site is a pain to repair, but ultimately all these threats result in compromising one (or more) of three building blocks of information security: CIA.

Confidentiality refers to the protection of data from unauthorized disclosure. Unauthorized, unintended, or unanticipated disclosure can result in legal action, financial loss, loss of public confidence, or embarrassment. For example, personal medical information is protected by law, and any unauthorized disclosure of such information, regardless of whether it was intentional or not, is illegal. Companies dealing with personal health information include hospitals, health clinics, doctors' offices, pharmacies, labs, and prosthetics companies, to name just a few. All are subject to these kinds of regulations. However, confidentiality also can include keeping trade secrets confidential from competitors or keeping embarrassing information from spreading through unintended or unanticipated channels.

Integrity has to do with the information being protected from unauthorized or unintended modification. Hackers often have as one of their goals the modification of data—whether that data include user permissions, network access, or business data modification such as pricing on a Web site or pay rates for employees. Integrity issues can stem from intentional acts such as wayward employees or external hackers, but it can also result from accidents and errors. Someone might make accidental changes, enter erroneous data, or corrupt a database just with a few incorrect clicks of the mouse. Inaccurate data may be from an error, it might stem from intentional fraud (such as changing payroll data or pricing on a Web site), or just bad decisions. Regardless of the intent behind it, these losses can also add up. In some cases, your company may face legal liabilities. There are almost always financial consequences including lost productivity, downtime, lost or lower sales, or untraceable losses, to name a few.

Availability pertains to critical business data being available when needed. If a database is corrupted, it is not available for use. If a Web site is hacked, it is not available for use. If an interface to a critical application is down, data are not available. These kinds of availability problems can also be intentional or accidental. Lack of availability impacts productivity for the IT department (busy fixing availability issues) and for end users (unable to retrieve needed information in a timely manner). Availability can be assured through a solid backup plan.

Anyone working in IT for any length of time knows about CIA and about the various methods used to attack these three areas of data security. You are also probably painfully aware of how unintentional errors or poor decisions can impact CIA as well. Users can be granted incorrect access, which can allow data to be changed or deleted with just one erroneous setting.

Most likely as you've worked in your IT operations, you've identified the critical data for your organization and ensured it was protected against loss of CIA. These are

basic operational areas that most IT departments do as part of defined security procedures. Basic steps such as creating backups, reviewing security logs, analyzing network traffic patterns, and other types of standard IT security operations typically are built into your everyday activities.

For your BC/DR planning, you'll need to review all your IT operations in light of the potential for these security threats occurring. For example, you might have a computer incident response team in place to address a breach in network security. Have you also taken it a step further and looked at what the impact on business operations would be if, say, a client database was attacked? How would your business recover from that? The likely answer is that it depends on the nature of the attack. You'd first probably need to understand whether the data were looked at, modified, or stolen, and how the attack was carried out. This would dictate your next steps and would also tell you the potential impact of the incident on short- and long-term operations. So, even though you may have plans in place to prevent and address potential data security issues, you may not have business continuity and disaster recovery plans in place related to these specific threat sources.

As a starting point, you can review your IT security processes and procedures and determine whether they need to be updated or expanded to address new and evolving threats. Then, take those procedures and include the security threat sources in this BC/DR risk assessment. From there, you can treat these threat sources as you would any other threat source except that you're probably already ahead of the curve with much of these data. Look across the enterprise to see how these incidents could disrupt not just IT activities, which you probably have already determined at length, but corporate operations as well.

LOOKING AHEAD . . .

Business Impact Analysis

BIA is the next step in the risk management process and it's covered in depth in [Chapter 5](#). However, let's take a moment to define BIA, so you can begin formulating ideas and thoughts about BIA while you're in the risk assessment phase. BIA is the process of identifying all potential impacts to your business from all identified threat sources that could disrupt the business. Later in this chapter, we'll analyze threat sources based on the company's vulnerability to these threats and you'll rank these in order of importance. You'll probably decide to limit your BIA to those threat sources that are most likely to occur and your company's vulnerability to those threats. After you've identified and analyzed the business impact of each selected threat source, you will use that data as the input for developing mitigation strategies. It's helpful to keep the overall process in mind as you move through each phase of the assessment so that information, ideas, or suggestions relevant to upcoming phases can be captured during the process.

Cyber crime

Cyber crime is an evolving field of study, and unfortunately, there is no dearth of people interested in perpetrating cyber crimes. In the United States, there are numerous federal and state agencies that may deal with cyber crimes, depending on factors

such as the suspected originating location of the crime, the scope or span of the crime, and the nature of the crime. For example, financial crimes and those related to personal identity theft for the purpose of financial gain are often handled by the U.S. Secret Service, a division of the U.S. Treasury. Other crimes are handled by the U.S. Department of Justice, and still others are handled by the FBI. The unfortunate reality is that cybercrimes are now perpetrated by state-sponsored or sanctioned groups. Governments across the globe are waging war with one another using cyber crime. If you work in a local, state, or federal agency, you are certainly aware of the potential threats in this arena. Private companies can become targets of state-sponsored attacks as was evidenced in 2012 when the *New York Times* newspaper was apparently hacked by Chinese government representatives who were looking for information about a story that was unfolding.

TIP**Cyber Security Resources**

For more on these national resources, visit these links:

- U.S. Secret Service Electronic Crimes Task Force: www.secretservice.gov/ectf.shtml (U.S. Secret Service Electronic Crimes, 2013)
- U.S. Secret Service Criminal Division: www.secretservice.gov/criminal.shtml (U.S. Secret Service Criminal Division, 2013)
- U.S. Department of Justice Computer Crime and Intellectual Property Section: www.cybercrime.gov/ (Note: The use of the acronym IP on this Web site indicates “intellectual property” and not “Internet Protocol.”) (U.S. Department of Justice, 2013)
- FBI’s Cyber Investigations: www.fbi.gov/cyberinvest/cyberhome.htm (U.S. Federal Bureau of Investigation, 2013)
- Federal Trade Commission: www.ftc.gov/ (U.S. Federal Trade Commission, 2013)
- Securities and Exchange Commission (SEC): www.sec.gov/ (U.S. Securities and Exchange Commission, 2013)

Unfortunately, the types of crimes committed are limited only by the twisted imaginations of people intent on wreaking *havoc*. The following is a brief list of the headlines that appeared in mid-February 2013 on the U.S. Department of Justice’s CyberCrime.gov Web site, which gives a good indication of the breadth and depth of cybercrime (U.S. Department of Justice, 2013):

- Three Alleged International Cyber Criminals Responsible for Creating and Distributing Virus That Infected over One Million Computers and Caused Tens of Millions of Dollars in Losses Charged in Manhattan Federal Court (January 23, 2013)
- Romanian National Sentenced to 21 Months in Prison for Role in Multimillion-Dollar Scheme to Remotely Hack into and Steal Payment Card Data from Hundreds of U.S. Merchants’ Computers (January 7, 2013)
- Russian Citizen Sentenced in Manhattan Federal Court to Three Years in Prison for Sophisticated International Cyber Crimes (January 4, 2013)

- International Cyber-Fraud Ring Responsible for Millions of Dollars in Fraud Dismantled (December 5, 2012)
- Third Member of Internet Piracy Group “IMAGiNE” Sentenced in Virginia to 40 Months in Prison for Criminal Copyright Conspiracy (November 30, 2012)
- Top Executives at Kolon Industries Indicted for Stealing DuPont’s Kevlar Trade Secrets (October 18, 2012)
- Christian County Men Charged with Attempting to Steal Trade Secrets from Their Former Employer (October 15, 2012)
- Federal Courts Order Seizure of Three Website Domains Involved in Distributing Pirated Android Cell Phone Apps (August 21, 2012)
- Former Bridgestone employee charged with theft of trade secrets, making false statements (August 14, 2012)

Not yet on their headline list: In January and February of 2013, Facebook, Apple, and Microsoft systems were hacked. All three companies detected an intrusion to a small number of corporate computers. As you can see, the crimes are rather diverse in nature and the list goes on and on. These were taken from press releases for the folks that got caught and sentenced; imagine how many more go unsolved and unstopped. [Visit <http://www.justice.gov/criminal/cybercrime/pr.html> to scroll through press releases going back to 2000.]

As an IT professional, you know how difficult it is to keep up on all the latest cyber crime methods, but you also know that if you or someone in your organization is not up to date, you may well fall victim to cyber crime. Rather than go into a long list of potential threats, let's just create a general list of items as a start. Remember, cyber crime is committed for three basic purposes—to make money, to earn bragging rights, or to disrupt business (or governments). Money usually is made by stealing electronic data and selling it or making unauthorized use of it. Clearly, this fits into the “confidentiality” element of the CIA model. Bragging rights often are sought by hackers, and those types of crimes often span the entire CIA framework. Finally, disruption of business or government often entails the integrity or availability of data, though breaching confidentiality can also create a disruption in some cases.

The common categories of cyber crimes include:

- Identity theft (through a variety of means)
- Corporate identity theft (through a variety of means)
- Hacking corporate network or intranet (to breach CIA)
- Hacking corporate Web site or extranet (to breach CIA)
- Creating backdoors for unauthorized access (to breach CIA)
- Stealing/selling confidential data (trade secrets, drawings, plans, intellectual property)

Loss of records or data-theft, sabotage, vandalism

Although loss of records or data falls under a variety of cyber crime categories, it's worth listing as a separate category anyway. An error or an intentional act can create data loss. Even in the case of unintentional loss (error), the perpetrator is unlikely to

come forward voluntarily. In some cases of error, the person may not even know they have caused a data loss. This can happen when ill-trained staff are given tasks to perform outside their skill levels. In other cases, a careless error is made, and the person making it is unaware of the error or the resulting data loss. Even if asked, he or she might not understand or realize that their actions may have caused the problem. However, in most cases, the person causing the problem is aware or becomes aware of it. If your company has the type of culture that will severely punish someone making that type of error, you won't likely get people volunteering the truth. It makes it difficult, then, to ascertain whether someone intentionally or inadvertently caused the problem. If it was intentional, you have sabotage going on and you need to find the source and remove access to systems. If it was an error, it may be a one-time event or you have a training issue on your hands. In that case, you may want to restrict access to those systems until the person can demonstrate reasonable competence. In planning for this type of threat, what would you do? Clearly, having security monitoring and log reviews in place can help as can education. Sometimes data leak out, which is an information security problem. Sometimes data are destroyed, which is a risk assessment problem.

IT system failure-theft, sabotage, vandalism

IT system failure is similar to loss of data—it can be intentional or unintentional. Intentional acts that bring systems or networks down are sabotage and should be addressed as crimes. Vandalism occurs when systems have been physically broken or destroyed. Unauthorized modification of a Web site is also considered vandalism, especially if it is modified in a way to visually indicate it has been breached such as changing the text or links on a page or inserting a banner, picture, or other data in the Web site. When we talk about IT system failure and theft, we're primarily concerned with the physical theft of equipment including servers, routers, firewalls, test equipment, software, cabling, and any other IT-related asset. The theft of these items disables one or more IT systems, thus falling in the category of IT system failure.

Infrastructure threats

Infrastructure threats are large, external environmental issues that you rarely have any control over preventing, addressing, or resolving. These issues include:

- Building-specific failures (structural damage, systems failures)
- Public transportation disruption (roads, railways, airports, seaports, waterways)
- Loss of utilities (power grid failure, gas supply failure, water supply failure)
- Petroleum or oil shortage
- Food or water contamination
- Regulatory or legal changes

Building-specific failures

Buildings are designed and built by humans, so there's always a chance that the architect or builder could make an error that results in part of the building becoming unstable or failing. Buildings can fail because of human error in the design and

construction of the building. The materials themselves can fail as has been the case where inferior concrete was used. Buildings not built to code or that are not properly inspected can be at risk of structural failure.

Other building-specific failures include non-IT system or equipment failures (IT system failures are covered in a later section), communications equipment failures (telephone lines, communications lines, Internet connections), safety systems (fire and alarm systems), internal power failure (circuit breakers, wiring issues, circuit capacity, etc.), heating/cooling failure, and manufacturing line (production) failure. These types of systems typically are managed by the facilities manager. In smaller companies, some or all of these systems may be managed by the building's management company or directly by the building owner/landlord. If you are occupying a building you do not own or manage, you may want to set up an appointment with the manager to go over the building's systems so that you understand things like how old the equipment is, the likelihood of it breaking, the estimated duration of critical repairs, and so on. For example, if you're occupying an older building and you learn that the heating system is 45 years old and that parts would be next to impossible to get, you should probably come up with a Plan B related to loss of heat. Statements like, "Yeah, the next time it breaks, we're just going to replace the system," should give you a clear indication that a heat failure could take days or weeks to repair.

Public transportation disruption

Disruption of public transportation can have a local impact such as the inability of employees to get to work in a timely manner (if at all) or the inability of employees to evacuate due to an impending storm. On a larger scale, your suppliers, vendors, and contractors can all be impacted by transportation disruptions, so your entire supply chain should be evaluated for vulnerabilities to the same threat sources you're looking at for your company.

Loss of utilities

Loss of utilities usually is localized to a specific region and can be caused by a number of things including weather events, sabotage, error, technology failure (a switch or transformer fails, for instance), or terrorism. In some cases, power loss can cover an entire geographic region, such as when power fails on an entire section of the U.S. power grid.

REAL WORLD

Gravest Short-Term Threat

In October 2012, the *New York Times* reported that "Defense Secretary Leon E. Panetta warned Thursday that the United States was facing the possibility of a 'cyber-Pearl Harbor' and was increasingly vulnerable to foreign computer hackers who could dismantle the nation's power grid, transportation system, financial networks and government" ([Bumiller & Shanker, 2012](#)). In May 2011, an ABC News article with this headline "Cyber Attack on U.S. Electric Grid 'Gravest Short Term Threat' to National Security, Lawmakers Say" included this unsettling

Continued

REAL WORLD—cont'd

information: "Earlier this month, the White House released a more comprehensive cyber security plan calling for industries vulnerable to cyber attacks, like electricity, to create plans that would make their computer systems more secure. Our critical infrastructure—such as the electricity grid, financial sector, and transportation networks that sustain our way of life—have suffered repeated cyber intrusions, and cyber crime has increased dramatically over the past decade," the report stated. "Our nation is at risk. The cyber security vulnerabilities in our government and critical infrastructure are a risk to national security, public safety, and economic prosperity" ([Khan, 2011](#)).

Disruption to oil or petroleum supplies

There has been a lot of discussion of late with regard to global oil supplies (especially, as it relates to global warming issues). Regardless of your opinions on the topic, oil supplies are finite and are managed by large groups—countries or cartels—and the availability and cost of oil and petroleum products are controlled by those few. Oil and petroleum supplies can be disrupted by war, civil unrest, sabotage, weather, or political will. If supplies are disrupted, how will your business fare? Employees may not be able to get to work (long gas lines or no gas, as was evidenced in the late 1970s in the United States); suppliers may not be able to manufacture or deliver their products to you (oil is used in manufacturing and for fuel); products needed for your manufacturing may be unavailable or significantly more expensive; timelines may be pushed out due to delays in getting materials and supplies; costs may skyrocket due to limited supplies; and the list goes on. If your company is dependent upon oil or petroleum production or supply, you clearly need to evaluate the threats and threat sources so you can create effective mitigation strategies. These tasks may fall outside your purview as an IT professional, but as with other business risks, it's important that you be as well informed as possible so you can participate fully in developing the best BC/DR plan possible.

REAL WORLD**Hubbert's Peak**

Geophysicist M. King Hubbert predicted in 1956 that U.S. oil production would reach its highest level in the early 1970s. Though severely criticized by oil experts and economists, Hubbert's prediction came true in 1970. The term "Hubbert's Peak" is used to indicate the peaking of oil production in a particular area. Oil companies routinely use Hubbert's calculations to help them determine the yield of a particular oil field, so clearly Hubbert's data have been found to be accurate over the years. Kenneth Deffeyes, a geologist who worked for Shell Oil Company and later became a professor at Princeton, built on Hubbert's work and found that worldwide oil production will peak in this decade. Regardless of which side of this debate you fall on, you might find some interesting information by using the search term "Hubbert's Peak" on your favorite search engine.

Food or water contamination

Contamination of the food or water supply is disruptive to all life forms. Contamination can be accidental as in the case of an oil or chemical spill, or it can be an intentional act of sabotage or terrorism. The impact of these events can be local,

regional, or national though they usually are contained to a specific geographic region. Chances are good that if food or water is in short supply in your area, your employees will not be concerned with coming to work but with finding food or water. Your company's operations will be secondary to survival in that event, and you may not need to plan for this other than to assume you will suspend operations until the issue is resolved. Food or water contamination or shortages in other areas could impact your supply chain, so looking at your business as well as that of your business partners may turn up some risks you hadn't seen that might be worth addressing in your mitigation plan. If you work in a mission-critical industry such as at a hospital or at a utility company, you may need to maintain operations despite such a disaster. If so, you'll need to figure out contingency plans that account for these variables. Developing this type of plan is larger than just IT, but if you think it through and ask what you could do in such an event, you can at least come to some high level decisions in advance.

Regulatory or legal changes

Changes to regulations or legal rulings setting precedents could impact your business, but the place they're most likely to impact you is after a disaster. For example, there may be health and safety regulations that impact your ability to resume operations, especially if something has happened to your facility. Opening your doors without adhering to these regulations could result in having operations shut down or having stiff legal and/or financial penalties imposed. Changes in any of the legal areas, such as data security, could also impact your firm in the aftermath of a disaster. If a server inadvertently ends up in the wrong hands and data were not encrypted or due diligence was not used to secure the data or the computer, you may have another disaster on your hands.

The best way to address this is to have someone on your team review the current regulatory and legal requirements for your firm and do a bit of research to find proposed or impending changes. Then, determine how your company would be impacted by these changes during normal business and in the aftermath of a disaster. This is especially true for data security requirements within the IT arena. You can begin to build in or modify processes to address these changes so that they are part of your everyday operations, if appropriate. Often it's easier and less costly to scan the horizon and build in your safeguards in this manner than to try to retroactively address these kinds of issues in the aftermath of a disaster.

We've looked at a wide variety of threats and threat sources, and continually tied them back to corporate operations and, where applicable, IT. As we've mentioned, it's not exhaustive and, in some cases, we did not go into tremendous detail because of changing threats or changing laws and regulations. However, this section should have given you a good idea of how to look at potential threats and threat sources as well as how to think through the potential threat and impact to your business.

CRITICAL CONCEPT**Organizational Disaster Preparedness**

As you can see from reviewing the numerous and varied types of threats, many of these go far beyond the scope of your IT responsibilities. In smaller organizations, you might be the only person thinking through these things and it may fall upon your shoulders to develop a disaster plan for your entire company. In medium or large companies, there is typically a group responsible for disaster preparedness and response. If that's the case, you need to ensure that IT is at the table—both as a supplier and as a customer. IT supplies the technology that companies rely on—from computers to network connectivity to wireless and phone service—and needs to be included as any other vendor would be. At the same time, you and your staff are employees of the company and are customers who would need disaster services (payroll, employee assistance, information about how to respond to the disaster, where to report, etc.). Proactively participate in corporatewide disaster and business continuity discussions to ensure assumptions about IT services in a disaster are correct and that your IT and staff needs are addressed by the planning.

Threat checklist

The list, shown in [Table 4.2](#), is provided for your convenience. It is a reiteration of all the threats listed in the previous sections. You may want to use this list as a starting point in your threat assessment. You can add any threats not included in the list and remove those you're confident will not impact your business. Again, be sure to avoid removing threats before you look at your company's total environment—internal, external, and extended (key suppliers, vendors, outsourcers, partners, and customers).

Examine how these threats and threat sources impact the *people, processes, and technologies* your company needs to operate as well as the *infrastructure*. In [Chapter 5](#), we'll look specifically at how these threats and threat sources can impact your immediate operations as well as how they might impact your key customers, suppliers, vendors, contractors, outsourcers, or partners. However, if you have any thoughts on impact as you move through this portion of the risk assessment, be sure to jot them down for later use.

For your convenience, in [Table 4.3](#), we've also included a slightly different view of some of the IT-specific threats you might want to consider in your planning. It's not intended to be comprehensive, but it should help get you started.

[Figure 4.5](#) shows the output from this phase of the risk assessment, which is a document listing all potential threats and threat sources you have looked at for your company. Although you may be able to skip over a few that clearly don't apply, your list should be inclusive rather than exclusive at this junction. This document will be used as the input for the vulnerability assessment phase, discussed later in this chapter. At the end of the entire risk assessment phase, you'll have a more streamlined list of threats that you'll use in your BIA, discussed in [Chapter 5](#).

[Table 4.4](#) provides a sample of how you could organize your threat data so that you're ready to move into subsequent phases. Regardless of how you organize your data, be sure you capture it in a consistent and logical manner.

Table 4.2 Threat Checklist*Natural/environmental threats*

Fire (can be human-caused)
Flood
Severe winter storm
Electrical storm
Drought
Earthquake
Tornado
Hurricane/typhoon/cyclone
Tsunami
Volcano
Avian Flu/Pandemics

Human-caused threats

Fire, Arson
Theft, Sabotage, Vandalism
Labor disputes
Workplace violence
Terrorism
Chemical and biological hazards
War, civil unrest

Infrastructure threats

Building-specific failures
Non-IT equipment. System failures
Heating/cooling, power failures
Public transportation disruption

Infrastructure threats

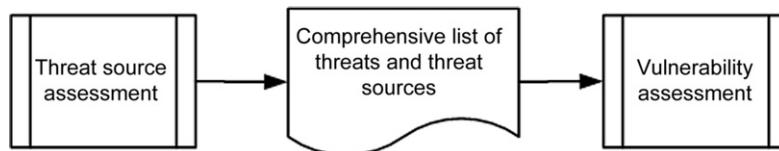
Oil, petroleum supply disruption
Food, water contamination
Regulatory, legal changes

IT-specific threats

Cyber threats (threats to Confidentiality, Integrity, or Availability of data)
Equipment or system failure
Production line equipment failure
Loss of data or records

Table 4.3 IT-Related Threats

Threat To...	Specific Threats
Hardware	Equipment failure (intentional, unintentional damage)
	Power outage
	Equipment reconfiguration (authorized, unauthorized)
	Equipment sabotage
Software	Equipment theft
	Bugs, glitches
	Data corruption
Infrastructure	Data security breach (deleted, stolen, modified)
	System configuration changes (errors or sabotage)
	Internet connection(s)—failure, tampering, destruction
	Wireless networks—failure, tampering, destruction
	Network backbone—failure, tampering, destruction
	Cabling—failure, tampering, destruction
	Routers, infrastructure hardware—failure, tampering, destruction

**FIGURE 4.5**

Deliverable from threat source assessment.

Table 4.4 Risk Assessment Table

Item No	Threat Name	Threat Source	Vulnerability Rating	Likelihood Rating	Existing Controls	Impact Rating	Overall Risk Rating
001	Fire	Internal					
002		External					
003	Flood	Internal					

This matrix shows Fire as a threat and then delineates the threat source as *Internal* or *External*. If there is a fire in the building, you may evacuate. If there is a fire in the area making leaving the area difficult or dangerous, your best solution might be to shelter-in-place. This is an example of how a single threat (fire) has two different sources and how the vulnerability, likelihood, impact, and mitigation strategies

might differ for each. Therefore, to list “fire” without listing the threat sources, you might miss something in your assessments. You may choose to create additional columns or include additional details. For example, an internal source of fire could be limited to the server room or could be elsewhere in the building. Is it useful for you to make that distinction? If so, add that detail. If not, don’t add unnecessary detail. Also in this table, we’ve included a column labeled *Existing Controls*, which can be used to list controls or measures that are already in place. For example, if your server room has a state-of-the-art fire suppression system, you can list that as a control. If your building has a fire suppression system and you practice fire evacuation drills, you can list that as a control. These are things that are already in place that are mitigating your risk. In some cases, these controls may be sufficient; in other cases, you’ll need to add layers of control to bring the risk down to an acceptable level. By listing controls already in place, you can spend less time on risks that are already addressed and more time on those that are not addressed in an effective manner. As you go through this assessment, it can be helpful to list these kinds of items or to add/delete columns as needed. Creating the right data fields now will make your work easier later on because this matrix will help you capture information as it comes up. The goal is to find a balance between too much and too little detail.

If you have a preferred method for approaching this that will account for your threats and threat sources adequately, feel free to use it. The end result is to have a comprehensive assessment from which you can build a plan without getting bogged down in useless detail. One final word: You may start out with more detail than you need and pare down as you see how your planning is progressing. Sometimes when you have a bit of perspective on the topic, you can see more clearly what *is* and *is not* needed. Err initially on the side of inclusion, pare down later.

THREAT ASSESSMENT METHODOLOGY

Before we head into the vulnerability assessment phase, we’re going to discuss threat assessment methodologies that might be useful to you in evaluating various threats. In essence, there are two ways you can approach this. The first is to use a *quantitative* approach, in which you attempt to use hard numbers to represent threats, vulnerabilities, and impacts. In some companies, this may be the norm or it may be required for some reason. The second method is a *qualitative* approach, where you attempt to define the relative threats, vulnerabilities, and impacts. You use qualitative, or value-based, language such as “high,” “medium,” and “low.” We’ll look at both methods and provide a few samples, so you can determine which approach would be best for your BC/DR team. Keep in mind that you should pick one approach and stick with it; mixing and matching can result in unclear or meaningless data. Once you’ve read through this section, you should have a good idea of which approach fits best with the culture and requirements of your company.

The reason we’re discussing these two different approaches is because if you’re fighting an uphill battle in your company with regard to the cost or benefit of this BC/

DR plan, you may need to come up with quantitative assessments to sway decision-makers. They may not be convinced by statements like “more” or “extremely high”; they might be convinced by “20% chance” or “\$250,000 loss.” If you have support for your BC/DR plan, you may opt for the qualitative approach, which is less precise but faster and easier to derive.

Quantitative threat assessment

A quantitative assessment can be defined as observations that involve measurements and numbers. They are specific and measurable. If you say, “The server costs \$1850 more than the desktop system,” you are making a quantitative statement. In contrast, if you say, “The server is more expensive than the desktop system,” you are making a qualitative assessment as “more” is not specific and measurable.

Let’s start with the threat of a power outage. We can look at the possible threat sources—what could cause a power outage? As you learned in the previous sections, there are numerous potential sources of a power outage. Let’s begin with an electrical storm with lightning that causes a localized power outage. If your building is susceptible to power outages in storms and those outages do not affect neighboring buildings, you may start with a power outage that impacts just your building. Again, this is where a thorough threat assessment is helpful. You can gather actual data from the National Weather Service or other reliable sources on the number of storms per year in your area, on average. If you want to know more about local weather conditions and history, you might be able to get some valuable information from your local news station’s meteorologist. Sometimes they are more than willing to share information with you, and they might be able to point you to resources you’d otherwise miss. You can also gather data from the power company on the number of times power has gone out in your building or your area over the past 5 years or on average. Data should ideally include both frequency and duration as both are key to understanding your risk of a power outage. Once you have that data, you have very specific, quantifiable information. When looking for quantitative data on any of your threats and threat sources, you may need to be creative.

REAL WORLD

Locating Your Data “Weasels”

In every company, there are always a few people (sometimes more) who relish the challenge of a good data search. At one company, there was a young man whom people had affectionately nicknamed “the data weasel” because he could “ferret” out just about anything—there was not a piece of information he could not eventually retrieve (though his typical turnaround time was less than 30 minutes). There may be people in your company who participate in “search engine races” to see who can find a specific piece of information the fastest (think of the TV show Who Wants to Be a Millionaire?—who in your company would make a great “Phone-A-Friend”?). If you need data on the number of storms in your area that have dumped more than 10 inches of snow in the past 10 years, or number, frequency, and duration of local power outages, turn to your company’s data weasels. Give them specific data to search for and a

Continued

REAL WORLD—cont'd

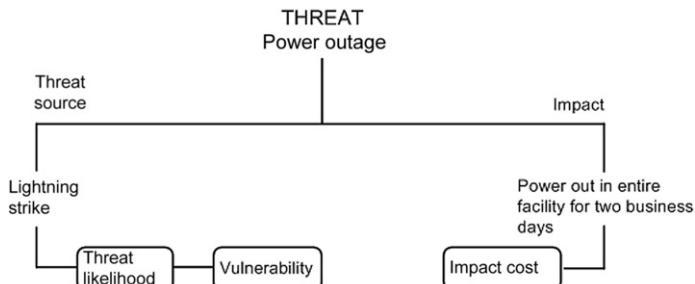
deadline for completion and leave them to it. Be sure to ask them to capture the source of their data, so you can be sure it's credible before relying upon it. By leveraging the natural skills and interests of people in your company or on your team, you can effectively delegate tasks to others who will enjoy the challenge and will produce great results.

What if you can't easily find that data? You can gather anecdotal evidence, though this by its very nature is much more qualitative than quantitative. You can probably talk to your facilities person or staff who have worked at the company for several years and get their input. Will they know exactly how many storms with lightning have come through the area? No. Will they have an idea of how many times power has gone out in the building or the area? Probably. They may not have an exact number but you may well get a response like, "It seems to happen every year or two" or "I can't remember the last time that happened and I've been here 5 years."

To create a quantitative assessment, we need to make sure we're comparing "apples to apples," so all numbers will be converted to annual numbers. For example, if you have a power outage every other year, the annual power outage would be 0.5 chance of an outage. If an outage occurs once every 4 years, you have a 25% or 0.25 chance per year because the risk is only one in four that you'll have a power outage in any given year. The numbers should all be annualized so that comparisons are accurate.

Let's look at a risk diagram, shown in [Figure 4.6](#). Remember that we'll quantify some of these other numbers through our assessments later in this chapter and in upcoming chapters. We'll quantify these in this section, so you can see how the process works and then you can develop the remainder of the needed input values later as you develop the data. In other words, you can do your likelihood assessment later and input the values later, but we'll review the entire model here so you can see the road ahead.

On the left side of the diagram, you can see one threat source listed. Ideally, each threat source for a power outage should be addressed in this manner. In this case, the *threat source* we're looking at is a lightning strike. First, we assess the likelihood of

**FIGURE 4.6**

Risk assessment methodology—quantitative.

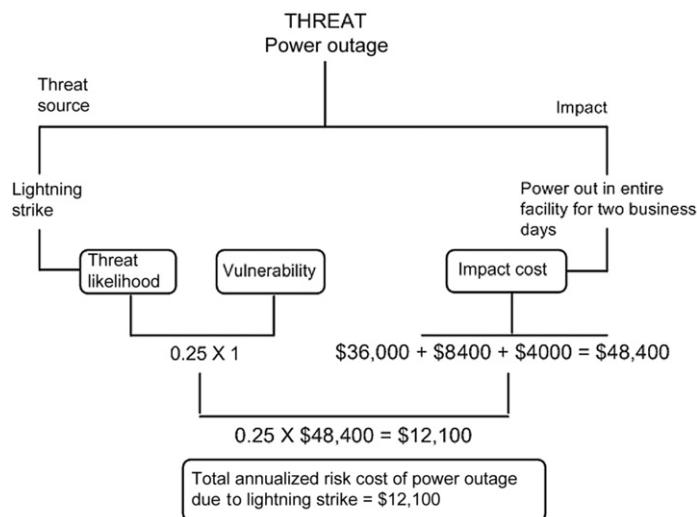
occurrence. If your data indicate that this happens once every 4 years, then you would enter the value of 0.25 under the threat likelihood since we want to know the likelihood in any given year. Keep in mind, this is not that lightning hits your building once every 4 years, but that once every 4 years or so, the power goes out due to a lightning strike somewhere in your area. Next, you would assess your vulnerability. In this case, let's say that every time there's a serious lightning strike (once every 4 years), your power goes out. That means that *when* lightning strikes in your immediate area, your power *will* go out. That's a 1:1 ratio, or 100%, so we'll insert the number 1. Now, on the threat source of this equation, we have: $0.25 \times 1 = 0.25$. This is sometimes referred to as the *risk value*. We're keeping the example very simple, so we can walk through the logic of it. In English, this equation says that although there's only a 25% chance the threat will occur, there's a 100% chance it will affect us when it does occur.

Next, we move to the other side of the diagram and look at the *impact*. In this example, we're assuming that when the power goes out, it's out in the entire facility and it's out for 2 days. (Of course, if your building loses power every 4 years for 2 days, you should be having a chat with your power company.) What is the cost of not being able to work for 2 days? Your servers are down; your employees cannot access desktops, printers, or IT resources; there are no lights; no heating/cooling—no productivity. How many sales do you lose? What impact does this have on your customers? Your inventory? Your order backlog? This is where having your assessment team comes into play as members from different parts of the organization can help you make these assessments. This is some of what we'll cover in [Chapter 5](#), but for now, let's assume the following for a small business:

- Lost sales per day: \$18,000, total cost \$36,000 for the outage
- Fixed costs per day: \$4200, total cost \$8400 for the outage
- Damage to reputation: unspecified, arbitrary value set at \$2000, total cost: \$4000

Note that you may decide to set a value for damage to reputation at a daily rate just to give you some measurement that can be used consistently. If you have a method for calculating this to a more exact figure, feel free to use it. Otherwise, a daily rate for these unspecified costs may help by providing an “order of magnitude” estimate. In this case, we're using \$2000 per day and this amount will be used for any “damage to reputation” suffered from any threat source. Therefore, we'll be able to understand the impact of a 1-day event versus a month-long event. Though there is a multiplier effect that occurs with an extended period of downtime or outage and you may choose to address this, we're using a single value. We also recognize that the use of an arbitrarily set value, such as \$2000 per day for “damage to reputation,” is qualitative in nature. Still, assigning a dollar value to it and using it consistently across all threats will mitigate that to some extent. Now, let's calculate our impact costs: $\$36,000 + \$8400 + \$4000 = \$48,400$.

So now we know that if this threat occurs, it will cost the company \$48,400. Now, let's input that into our earlier equation as shown here and reflected in [Figure 4.7](#): $0.25\% \times \$48,400 = \$12,100$.

**FIGURE 4.7**

Total risk cost per year of power outage from lightning strike.

If you know that your annualized risk cost is \$12,100 for a power outage from a lightning strike, it's much easier to determine whether a \$10,000 backup power generator makes sense. You may also decide that it's worth investing \$5000 to have the power company install equipment that will make your power system less likely to fail. Finally, it helps you decide whether a \$1000/year insurance rider to cover utilities outages is a good investment or not. Remember, you can accept, avoid, reduce, or transfer risk. In this case, transferring via an insurance policy would be a good investment—\$4000 over 4 years vs. \$12,100. Still you could choose to take mitigating steps and accept the risk. These are your risk mitigation strategies that we'll develop in [Chapter 6](#). You can see that having an annualized value can certainly help you and your team come up with a number of reasonable risk mitigation strategies. Clearly, a solution that costs \$100,000 is probably not a good investment because it would take you about 8 years to recoup your investment ($\$100,000/\$12,100=8.26$). How cost-effective is additional equipment for \$5000 to make the problem go away? Probably very effective and as such, an excellent investment. We use terms like "probably" in this case because there may be mitigating circumstances we don't know about. For example, suppose that \$5000 solution costs \$1000 annually to maintain. Is it still a good deal? What if it lasts for only 4 years? Is it still a good solution? Without knowing all the details, it's hard to make a solid assessment. This is part of what's covered later in [Chapter 6](#). For now, we'll use straight numbers and assume that a \$5000 solution is just that—and as such, it would make sense.

The second thing to consider when looking at potential mitigation strategies is that there may be additional *benefits* to a particular solution. If, for example, the \$100,000 solution would also extend the serviceable life of all computers in the building by 1.37 years, it might be a better solution. You'd need to calculate the value

of extending all computers' serviceable life by 1.37 years and compare that with the cost of the solution. Another possibility is that the \$100,000 solution meets industry requirements that will be enforced starting in 3 years; the \$5000 solution does not meet requirements. Now what's your best option? This is certainly a place where getting your finance folks into the loop will help; they can develop what-if scenarios for your different options and you, as the IT expert, can help everyone understand the additional benefits (or risks) that come with various solutions. Some solutions you'll consider may inject a new risk into the mix; some solutions will mitigate risks in areas you hadn't expected. Keeping your eyes open for possibilities will help you maximize your results.

Will calculating your values be this easy? Probably not. You most likely have far more factors to consider when calculating the cost of an outage, for example. However, you can also decide as a team what degree of accuracy you require in order to create an effective plan. If exact numbers are not required, you can use a qualitative model.

TIP**Triage**

When working through your assessment, you're going to need to use a technical term used in healthcare known as *triage*. Triage is simply the act of quickly assessing and treating the most critical first. In the case of your assessment, start with the things that are most likely to occur and have the biggest impact. Fire and power outages are usually at the top of the list followed by loss of cooling in the data center. If you work through your quantitative (or semiquantitative) assessment starting with these high-priority items, you'll not only address the key items first but also be able to look at how some of these mitigation strategies might enhance current operations. When you can leverage a solution to meet multiple needs, you are effectively leading your IT organization and utilizing resources effectively (i.e., good use of staff time, good use of funds allocated for operational or capital purchases, etc.).

Qualitative threat assessment

Qualitative assessments use words or relative values to express risk, cost, and impact. The first step in using a qualitative system is to define the scale you want to use and then use it consistently. You can use systems like those shown in [Table 4.5](#) or [Table 4.6](#) (Hash, 2002, p. 21), or you can develop a customized scale to fit your needs.

Table 4.5 Qualitative Scale Example

Numeric	Frequency	Impact
6	Constant	Extremely high
5	Very frequently	Very high
4	Frequently	High
3	Infrequently	Low
2	Very infrequently	Very low
1	Never	Extremely low

Table 4.6 NIST Likelihood Matrix

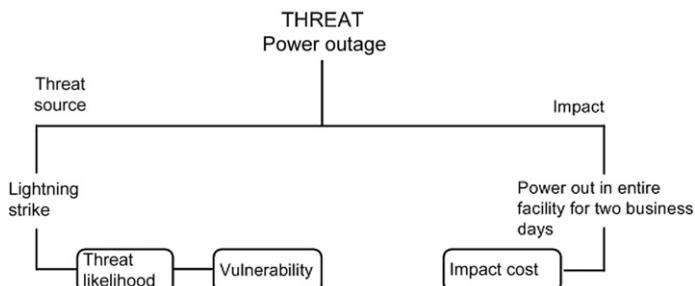
Likelihood Level	Description
High	The threat source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective
Medium	The threat source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability
Low	The threat source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised

One suggestion is that you use a scale with an *even* number of variables; the one we used has six. This forces a choice between two options, “frequently” or “infrequently” or “high” or “low,” and can prevent someone from selecting the middle value (present when there are an odd number of choices) to be safe. Whatever scale you use or whatever number of variables you opt to use, be sure to define these elements to everyone’s satisfaction. It’s important to have a shared understanding of what these values mean so that when you’re using them for the risk assessment, you’re all using them in the same manner.

When assessing likelihood, you can define a scale that works for your organization. [Table 4.6](#) shown previously is the likelihood matrix developed by the National Institute of Standards and Technology. This matrix is specific to security risk vulnerabilities but provides a good example of how to define these types of qualitative assessments.

Now, let’s look at the same example we looked at previously only this time, let’s use the qualitative method. First, we map out the threat, as shown in [Figure 4.6](#) earlier and repeated here in [Figure 4.8](#) for your convenience.

Now let’s assign values. Let’s say we know that these outages happen once every 4 years. We might determine that outage deserves a rating of “infrequently,” and we can assign it the value of 3. Using the same system, we can say that the vulnerability

**FIGURE 4.8**

Power outage threat assessment—semiquantitative.

when the storm hits is 100% (per our quantitative assessment), which would place it on the scale as “extremely high” and give it a rating of 6. So, the left side of our equation = 2, 6.

On the right side, we want to assess the impact cost, but we’re not using exact dollar amounts. We could say well the cost of being down 2 days would be about average because we can catch up later without too much trouble and our fixed costs aren’t through the roof. Therefore, you might assess your impact cost as being “low” or a level 3. If you take the average of these, you have $2 + 6 + 3 = 11 / 3 = 3.66$. This puts it on the scale at “high” if we round up (any number above 3.5 would be 4, any number 3.5 and below would be 3). This is depicted in [Figure 4.9](#).

You might decide you don’t like converting these assessments to numbers—that’s fine. You might also decide you want a scale with a few more options, say a 10-item scale—that’s fine, too. The point here is that you can make assessments without hard dollar figures and still come up with a meaningful assessment. In the case of the power outage, you might argue that the value of 6 for “very high” under vulnerability skews these data in a way you don’t like because it’s not weighted. However, when you do this assessment using this scale for a number of threat sources, you may find that your data shake out as expected. For instance, you might perform this same assessment on a power outage from an internal failure and decide its total risk value is 3.5. You can then look at these two sources and ask, “Do we really have a slightly greater risk value if we experience a two-day power outage every four years versus our internal power failure that could take us down for a week but only happens once every eight years?” If the answer is no, you may want to go back and better define your scale or reassess the values you used

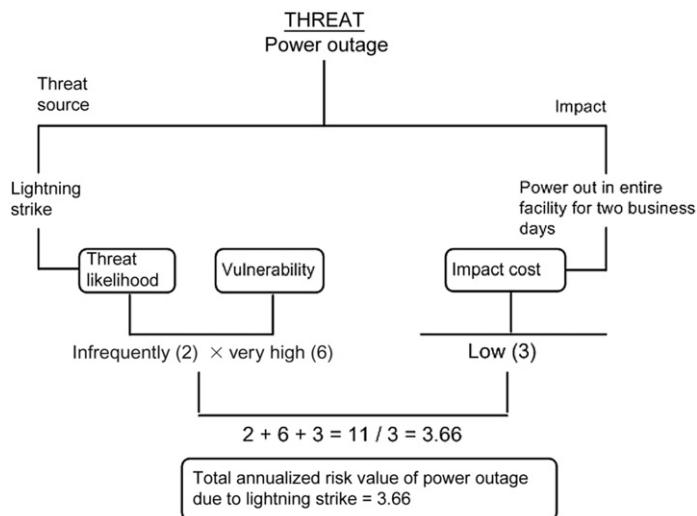


FIGURE 4.9

Total risk value per year for power outage from lightning strike.

in one or the other assessment. However, in most cases what you'll find is that after a few of these, you get the feel for the scale and you begin to see that your data track with the reality of the situation. Once you're confident your scale is working, you can tackle the more difficult or more intangible threat sources.

Another rating scale could range from 1 to 100 to give you a bit more fine-tuned result. An example of this is shown in [Figure 4.10](#). If you really want to keep it simple, you can use a five-element, single-rating system and come up with something similar to that shown in [Figure 4.11](#).

In [Figures 4.10](#) and [4.11](#), the costs are delineated in terms of the relative impact cost of (1) loss of revenue, (2) damage to servers, (3) damage to the database, and (4) damage to user computers. These two examples assume that the servers were able to

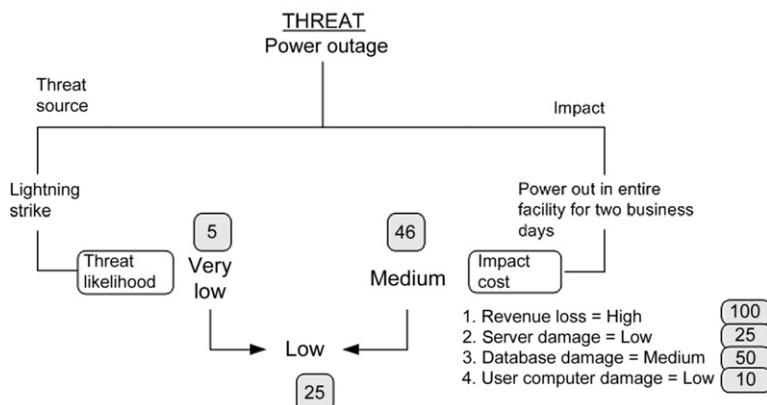


FIGURE 4.10

More refined qualitative scale.

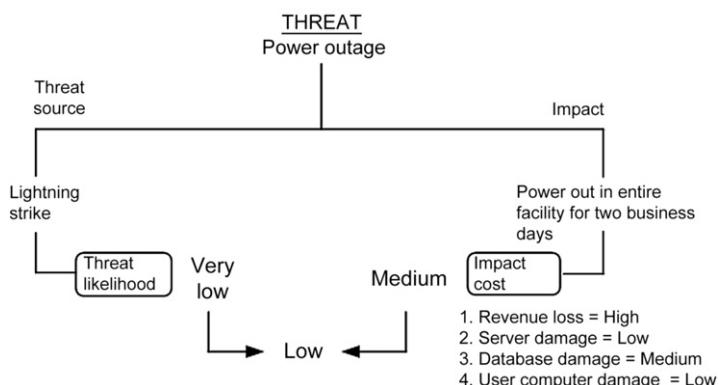


FIGURE 4.11

Simple qualitative scale.

shut down without incident but that there was damage to a database as a result of the sudden loss of power. This is just an example to show you how you might assess your IT components. You might also choose to delineate things like firewalls, routers, and cabling in your list, if it's helpful in making a qualitative assessment.

Whether you choose to use a *quantitative* system or a *qualitative* system, be sure everything is clearly defined and that you apply these ratings consistently. What you'll end up with at the end of your risk assessment phase is a chart, table, or document delineating each threat, the likelihood of that threat, the vulnerability to that threat, and the impact should that threat occur. From there, you'll develop your risk mitigation strategies because you'll be able to see the big picture and create optimal solutions for your firm.

CRITICAL CONCEPT

Assessment Scales

According to the U.S. Department of Commerce's National Institute of Standards and Technology (NIST), Special Publication 800-30 Revision 1 "Guide for Conducting Risk Assessments" (September 2012), there are several ways to complete your assessment. In this section, we'll look at several different approaches you can use. If you're interested in digging deeply into the risk assessment portion of your plan, you would be wise to read the entire 95 pages of 800-30 R1 ([National Institutes of Standards and Technology, 2012](#)).

You must first determine whether a threat is adversarial (someone's out to get you) or nonadversarial (act of nature, error). That distinction, in itself, can be helpful in focusing you on potential threats. We'll assume for this section that we're looking just at nonadversarial events. We can create a semiquantitative assessment using this matrix, found in Appendix G of the NIST 800-30 R1 document, and shown in Table SB.1.

Now, let's look at the likelihood of a threat event resulting in an adverse impact. That's a similar type of semiquantitative approach, shown in [Table SB.2](#).

Finally, you can take the data from these two previous assessment scales and merge them to understand the overall likelihood, as shown in [Table SB.3](#).

This merging of two semiquantitative assessments into a qualitative result is one approach. You could also use numerical values from the previous tables to generate a numerical value and correlate that into likelihood statements. The key is to ensure you're using the same methodology throughout so that when you complete your risk assessment, you'll have a result that you can use to plan which threats you want to address and which are not worth the effort. Note that if you choose not to mitigate or address a risk, make a note of the rationale for future reference. That way, you'll know it was a conscious decision and not an oversight.

VULNERABILITY ASSESSMENT

A *vulnerability* is defined as the weakness, susceptibility, or exposure to hazards or threats. A vulnerability in a software program, for example, is a weakness that poses a problem if discovered and exploited. Vulnerabilities in the case of business continuity and disaster recovery are the various areas of the business and IT systems that are exposed or susceptible to the threats defined in the previous assessment phase. Vulnerabilities can be exploited intentionally or triggered unintentionally. As you know, a change to a security setting in one area of the operating system can create

Table SB.1 Assessment Scale—Likelihood of Threat Event Occurring

Qualitative Value	Semiquantitative Values	Description
Very high	96-100	Error, accident, or act of nature is almost certain to occur; or it occurs more than 100 times per year
High	80-95	Error, accident, or act of nature is highly likely to occur; or it occurs between 10 and 100 times per year
Moderate	21-79	Error, accident, or act of nature is somewhat likely to occur; or it occurs between 1 and 10 times per year
Low	5-20	Error, accident, or act of nature is unlikely to occur; or it occurs less than once a year but more than once every 10 years
Very low	0-4	Error, accident, or act of nature is highly unlikely to occur; or it occurs less than once every 10 years

Table SB.2 Assessment Scale—Likelihood of Adverse Impact

Qualitative Value	Semiquantitative Values	Description
Very high	96-100	If the threat event is initiated or occurs, it is almost certain to have adverse impacts
High	80-95	If the threat event is initiated or occurs, it is highly likely to have adverse impacts
Moderate	21-79	If the threat event is initiated or occurs, it is somewhat likely to have adverse impacts
Low	5-20	If the threat event is initiated or occurs, it is unlikely to have adverse impacts
Very low	0-4	If the threat event is initiated or occurs, it is highly unlikely to have adverse impacts

Table SB.3 Assessment Scale—Overall Likelihood

Likelihood of Threat Event Occurrence	Likelihood Threat Event Result in Adverse Impact				
	Very Low	Low	Moderate	High	Very High
Very high	Low	Moderate	High	Very high	Very high
High	Low	Moderate	Moderate	High	Very high
Moderate	Low	Low	Moderate	Moderate	High
Low	Very low	Low	Low	Moderate	Moderate
Very low	Very low	Very low	Low	Low	Low

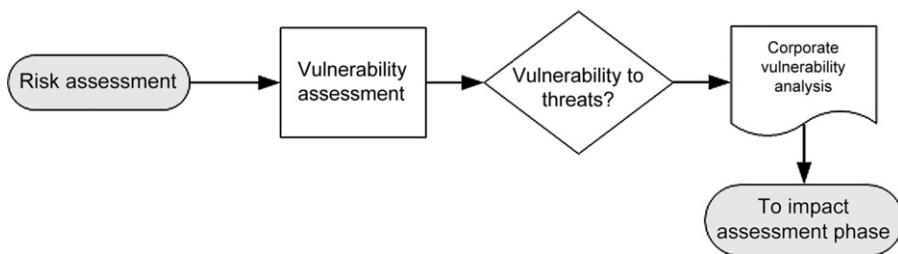


FIGURE 4.12

Vulnerability assessment phase of overall risk assessment.

a vulnerability elsewhere in the system without the IT administrator even being aware of it. The analysis of vulnerabilities in BC/DR planning must include IT systems, but it should not be limited to IT systems. Clearly, people, processes, technology, and infrastructure are vulnerable to the threats delineated earlier. Therefore, while our focus will continue to be IT-related data, we have to cast a wider net so that the BC/DR plan is complete.

The result of the threat assessment becomes the input to the vulnerability assessment, as shown in [Figure 4.12](#), the second section of the larger image presented at the beginning of the chapter in [Figure 4.2](#).

As you may recall at the outset of this chapter, we discussed selecting an approach for your analysis. We asked “Do you want to look at your risk from a threat orientation, an asset/impact orientation or a vulnerability orientation?” We’ve looked at threats and discussed how those threats might impact your organization. If you’re working from a threat or asset/impact orientation, you should have the data elements needed. Regardless of the approach you take, you will need to look at your vulnerabilities, which is the focus of this section.

Some people like to break out this assessment into likelihood of occurrence and vulnerability to the threat based on the likelihood. Others prefer to keep it simple and use a straightforward vulnerability assessment. The value in breaking it out, as shown in the previous section, is that the likelihood of something occurring may be high, but the vulnerability to that threat source may be low. Conversely, you could say something is unlikely to occur but if it does, you are very vulnerable, as would be the case with a major earthquake or hurricane. Thus, the value in breaking it out into likelihood and vulnerability for each threat source might be that you can address those issues unlikely to occur but to which you’re very vulnerable as a separate element of your BC/DR planning. Another approach is to simply look at the vulnerability as the likelihood of occurrence and then assess the potential impact through the BIA.

Once you have your threat sources listed in detail, you may choose to subdivide your list and assign segments to appropriate subject matter experts. For example, you could give the entire list to four subteams, each specializing in a particular area such as IT, facilities, finance, HR, and/or operations. You could also create subteams to look at each threat source from the people, process, technology, and infrastructure

framework. You could divide your team in two and have half address the internal threat sources and the other half address the external threat sources. Of course, before you send each team off to do its own work, you should have a detailed list of what you expect them to accomplish, what a successful outcome looks like and a deadline or timeline for delivery (if that sounds suspiciously like a small project plan, you're right on track). Without a clear set of objectives, tasks, and milestones, this portion of the project could simply meander. It should be a relatively fast, focused effort. As it will need to be refreshed on a frequent basis, this body of work shouldn't take a long time to complete.

Whatever way you choose to subdivide the work, you should hold a final full team review to ensure there are no gaps or discrepancies. If time and resources allow, you could have each group's deliverable be handed to another subgroup so that each group's work is reviewed by another group (i.e., Group A's results are reviewed by Group B; Group B's results are reviewed by Group C; Group C's results are reviewed by Group A). The point is not to call out another group for errors or omissions but simply to make sure every angle has been considered and reviewed appropriately with fresh eyes.

TIP

Understanding the Bigger Picture

The Business Continuity Institute (www.thebci.org) provides certification in business continuity planning ([The Business Continuity Institute, 2013](#)). In conjunction with the Disaster Recovery Institute (www.drii.org), they have developed and published a set of guidelines that describe best practices ([Disaster Recovery Institute, 2013](#)). These are focused not on IT but on the overall organization, which can be helpful in providing you a broader view of BC/DR. You can purchase the Good Practice Guideline from BCI by visiting the Web site.

People, process, technology, and infrastructure

We've pointed out that BC/DR planning activities require research into the impact on people, processes, and technology. In the case of BC/DR plans, infrastructure might be a fourth category that could be included (some might include it in technology). Infrastructure in this case includes the building itself, heating/cooling systems, and power to the building, among others. In other words, it's outside the normal scope of IT (people, process, technology), but these areas are vital to the success of your IT operations and must be included in your planning. When you're assessing your business risks, these four areas come into play. When you begin your vulnerability assessment, these four areas should also be considered to ensure there are no gaps or erroneous assumptions about what is and is not covered.

People

In the threat assessment phase, we saw that people can pose a threat to IT system in a number of ways. Now, we shift our focus to how people are vulnerable to various threat sources. When performing a vulnerability assessment, you need to ask and

answer the question: How vulnerable are our staff and the people in our community to these threats we've identified? Some threats may not impact people beyond their ability to be productive at work (a 1-hour power outage, for example). Other threats may not only impact your staff but the surrounding community, as is the case in major natural disasters. If you look at how vulnerable people are to the various threats, you can determine your overall risk with each threat source. For example, people are particularly vulnerable to phishing and social engineering. This is not a system's vulnerability—there is only so much a system can do to stop a person from deciding to respond to a sophisticated (and ever-changing) phishing or social engineering ruse. So, if someone willingly hands over a "power user" account name and password, the system is vulnerable, but only because a person was vulnerable first. Looking at threats and vulnerabilities in this light will help not only in determining the overall risk value of each threat source but also in developing effective mitigation strategies later.

Process

How vulnerable are your business and IT processes to these various threat sources? In some cases, your processes may not be very vulnerable at all, as might be the case in a brief power or server outage. You already have processes in place for normal IT operations, and minor outages and equipment failures are probably covered in your standard operating procedures. Other processes might be very vulnerable, such as is the case when a natural disaster occurs. In those cases, it's typical that all business and IT processes are vulnerable because there is nothing about a disaster that is "business as usual." For example, how would you handle, process, and fulfill customer orders after a disaster that made your building uninhabitable for weeks? What could you do to get back up and running? How would your processes have to flex or change? As you review the vulnerability of each of your critical business processes to the various threat sources, you'll begin to see which processes need to be reviewed, revised, or reinvented for use in an emergency. We'll discuss this in the BIA as well as in the mitigation strategy development chapters.

REAL WORLD

Using Standard Work to Guide Effort

There's a concept in the *Lean* methodology called Standard Work. It is the standardized set of tasks a person performs each day, week, or month. That standard work varies depending on the person's role within the organization. If your company uses standard work (or anything similar), you can use it as part of your assessment of process vulnerabilities. In short, any process that is well-defined, well-documented, and ingrained into the daily activities of the company becomes a valuable tool in business continuity. If you have clearly defined work products, it's much easier to understand how these tasks would be impacted by various threat sources. It's also much easier to bundle your standard work into your business continuity plans by determining which standard work tasks could continue after an IT outage. You would also be able to more easily determine which tasks would have to change and in what manner they should change. With standard work defined, many process questions are easily answered.

Technology

Clearly, technology is vulnerable to numerous threat sources and as an IT professional, you're probably well aware of the most common ones. How vulnerable is your server to an internal or external attack? How vulnerable is your Web server? These are questions you've probably already addressed through standard IT security assessments and operating procedures. As you go through this particular risk assessment process, you also need to broaden your outlook a bit and ask how vulnerable your systems are to the disaster threat sources such as floods, hurricanes, and fires. Since your perspective is an IT-centric perspective, you probably have the most detailed information available on this subject. As you go through the vulnerability assessment, these data should be captured. Don't assume that your standard operating procedures have addressed the vulnerabilities and don't assume that your current "emergency plans" will be adequate for all threat sources. Approach this topic with fresh eyes to see what else you can add to the process.

In addition, you should look at non-IT technology platforms. In some organization, such as hospitals, there are numerous technologies that tie into IT infrastructure but may not be under the direct control or management of the IT department. Imaging systems, specialized medical systems (hemodynamics, lab systems, pharmacy systems, etc.), movable and nonmovable medical equipment, phone systems, paging systems, nurse call, and cable TV systems are examples in healthcare of systems that may or may not be under IT control. Some of these items may be included in your vulnerability assessment, some may not be appropriate for your plan. However, it's important to look beyond the walls of the data center for systems that you should be either including in your plan or ensuring someone else has in their plan.

Infrastructure

Clearly, infrastructure is vulnerable to some threat sources and not to others. A building is vulnerable to flooding if it's in a low-lying area or in a location that could flood. If the building is at the top of a hill or at the highest point in a geographical region without rivers or lakes, there's a good chance it is not vulnerable to external flooding. However, any building could potentially be vulnerable to internal flooding (broken plumbing within the facility). As you review your threat sources, your facilities expert will likely be in the best position to understand the vulnerability of the company's infrastructure to threat sources. As a team, you may all want to think about the vulnerability of external infrastructure in your area to threat sources as these will clearly impact your business. For example, is there a seaport, power plant, airport, or dam nearby that could be vulnerable to the threat sources? If so, what impact would these have on your business?

Vulnerability assessment

A vulnerability assessment can be qualitative or quantitative, but in many cases, companies use a qualitative assessment or semiquantitative method. It's often difficult to put an exact number on a vulnerability, so using a rating scale such as those

shown in [Table 4.5](#) is usually most effective. The key is to get an accurate picture of the vulnerability to each threat source and to compare them using a consistent methodology. At the end of the planning and assessment phases, you'll need to address these risks and vulnerabilities in the order of importance. A consistent rating system will ensure you deal with the most important elements first. When viewed in total, you'll be able to make any needed adjustments to individual vulnerability ratings. For example, you might use a scale of 1-100, with 100 being the most vulnerable and 1 being the least vulnerable. When you view your final list of threat sources and vulnerabilities, you might see that some of the vulnerability ratings are out of sync with the rest—those can be modified so that your overall vulnerability picture is accurate. As with other rating systems, be sure that you define it and then use it consistently. Also, because you may choose to subdivide the work, it's vital that everyone have the same understanding of the ratings and apply them in the same manner.

A vulnerability assessment typically uses various data sources as input. These include prior risk assessments, security requirements, security test results, regulatory requirements (HIPAA, GLBA, etc.), and prior problems. According to the National Institute of Standards and Technology's "Risk Assessment Guide for Information Technology Systems," the types of vulnerabilities that exist and the methodologies needed to determine vulnerabilities will vary depending on the nature of the system and, in particular, the phase of the SDLC it is in. Accordingly,

- If the system has not been designed yet, the vulnerabilities assessment should focus on the organization's security policies, planned security procedures, system requirements definitions, and vendor's (or developer's) security product analyses (white papers, etc.).
- If the system is in the process of being implemented, the vulnerabilities assessment should focus on more specific information such as the planned security features; security and design documentation; and the results of system certification, testing, staging, and evaluation.
- If the system has been implemented and is operational, the vulnerabilities assessment should include the analysis of the system's security features, security controls (technical, operational, and environmental), and standard IT operating procedures.

However, we are looking beyond just IT systems to the larger organization, so we need to expand our view of vulnerabilities just a bit. Even though these other areas may fall outside your direct line of authority, you should be familiar with them so you can participate fully on the BC/DR planning team or head it up effectively, whichever the case.

The vulnerability assessment can be accomplished using the same methods described earlier in the threat assessment: questionnaires, interviews, document reviews, and research. In addition, you can develop scenario questions based on the identified threat sources to help you assess vulnerability. For example, you might

Table 4.7 Vulnerability Assessment Sample

Statement	High	Medium	Low
1. If the plumbing pipes in the building were to burst, what is the vulnerability of our IT systems to water damage?			
2. If the building were to catch on fire, what is the vulnerability of our IT systems to water damage from fire suppression systems?			
3. If the building were to become flooded by heavy rains, what is the vulnerability of our IT systems to water damage?			

ask your subject matter experts to respond to a set of questions similar to those shown in [Table 4.7](#).

As you can see from these sample statements, we've identified three threat sources for water damage/flooding: internal flooding, water damage from fire suppression systems (which might not be in the server room but adjacent to or above the server room), and external flooding. We have also not asked (here) what the likelihood is of these threats occurring. We are simply assessing how vulnerable we believe these systems would be should these events take place.

Once the vulnerability assessment is complete, you can develop a risk value for each of the threat sources. This risk value can be derived numerically if you've used either a quantitative system or a qualitative system that uses numbers for the scale (semiquantitative).

Once the vulnerability assessment is complete, you can begin to analyze the data. This analysis should include a thorough review of all the threat sources, likelihood, and vulnerabilities ratings. A final assessment of the data should allow you to adjust ratings that seem out of balance with other data, which is sometimes the case with qualitative assessments. The interim "risk value" for each threat source should be reviewed and verified. The value is considered interim at this point because we have not yet conducted the impact analysis. Therefore, you will have a "risk value subtotal" in a sense, which can be reviewed at this juncture. If you recall, the risk equation can be stated as:

$$\text{Risk} = \text{Threat} + (\text{Likelihood} + \text{Vulnerability}) + \text{Impact}$$

Rather than repeat the material presented in the previous section, we'll leave it to you to go back through your threat source list and perform the vulnerability assessment. The result of this phase is a document that lists, at minimum:

1. All potential threat sources (except those purposely excluded).
2. The likelihood of each threat source occurring.
3. The vulnerability of your company and IT systems to those threat sources.
4. Interim risk value for each threat source.

The deliverable from this phase is the vulnerability assessment and analysis, as shown in [Figure 4.13](#). These data are used as the input to the BIA phase, covered in

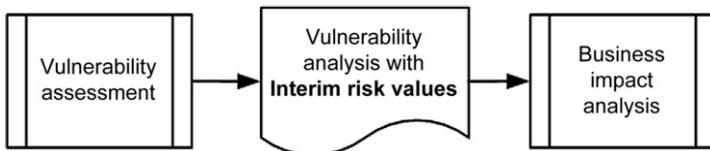


FIGURE 4.13

Deliverable from vulnerability assessment.

detail in [Chapter 5](#). You might have a team meeting to review the final data and present a report to your project sponsor and your corporate executives at this juncture. This can help bring visibility to your efforts and progress. The document can also be provided to various subject matter experts within the firm for one final review to ensure there are no gaps or errors at this point in the process. If you have a formal sign-off procedure in place, you may want to obtain formal approval for this document before moving onto the next phase of your project plan.

LOOKING AHEAD . . .

Business Impact Analysis

The next step in the risk assessment is to perform the BIA. It is in this phase that you will look at the company's business processes (including those associated with IT functions) and develop a rating or assessment of the criticality of those systems. Then, you can determine which business functions must be restored and in what order. Clearly, in the aftermath of a disaster or business disruption, functionality must be restored in a methodical and logical manner and the BIA will provide that roadmap. The input to the BIA is the output from this phase of the assessment, so don't launch your BIA until you've completed this phase to your satisfaction.

SUMMARY

Business continuity and disaster recovery planning begins with a thorough risk assessment. Risk assessment is part of a larger risk management process found in most businesses. The four major components of the BC/DR risk assessment are threat assessment, vulnerability assessment, impact assessment, and risk mitigation strategy development. In this chapter, we focused on threat and vulnerability assessment. In order to perform a thorough threat assessment, you need to look at threats and threat sources both internal and external to the company. It is often helpful to assess risk based on the potential risks to people, process, technology, and infrastructure. People are not only the company's employees but also its vendors, partners, customers, and the larger community in which it operates. Processes are all the business and IT processes used in the business. Processes are used to generate revenue, track expenses, and manage operations from facilities management to human resources and beyond.

From an IT-centric viewpoint, the key components to address in the risk assessment are people, process, technology, and infrastructure. It includes hardware,

software (OS and applications), system interfaces (internal, external connection points), people who support the IT systems, users who use the IT systems, data, information and records, processes performed by the IT systems, system's value or importance to the organization (system criticality), and system and data sensitivity (confidential, trade secret, medical data, etc.). The operating environment in which the IT systems function includes a wide variety of elements. Among them are the functional and technical requirements of the systems; security policies, procedures, and controls; network topology and information flow diagrams, data storage protection policies, procedures, and controls; encryption, physical, and environmental controls.

The methods used to gather data for any of the assessment phases typically include questionnaires, interviews, document reviews, and research. Questionnaires not only can be helpful in structuring desired input but also can have the downside of containing built-in biases, often unintentionally. Interviews can be conducted with subject matter experts and yield more useful information than questionnaires but may also generate a lot of tangential or unneeded data. Reviewing documents and performing research can supplement the questionnaire and interview process.

Once you've defined the methods you'll use to gather the necessary data, you can begin your review of various threats. We discussed many different types of threats that fall into three primary categories: natural and environmental threats, human-caused threats, and infrastructure threats. Infrastructure threats are caused by either natural or human causes, and it's important to delineate these because they involve people, processes, and technologies outside the company and the company's control. As such, they sometimes can be overlooked in IT BC/DR planning. Natural threats include those we might commonly think of such as fire, flood, or earthquake, but we also discussed other less obvious threats including volcanoes, droughts, and pandemics. Human-caused threats can be intentional as in the case of terrorism, labor disputes, or workplace violence, or they can be unintentional as can be the case with fire, flood, or a security breach. Infrastructure threats include those to the building as well as external to the building and the company. Public transportation including roads, rails, seaports, and airports are all external infrastructure elements that need to be assessed. Other external elements include threats to water and food supplies, biological and chemical hazards, and public utilities such as the power grid, petroleum and fuel supplies, or telecommunications.

The threat assessment methodology begins with a list of all potential threats and threat sources. Each threat source is then evaluated. Some people like to assess likelihood of occurrence and vulnerability to the threat; others prefer to include both likelihood and vulnerability in a single assessment. Regardless of whether you choose to break them into two distinct ratings or one rating, the likelihood of occurrence and vulnerability rating(s) should be assessed for each threat source. The argument for making two separate assessments is that a threat may have a high likelihood of occurring, but your company and its people, processes, technology, and infrastructure may not be vulnerable to those threat sources. Others would argue that if there is a low vulnerability, the likelihood of occurrence doesn't come into play and should

therefore not be assessed separately. Either method is acceptable as long as you make a conscious decision as to how to proceed and use the same process throughout your risk assessment cycle.

You can perform a quantitative assessment in which actual values such as dollars or frequency are known. The benefit to this type of assessment is that you can generate hard data that can be used in a standard cost/benefit analysis. The downside is that not all values are easy (or possible) to derive, and an unacceptable amount of time or money may be required to generate that data. You can also perform a qualitative assessment in which values are relative. These types of assessments use labels such as high, medium, and low or an arbitrary numbering system such as 1-100 where 1 = no chance or extremely low, 50 = medium chance or about average, and 100 = will occur or extremely high chance. These kinds of systems are much easier to implement but typically generate less specific data that are unsuitable for a standard cost/benefit analysis. In analyzing threat data, qualitative measurements are often sufficient to generate a clear picture of the threats facing the organization.

The vulnerability assessment may include the likelihood of occurrence or it may be a separate rating. However, the same processes can be used to evaluate vulnerability as were used to assess threats. Questionnaires, interviews, document reviews, and research can help in generating data needed to assess the actual or relative vulnerability to a threat. This rating is compiled with the threat assessment data and is used as the input to the BIA phase, discussed in [Chapter 5](#).

The bottom line is that your risk assessment activities will end up, generating a list of threats and threat sources that you'll be able to evaluate. You can sort the list and decide which risks you need to address, which can be accepted, and which should be transferred. You'll have the data to make this decision once you complete the BIA, the third major step in the risk assessment process.

KEY CONCEPTS

Risk management basics

- Risk management is a business process used to manage all kinds of risks facing business today.
- A standard risk management process includes four phases: threat assessment, vulnerability assessment, impact assessment, and risk mitigation strategy development.
- When assessing threats for a business continuity and disaster recovery plan, you can use the framework of people, process, technology, and infrastructure to ensure you're looking at all aspects of your business.
- IT-specific risk management is related to three objectives: securing systems more fully, enabling management to make sound IT purchasing decisions, and enabling management to authorize/accredit IT systems.
- IT risk management often uses the framework of the SDLC model. As you perform your BC/DR assessments, systems being considered, developed, and

implemented must be assessed. Some BC/DR risk controls may already be in place, others can be incorporated in the SDLC process.

- Risk can be expressed as an equation: Risk = Threat + (Likelihood + Vulnerability) + Impact.

Risk assessment components

- Risk assessment components include threat, vulnerability, impact, and mitigation. In this chapter, we focused on threat and vulnerability assessments.
- Threats typically are categorized as natural/environmental in nature or human-caused. Threats to the infrastructure, caused by both natural and human actions, are delineated separately in order to ensure they are adequately addressed.
- Natural and environmental threats to the business must be assessed in terms of not only how they directly impact the company but also how they indirectly impact the company. Disasters or business disruptions to your business customers, partners, and vendors can have a major impact on your business and must be assessed.
- Human-caused events include not only acts of terror, theft, and sabotage but also things you might not consider such as labor disputes or workplace violence.
- Threats to infrastructure are typically outside your direct control, but they often have a direct (or indirect) impact your business. These include damage to airports, seaports, highways, and rail stations as well as problems with the delivery of utilities.
- Though IT-specific threats are caused by either natural events or human actions, we listed them separately in order to delineate the various threats to be considered in an IT-centric plan.

Threat assessment methodology

- Four major types of tools can be used to assess threats: questionnaires, interviews, document reviews, and research. Each will yield specific data. A comprehensive review will use all four methods and combine data.
- Questionnaires can have built-in biases that may limit the information gathered.
- Interviews can avoid the built-in bias but can generate tangential data that either get you offtrack or simply are not helpful in your BC/DR planning.
- Document reviews and research should be a part of the threat assessment process to review what is already known and to gather statistical and factual data pertinent to your BC/DR plan.
- Threats can be assessed using quantitative or qualitative assessments. A quantitative assessment uses hard numbers that can be used in a cost/benefit analysis. A qualitative assessment uses arbitrary numeric values or labels such as high, medium, and low to assign a relative value. Although this cannot as easily be used in a cost/benefit analysis (if at all), it is often easier to derive these types of values.
- Threats should be assessed with regard to the various threat sources, the likelihood of occurrence and the vulnerability of an asset to the threat source.

- Some people may prefer to assess threat with likelihood and vulnerability assessed as two separate values; others may prefer to assess these two traits as one value. Either method is acceptable as long as you consider both the likelihood of an occurrence and the vulnerability of an asset to that occurrence.

Vulnerability assessment

- The vulnerability assessment uses the output of the threat assessment phase as its input. The complete list of threats and threat sources is evaluated with an eye toward the likelihood of such an occurrence and the vulnerability of corporate assets to those threats.
- Corporate assets and operations may be highly vulnerable to an event that may be unlikely to occur, such as an earthquake or a volcanic eruption. As these factors are evaluated, you can create an overall risk value for each threat source.
- The data from the vulnerability assessment are analyzed and are used as input to the business impact assessment phase, discussed in Chapter 5.
- The key at this juncture is to be inclusive and not rule out anything until the assessments are complete. This helps prevent inadvertently creating gaps in your BC/DR plan.

References

- Bumiller E, Shanker T. Panetta warns of dire threat of cyberattack on U.S. <http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html>; 2012 [Retrieved May 26, 2013], from The New York Times.
- Carnegie Mellon Computer Emergency Response Team. Operationally critical threat, asset, and vulnerability evaluation. www.cert.org/octave; 2013 [Retrieved May 26, 2013], from Carnegie Mellon Computer Emergency Response Team.
- Center for Internet Security. Home page. <http://www.cisecurity.org/>; 2013 [Retrieved May 26, 2013], from Center for Internet Security.
- Computer Security Institute. Home page. <http://www.gocsi.com>; 2013 [Retrieved May 26, 2013], from Computer Security Institute.
- Disaster Recovery Institute. Home page. <http://www.drii.org>; 2013 [Retrieved May 26, 2013], from Disaster Recovery Institute.
- Federal Bureau of Investigation. <http://www.fbi.gov/cyberinvest/cyberhome.htm>; 2013.
- Federal Emergency Management Agency. Home page. <http://www.fema.gov/business/nfip/>; 2013 [Retrieved May 26, 2013], from Federal Emergency Management Agency.
- Federal Emergency Management Agency. Response and recovery. <http://www.fema.gov/response-recovery>; 2013 [Retrieved May 26, 2013], from Federal Emergency Management Agency.
- Flu.gov. Business planning. <http://www.flu.gov/planning-preparedness/business/index.html#>; 2013 [Retrieved May 26, 2013], from Flu.gov.
- GIAC. Global information assurance certification. <http://www.giac.org/>; 2013 [Retrieved May 26, 2013], from GIAC.
- Hash JS. Risk management guidance for information technology systems. <http://www.itl.nist.gov/lab/bulletins/bltnfeb02.htm>; 2002 [Retrieved May 26, 2013].

- International Organization for Standardization. Home page. <http://www.iso.org/iso/home.html>; 2013 [Retrieved May 26, 2013], from International Organization for Standardization.
- ISACA. COBIT 5: a business framework for the governance and management of enterprise IT. <http://www.isaca.org/cobit.htm>; 2013 [Retrieved May 26, 2013], from ISACA.
- ISACA. Home page. <http://www.isaca.org>; 2013 [Retrieved May 26, 2013], from ISACA.
- ISACA CRISC. Certified in Risk and Information Systems Control (CRISC). <http://www.isaca.org/Certification/CRISC-Certified-in-Risk-and-Information-Systems-Control/Pages/default.aspx>; 2013 [Retrieved May 26, 2013], from ISACA.
- Khan H. Cyber attack on U.S. electric grid ‘gravest short term threat’ to National Security, Lawmakers Say. <http://abcnews.go.com/blogs/politics/2011/05/cyber-attack-on-us-electric-grid-gravest-short-term-threat-to-national-security-lawmakers-say/>; May 31, 2011 [Retrieved May 26, 2013], from ABC News.
- National Drought Mitigation Center. Home page. <http://drought.unl.edu/>; 2013 [Retrieved May 26, 2013], from National Drought Mitigation Center.
- National Institutes of Standard and Technology. Computer security center resource publications. <http://csrc.nist.gov/publications/index.html>; 2013 [Retrieved May 26, 2013], from NIST Information Technology Library.
- National Institutes of Standards and Technology. Guide for conducting risk assessments. http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf; 2012 [Retrieved May 26, 2013], from National Institutes of Standards and Technology.
- Occupational Safety & Health Administration. <https://www.osha.gov/SLTC/workplaceviolence/>; 2013.
- SANS Institute. Home page. <http://www.sans.org/>; 2013 [Retrieved May 26, 2013], from SANS Institute.
- Securities and Exchange Commission. Home page. www.sec.gov; 2013.
- Stoneburner G, Goguen A, Feringa A. Risk management guide for information technology systems. <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>; 2002 [Retrieved May 26, 2013], from National Institute of Standards and Technology.
- The Business Continuity Institute. Home page. <http://www.thebci.org>; 2013 [Retrieved May 26, 2013], from The Business Continuity Institute.
- U.S. Centers for Disease Control and Prevention. www.cdc.gov/niosh/docs/video/violence.html; 2013.
- U.S. Centers for Disease Control and Prevention. Violence on the job. www.cdc.gov/niosh/docs/video/violence.html; 2013 [Retrieved May 26, 2013], from U.S. Centers for Disease Control and Prevention.
- U.S. Department of Homeland Security. Home page. www.dhs.gov/index.shtml; 2013 [Retrieved May 26, 2013], from U.S. Department of Homeland Security.
- U.S. Department of Justice. Computer crime & intellectual property section. <http://www.cybercrime.gov>; 2013 [Retrieved February 2013], from U.S. Department of Justice.
- U.S. Geological Survey. Putting down roots in earthquake country. <http://pubs.usgs.gov/gip/2005/15/>; 2005 [Retrieved May 26, 2013], from U.S. Geological Survey.
- U.S. Geological Survey. Seismicity of the United States. <http://earthquake.usgs.gov/earthquakes/states/seismicity/>; 2007 [Retrieved March 6, 2007], from U.S. Geological Survey Earthquake Hazards Program.
- U.S. Geological Survey. Home page. http://www.usgs.gov/natural_hazards/; 2013 [Retrieved May 26, 2013], from U.S. Geological Survey.
- U.S. Geological Survey. Natural hazards. http://www.usgs.gov/natural_hazards/; 2013 [Retrieved May 26, 2013], from U.S. Geological Survey.
- U.S. Secret Service Criminal Division. <http://www.secretservice.gov/criminal.shtml>; 2013.
- U.S. Secret Service Electronic Crimes. <http://www.secretservice.gov/ectf.shtml>; 2013.

Business Impact Analysis

5

IN THIS CHAPTER

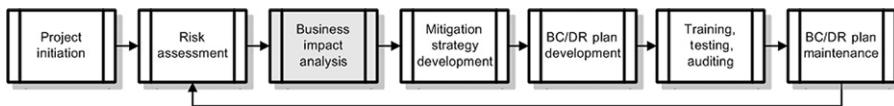
- Business impact analysis overview
- Understanding impact criticality
- Identifying business functions and processes
- Gathering data for the business impact analysis
- Determining the impact
- Business impact analysis data points
- Preparing the business impact analysis report
- Summary
- Key concepts

INTRODUCTION

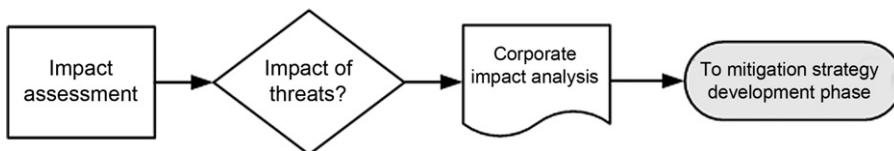
In [Chapter 4](#), you learned about risk management and the process for assessing risks. In this chapter, we turn our attention to the process of business impact analysis (BIA). Risk assessment looks at the various threats your company faces; BIA looks at the critical business functions and the impact of not having those functions available to the firm. The risk assessment starts from the threat side, and the BIA starts from the business process side. When you’re managing general business risk, you might actually start with the BIA. However, in planning for business continuity as related to disaster recovery, it makes more sense to understand the full picture regarding risks and threats and then look at business impact. That said, if you have a methodology you use that starts with BIA, that’s fine. Both outputs—from the risk assessment and the BIA phases—are used as input to the mitigation strategy development. As long as you have those ready before you start the mitigation phase, which we’ll discuss in [Chapter 6](#), you should be all set. [Figure 5.1](#) depicts where we are in the planning process thus far.

You can see, from [Figure 5.2](#), that we’ll be focusing on the third and final segment of the risk assessment phase introduced in [Chapter 4](#) (refer to [Figure 4.2 in Chapter 4](#) for the full diagram).

In this chapter, we’re going to concentrate on the impact of various business functions on your operations. We begin with discussing the general framework of

**FIGURE 5.1**

Business continuity and disaster recovery project progress.

**FIGURE 5.2**

Business impact analysis phase.

performing a BIA and conclude with the specifics of performing an impact analysis for your business continuity and disaster recovery (BC/DR) plan.

BUSINESS IMPACT ANALYSIS OVERVIEW

The fundamental task in the BIA is to understand which processes in your business are vital to your ongoing operations and to understand the impact the disruption of these processes would have on your business. From an IT perspective, as the National Institute of Standards and Technology views it: “The BIA purpose is to correlate specific system components with the critical services that they provide, and based on that information, to characterize the consequences of a disruption to the system components.” (Swanson et al., 2010, p. 15) So, there are two parts to the BIA: the first is to understand mission-critical business processes and the second is to correlate those to IT systems.

As an IT professional, you certainly understand the importance of various IT systems, but you may not be fully aware of the critical business functions performed in your company. Even if your role in this project is limited to managing the IT elements in this BC/DR plan, you should still pay close attention to the material in this chapter for two main reasons. First, understanding the critical business functions is important in terms of understanding how to recover IT systems in the event of a significant business disruption. You might think that System A is most critical, based on a number of assumptions you’re making. However, through this process, you might find that System B or C is really what keeps the company up and running on a day-to-day basis or that without System D, System A doesn’t really matter. Second, if you have any aspirations at all of moving up the corporate ladder toward that CIO job, your understanding of the overall business will certainly help you achieve those goals. Today’s CIO needs to have a solid background in technology *and* business,

so understanding the critical business functions in your company will pay off in many ways for you.

According to [Business Continuity Institute \(2013\)](#) (www.thebci.org), a recognized leader in BC management and certification, there are four primary purposes of the BIA ([The Business Continuity Institute, 2005](#), p. 21):

- Obtain an understanding of the organization's most critical objectives, the priority of each, and the time frame for resumption of these, following an unscheduled interruption.
- Inform a management decision on maximum tolerable outage (MTO) for each function.
- Provide the resource information from which an appropriate recovery strategy can be determined/recommended.
- Outline dependencies that exist both internally and externally to achieve critical objectives.

BIA is the process of figuring out which processes are critical to the company's ongoing success, and understanding the impact of a disruption to those processes. Various criteria are used, including customer service, internal operations, legal or regulatory, and financial. From an IT perspective, the goal is to understand the critical business functions and tie those to *specific* IT systems. As part of this assessment, the interdependencies need to be fully understood. Understanding these interdependencies is critical to both DR and BC, especially from an IT perspective. Would it make sense for your IT staff to spend 3 days trying to recover System D if System A is still out of commission? Until you perform the BIA, there may be no real way to know.

BIA includes the steps listed earlier, but we can break them up into a few more discrete activities or steps:

1. Identify key business processes and functions.
2. Establish requirements for business recovery.
3. Determine resource interdependencies.
4. Determine impact on operations.
5. Develop priorities and classification of business processes and functions.
6. Develop recovery time requirements.
7. Determine financial, operational, and legal impact of disruption.

The result of performing these seven steps is a formal BIA, which is used in conjunction with the risk assessment analysis to develop mitigation strategies (discussed in [Chapter 6](#)).

The two primary impact points of any business disruption are the operational impact and the financial impact. The operational impact addresses the nonmonetary effect including how people, processes, and technology are impacted by a business disruption and how best to address that impact. The financial effect addresses the monetary impacts and how a business disruption will impact the company's revenues, costs, and overall viability, both short- and long term.

CRITICAL CONCEPT**Impact Areas to Consider**

A disaster can have a widespread impact on an organization. Throughout this book, we reference areas of focus outside of IT in order to ensure your organization does not have gaps in its overall disaster and BC plan. In IT, it's easy to focus solely on your own internal people, processes, and technologies, but in the BIA portion of planning, you need to look beyond IT and into the business. Here are some areas of impact identified by DRI International (www.drii.org) as topics to consider (Disaster Recovery Institute, 2013):

1. Customer impact
 - a. How soon will customers become aware of your problem?
 - b. How quickly will they take their business to your competitor?
 - c. How quickly will contractual providers (anyone who provides service to your customers on your behalf) move to a competitor?
 - d. What is the impact on your contractual service level agreements?
 - e. What is the impact to the supply chain for your key customers?
 - f. What are the upstream and downstream implications for your key customers?
2. Financial impact
 - a. Loss of revenue and income
 - b. Cost to recover from a disaster
 - i. Overtime and temporary labor
 - ii. Travel and expense for consultants and vendors
 - iii. Insurance deductibles
 - iv. Out-of-pocket expenses not covered by insurance
 - v. Lost equipment, materials, and supplies
 - c. Clean up and restoration costs
 - d. Costs to improve during new construction (improving existing)
 - e. Impact on market share
 - f. Impact on short-term and long-term stock price or valuation
 - g. Contractual or regulatory fines and penalties
 - h. Potential lawsuits (all associated fees)
3. Reputational impact
 - a. Board of directors
 - b. Shareholders
 - c. Customers
 - d. Community
 - e. Media and social media attention
 - f. Competitors leveraging your disaster
4. Operational impact
 - a. Reduced service levels or output
 - b. Increased materials cost (emergency orders)
 - c. Increased overtime or labor costs with reduced output
 - d. Workflow disruptions (manual work-arounds, etc.) and reduced efficiencies
 - e. Loss of control (quality)
 - f. Inability to meet key deadlines and deliverables
 - g. Disruption to ongoing projects and/or processes
 - h. Supply chain disruption
5. Human impact
 - a. Loss of life and serious injury
 - b. Impact to community functions
 - c. Stress (impact on family, work, and community)

Continued

CRITICAL CONCEPT—cont'd

- d. Increased use of community or social services
- e. Long-term emotional impact on family, work, and community

As you can see, there are numerous potential areas of concern for your BIA. Are they IT related? Many are not. However, it is wise to consider these factors in your IT BIA process because these factors will impact your plan and process if you are ever called upon to implement them. You may not need to plan specifically for lost revenue, for example, but you need to be aware that this constraint on the organization will impact decisions being made about how to prioritize spending in the aftermath of a disaster. Make sure *your* plan accounts for this.

Upstream and downstream losses

In addition to the direct impact of a business disruption such as an earthquake or flood, there are indirect impacts you should consider. These can be viewed as upstream and downstream losses. *Upstream losses* are those you will suffer if one of your key suppliers is affected by a disaster. If your company relies on regular deliveries of products or services by another company, you could experience upstream losses if that company cannot deliver. If you run a manufacturing company that relies on raw materials arriving on a set or regular schedule, any disruption to that schedule will impact your company's ability to make and sell its products. This is how a disaster elsewhere can impact you, even if your company is unharmed. *Downstream losses* occur when key customers or the lives in your community are affected. If your business supplies parts to a major manufacturer that is shut down due to a hurricane or earthquake, your sales will certainly suffer. Similarly, if your company provides any type of noncritical service to your community and there is a flood or landslide, your sales could take a hit while residents of the community deal with the disaster. If you operate a chain of restaurants or movie theaters or golf courses, residents will be more focused on dealing with the disaster than on entertainment and leisure pursuits. These are considered downstream losses even if your business, itself, has not taken the direct impact of a disaster.

Keep in mind, too, that people, businesses, and communities are interrelated; very few (if any) companies exist in isolation. A natural disaster or serious disruption can create a chain reaction that ripples through the business community and impacts the local or regional economy.

REAL WORLD**Protecting Your Assets**

BC/DR planning can certainly help you mitigate some of your risks. In [Chapter 6](#), we'll develop specific strategies for doing so. However, keep in mind that various types of insurance can help as well. This is considered risk transference and is a well-accepted business practice. If you're a small company, have the owner or general manager consider looking into purchasing business income interruption and extra expense insurance. If a business disruption occurs, there could

Continued

REAL WORLD—cont'd

be both an immediate and long-term impact on your company's revenues. Not only will it not be business-as-usual, you'll have the added expenses of lost productivity, lost customers, and higher costs. Some of your out-of-pocket expenses might ultimately be covered by insurance, such as the loss of equipment from a storm or building collapse. Other expenses, however, won't be covered. When revenues decrease and expenses increase, it can create a devastating financial picture for your company. Some basic business insurance policies cover expenses and loss of net business income, but it may not cover business interruptions that occur away from your business, such as to your key supplier, vendor, customer, or even your utility company. This type of insurance can typically be purchased as additional coverage to an existing policy. We're not suggesting you purchase additional insurance (and we have no connections to the insurance industry), but we do suggest you, your financial folks or your general manager (CEO, founder, and owner) look at your financial exposure and your current insurance policy and decide if you're properly protected. Of course, insurance alone will not protect your business from failing in the face of a serious disruption or event—that's where a solid BC/DR plan comes in.

Understanding the human impact

Although this chapter is focused on recovering business systems, it's clear that people are a major factor in BC efforts—not only from a planning and implementation perspective but also from the impact perspective as well. If a natural disaster strikes, it's possible that some or all of your company's employees will be impacted. It's possible that some may die or be seriously injured. Although no one likes to think about these possibilities, they cannot be ignored in a BC/DR plan. As you assess business functions and business processes, you'll also need to identify key positions, key knowledge, and key skills needed for BC. In some sense, this begins to cross over into what is traditionally called *succession planning*. In publicly traded companies or high-profile start-ups, the company often purchases what's called *key man insurance*. This insurance covers the cost of losing a high-ranking executive in the company, the assumption being that if someone at that level were suddenly unavailable to carry out that function, the business would suffer financial losses.

Key positions

Succession planning in companies covers many areas, but typically it's discussed in terms of replacing key employees as well as how to transfer the reins of the company from one leader to the next. Succession planning can include training employees to move up the corporate ladder and assume leadership positions. From a risk management perspective, it can also address who will replace key employees in the event of a planned or unplanned departure. For example, if a company was started by a couple of business partners, at some point before their retirement, they should spend time identifying their successors—whether family members or trusted employees—and identifying the path to hand over the leadership of the company. When done in a thoughtful and predetermined manner, this can help smooth the transition. In terms of BC/DR, this plan can help identify who should step up, should something happen to the company's founders or executives.

Beyond key man succession and planning, the BC/DR plan needs to look at key positions within the IT department and understand the role of each in the BC realm. For example, if you have complex database applications, you may identify a database administrator (DBA) as a key role in the business recovery process. Ideally, your existing DBA would take care of this, but what if she was unable to respond to the business disruption because she was injured or unable to get to the site (or worse)? Rather than identifying specific people, you should identify roles, responsibilities, skills, and knowledge needed. Even though you'd prefer your own DBA to recover the system, if she was unavailable for any reason, you would know that you need a DBA to recover your systems and you could go to external sources to locate a temporary or permanent DBA replacement.

Similarly, IT management skills need to be identified to ensure that roles and responsibilities for BC/DR are both identified and assigned. If you have key leadership in your IT department, these should also be noted during your BIA.

Human needs

Beyond replacing needed skills and positions, it's important to keep the human impact in mind throughout your planning. As mentioned earlier in the book, everyone responds to disasters differently. If a portion of the building catches fire and burns, it's likely that those employees in the area at the time the fire breaks out will experience the event in a variety of ways. Some people will evacuate and stand in the parking lot laughing about the close call, even as the fire engines pull in. Others probably will be frightened by the experience and may become shaky, disoriented, or panicky. Still others might seem fine immediately afterward but days or weeks later, they begin to display odd behavior that might be the result of a delayed onset of stress from the event. Clearly, the bigger the event (earthquake, tornado, or hurricane), the bigger the human toll in terms of death, injury, and emotional distress.

A good BC plan will address the human factors for two reasons. First, addressing employee needs is simply the right thing to do. Although there are companies that may demand that employees report to work following a serious business disruption or face termination, most companies understand that everyone will have different needs. Some may report back to work, some may need to deal with family problems, and some may be physically or emotionally unable to return to work immediately. The company's policies with regard to employee needs and requirements in the aftermath of a business disruption or natural disaster should be developed by your Human Resources (HR) department; however, your BC/DR plan must take these varied responses into consideration. If your IT systems recovery effort hinges on two experienced network administrators, you need to address these as risks in your plan and develop mitigation strategies along with them.

The second reason for addressing employee needs in your BC/DR plan is because it makes good business sense. The ideal scenario might be that everyone is fine and shows up for work, but reality is often far different from that. You can demand all you want that people show up, but if faced with a choice between work and family, between work and health, people will usually choose family and health first. In some

cases, insisting people return to work before they are ready can make things worse—they may not be able to concentrate and therefore may make recovery efforts worse instead of better. Incorporating this reality into your plan will mean that you and your team come up with appropriate alternatives that can address the lack of key staff in the aftermath of a business disruption. This helps the employees who may be unable to come back immediately and also helps the company recover in the fastest, most efficient manner possible. Creating plans for backup personnel, both from internal sources and potential external sources, should be incorporated into your plans.

We won't dwell on the human element in this chapter, but we mention it again in key places to keep it foremost in your mind so that as you determine the impact of various risks, you can also keep the human factor in mind.

UNDERSTANDING IMPACT CRITICALITY

As you're thinking about your company and its critical functions, which we review following this section, you should keep a rating scale in mind. Later, after you've compiled your list, you can assign a "criticality rating" to each business function. It's important to have an idea of your rating system in mind before you review your business functions so you can spend the appropriate amount of time and energy on mission-critical functions and less time on minor functions. For example, when you sit down with the finance group, you want to keep them focused on defining the mission-critical business functions while listing all business functions that would be needed for business continuation.

Criticality categories

You can develop any category system that works for you but as with all rating systems, be sure the categories are clearly defined and that there is a shared understanding of the proper use and scope of each. Here is one commonly used rating system for assessing criticality:

- Category 1: Critical functions—Mission-critical
- Category 2: Essential functions—Vital
- Category 3: Necessary functions—Important
- Category 4: Desirable functions—Minor

Obviously, your BC plan will focus the most time and resources on analyzing the critical functions first, essential functions second and so on. It's possible you will delay dealing with necessary and desirable functions until later stages of your business recovery. You should identify these categories of criticality for all systems your IT department is responsible for, then set timelines for each of these categories to indicate when a system in that category will be functional following a business disruption. Let's look at each category in more detail. You can use these category descriptions as is or you can tweak them to meet your company's unique needs. Feel

free to expand the list to include more categories, but beware of making it too complex at the start. After you've read through this chapter, you may choose to expand or contract the category list prior to embarking on your BIA.

Critical functions—Mission-critical

Mission-critical business processes and functions are those that have the greatest impact on your company's operations and need for recovery. Almost everyone working in a company has an innate understanding of the mission-critical operations within their department. The key is to gather all that data and develop a comprehensive look at your mission-critical processes and functions from an organizational perspective. What are the processes that must be present for your company to do business? These are the mission-critical functions. One way to get people to focus on the mission-critical functions is to ask (whether through questionnaire, interview, or workshops) what the first three to five things people would do in their department following a business disruption once the emergency or imminent threat of a business disruption subsides. This often gives you the clearest view of the mission-critical business functions in each department.

From an IT perspective, the network, system, or application outage that is mission-critical would cause extreme disruption to the business. Such an outage often has serious safety, legal, operational, and financial ramifications. This type of outage may threaten the health, well-being, and safety of individuals (hospital systems come to mind). This type of outage may threaten the very existence of the company. These systems may require significant efforts to restore and these efforts are almost always disruptive to the rest of the business (in the case that any other parts of the business are actually able to function during such an outage). The tolerance for such an outage, whether from the IT system or the function/process it provides, is very low and the recovery time requirement is often described in terms of hours, not days.

Essential functions—Vital

Some business functions may fall somewhere between mission-critical and important, so you may choose to use a middle category that we've labeled "essential" or "vital." How can you distinguish between mission-critical and vital? If you can't, you may not need to use this category. However, you might decide that certain functions are absolutely mission-critical and others are extremely important, but should be addressed immediately after the mission-critical functions. Vital functions might include things like payroll, which on the face of it might not be mission-critical in terms of being able to get the business back up and running immediately but which can be vital to the company's ability to function beyond the DR stage. A vital function could be supply chain systems or other systems directly related to producing goods and services.

From an IT perspective, vital systems might include those that interface with mission-critical systems. Again, this distinction may not be helpful for you.

If not, don't try to force your systems into this framework; simply don't use this category. You'll end up with just three categories—mission-critical, important, and minor. If that works for you, that's fine. If you use this categorization, your recovery time requirement might be measured in terms of hours or a day or two.

Necessary functions—Important

Important business functions and processes won't stop the business from operating in the near-term, but they usually have a longer-term impact if they're missing or disabled. When missing, these kinds of functions and processes cause some disruption to the business. They may have some legal or financial ramifications and they may also be related to access across functional units and across business systems.

From an IT perspective, these systems may include e-mail, Internet access, databases, and other business tools that are used in a support or reporting function, whether to support business functions or IT functions. If disabled, these systems have to wait in line and may wait a moderate amount of time (as compared to mission-critical) to restore to a fully functioning state. The recovery time requirement for important business processes often is measured in days or weeks.

Desirable functions—Minor

Minor business processes are often those that have been developed over time to deal with small, recurring issues, or functions. They will not be missed in the near-term and certainly not while business operations are being recovered. They will need to be recovered over the longer term. Some minor business processes may be lost after a significant disruption and in some cases, that's just fine. Many companies develop numerous processes that should at some point be reviewed, revised, and often discarded, but that rarely occurs during normal business operations due to more demanding work. In some sense, a business disruption can be good for those small business functions and processes as they may be reworked or revised or simply pared down after a disruption. You may use the process of performing your BIA to recommend paring down these minor business functions as well, though your time is better spent focusing on the mission-critical and vital elements. You may make notes about which functions and processes could be pared down outside of the BC/DR planning process and hand this off to the appropriate subject matter experts (SMEs) for later action. Many companies lack a practice of clearing out old data and outdated processes. They become data hoarders, which creates an electronic mess. Don't drag that forward with you. Seriously consider not having a recovery option for this category. If it's really that unimportant, it won't be missed if it's lost in a disaster event.

From an IT perspective, these types of system outages cause minor disruptions to the business and they can be easily restored. The recovery time requirement for these types of processes often is measured in weeks or perhaps even months.

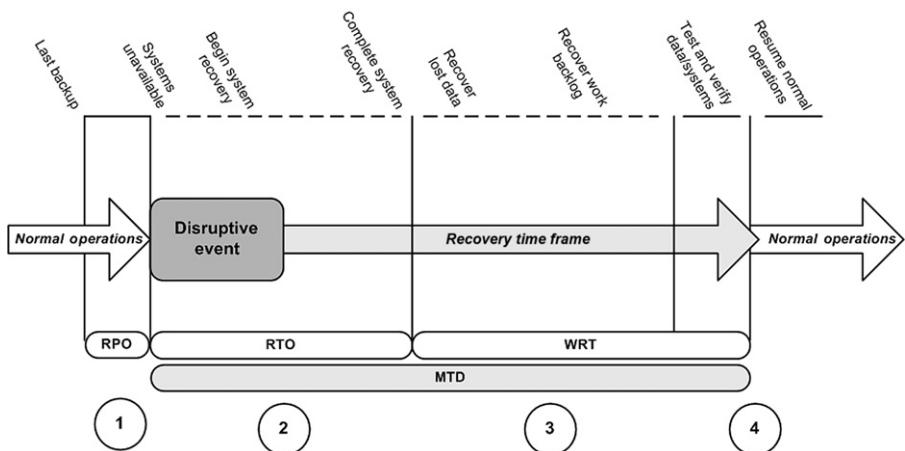
TIP**Seasonal and Occasional Business Functions**

When you embark upon your BIA interviews, be sure to prompt participants to think about all business processes throughout the year. Some functions and processes occur only during certain times of the year, such as tax season, year end, and holidays, and these might be missed during the process. If they're important enough processes, there's a good chance they'll be included, but project management best practices don't rely on luck—they rely on process. Be sure to ask about any special processes that occur throughout the calendar year that might not immediately come to mind for participants.

Recovery time requirements

Related to impact criticality are recovery time requirements. Let's define a few terms here that will make it easier throughout the rest of the analysis to talk in terms of recovery times. As you read through these definitions, you can refer to [Figure 5.3](#) for a representation of the relationship of these elements.

Maximum tolerable downtime (MTD). This is just as it sounds—the *maximum* time a business can tolerate the absence or unavailability of a particular business function. (*Note:* The BCI in the United Kingdom uses the phrase MTO instead.) Different business functions will have different MTDs. If a business function is categorized as mission-critical, or Category 1, it will have the shortest MTD. *There is a correlation between the criticality of a business function and its maximum downtime.* The higher the criticality, the shorter the MTD is likely to be. Downtime consists of two elements, the *systems recovery time* and the *work recovery time*. Therefore, $\text{MTD} = \text{RTO} + \text{WRT}$.

**FIGURE 5.3**

Business recovery timeline.

Recovery time objective (RTO). The time available to recover disrupted systems and resources (systems recovery time). It is typically one segment of the MTD. For example, if a critical business process has a 3-day MTD, the RTO might be 1 day (Day 1). This is the time you will have to get systems up and running. The remaining 2 days will be used for work recovery (see “work recovery time”). The RTO is a measure of when the system will be available to begin processing recovery work before being put back into a normalized production mode.

Work recovery time (WRT). The second segment that comprises the MTD. If your MTD is 3 days, Day 1 might be your RTO and Days 2-3 might be your WRT. It takes time to get critical business functions back up and running once the systems (hardware, software, and configuration) are restored. Upstream and downstream systems or interfaces need to be synchronized, data need to be tested to ensure backups are correct and in sequence, data captured manually during a downtime needs to be input, validated, and integrated into existing data. This is an area that some planners overlook, especially from IT. If the systems are back up and running, they’re all set from an IT perspective. From a business function perspective, there are additional steps that must be undertaken before it’s back to business. These are critical steps and that time must be built into the MTD. Otherwise, you’ll miss your MTD requirements and potentially put your entire business at risk.

Recovery point objective (RPO). The amount or extent of data loss that can be tolerated by your critical business systems. For example, some companies perform real-time data backup, some perform hourly or daily backups, some perform weekly backups. They may be full backups, incremental, differential, mirrored, local, remote, or cloud-based. If you perform weekly backups, someone made a decision that your company could tolerate the loss of a week’s worth of data (which should be validated during the BIA process). If backups are performed on Saturday evenings and a system fails on Saturday afternoon, you’ve lost the entire week’s worth of data. This is the RPO. In this case, the RPO is 1 week. If this is not acceptable, your current backup processes must be reviewed and revised. The RPO is based both on current operating procedures and your estimates of what might happen in the event of a business disruption. For example, if a tornado touches down in your town and your data center is without power, you may implement your BC/DR plan. If you have an alternate computing location, you may transfer operations to that location.

Your next step would be to determine the status of the data. Are you attempting to update systems using backups or were these alternate locations kept up to date? When was the last data backup performed relative to business operations? What do you need to bring systems up to date? These are the questions you’d need to answer after a business disruption. Therefore, it’s important to define your RPO beforehand and ensure your recovery processes address these timelines.

Let’s look at how these elements interact. [Figure 5.3](#) graphically depicts the interplay between MTD, RTO, WRT, and RPO. If your company has mission-critical and vital business processes that do not interact with computer systems of any kind, you still need to perform a BIA in order to understand how these manual systems may be impacted by a business disruption, especially natural disasters. At the end of this

chapter, we walk through an example to help illustrate these concepts. Most companies use technology and computer systems to some extent and the graphic in [Figure 5.3](#) shows how the recovery time is impacted by a business disruption.

- *Point 1:* RPO—The maximum sustainable data loss based on backup schedules and data needs.
- *Point 2:* RTO—The duration of time required to bring critical systems back online.
- *Point 3:* WRT—The duration of time needed to recover lost data (based on RPO) and to enter data resulting from work backlogs (manual data generated during system outage that must be entered).
- *Points 2 and 3:* MTD—The duration of the RTO plus the WRT.
- *Point 4:* Test, verify, and resume normal operations.

During normal operations, there is usually some gap between the last backup performed and the current state of the data. In some operations, this may be minutes or hours; in most organizations it is hours or days. This time frame is the RPO. In most organizations, this is the same as the period of time between backups. We see at circle 1 that there is a gap showing the point of the last backup and the state of current data, just before the disruption occurs. That's the point at which one or more critical systems becomes unavailable and BC/DR planning activities are initiated. The first phase of the MTD is the RTO. This is the time frame during which systems are assessed, repaired, replaced, and reconfigured. The RTO ends when systems are back online and data are recovered to the last good backup. The second phase, WRT of the MTD then begins.

This is the phase when data are recovered through automated and manual data collection processes. There are two elements of WRT. The first is the manual collection and entry of data lost, typically because systems went down between backups. The second phase addresses the backlog of work that may have built up while systems were down. Most companies try to recover the data up to the disruptive event to bring the systems current and then address the backlog, but your business processes may dictate a different recovery order. The key is to understand that there is a delay between the time the systems are back online and the time when normal operations can resume. During the periods indicated by circles 2 and 3, emergency work-arounds and manual processes are being used. These are processes that will be developed later in your BC/DR planning process. For example, if a CRM system is down, what processes will your sales, marketing, and customer service teams use to interface with and manage customer service delivery? You'll define that in the planning process. Circle 4 indicates the transition from DR and BC back to normal operations. There may be some overlap as manual processes are turned back over to automated processes and you may choose to do it in a rolling fashion—perhaps by department or geographic region.

As you collect your impact data, you'll also need to begin determining the RTOs. You may choose to create a rating system, so you can quickly determine RTOs.

For example, you might determine that mission-critical business systems or functions should have recovery windows as follows:

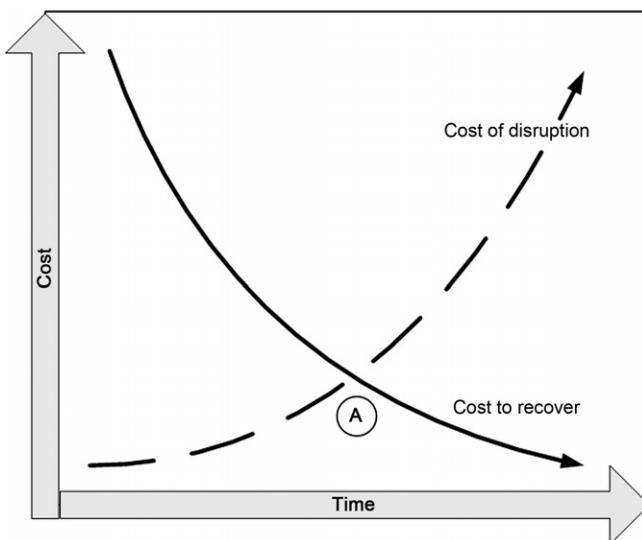
- *Category 1: Mission-critical—0-12 hours*
- *Category 2: Vital—13-24 hours*
- *Category 3: Important—1-3 days*
- *Category 4: Minor—more than 3 days*

You and your team, with input from the SMEs, can determine the appropriate MTD requirements. For some companies, a mission-critical business function could have an MTD of a week. For others, it might be 0-2 hours. *There is an inverse correlation between the amount of time you can tolerate an outage and the cost of setting up systems that allow you to recover in that time frame.* If you can't afford much downtime, you'll clearly have to invest more in preventing downtime and in having systems in place that allow fast recovery times. If you're a small company and can afford a longer MTD, you can spend less on preventing or recovering from outages.

Let's look at an example. In a small company, you may very well be able to do without even mission-critical systems for a couple of days or a week if you really had to. It's possible that you contract with an outside IT service provider to maintain, troubleshoot, and repair your computer systems. If you want a guaranteed 2-hour response time, your monthly maintenance costs will be significantly higher than if you sign up for a guaranteed next business day response. So, if you really can't afford to be without that mission-critical business function for more than about 8 hours (2-hour response time and 6-hour repair time), you'll have to pay more to your service company and you'll probably also have to purchase additional computer equipment to provide some redundancy to prevent extended downtime. These costs add up and the less disruption your business can afford, the more it will cost you to prevent or mitigate those risks. We'll discuss this in more detail in [Chapter 6](#), but it's within the BIA segment where you have to begin making these kinds of assessments.

Let's look at another example on the other end of the spectrum. Suppose you manage the centralized IT department for a multihospital, multistate healthcare system, and a serious power surge in the data center causes the hardware cluster running your electronic medical record system to fail. The potential cost to patients, providers, and the hospital system for that system to be down is enormous, so the investment the organization should be willing to make to ensure that data are always available (highly available, highly redundant, and no single point of failure) should also be large. In general, there should be a direct correlation between the criticality of the data and the investment the organization is willing to make to protect it.

It's important to note during your impact analysis and subsequent mitigation planning phases that there is an optimal recovery point. [Figure 5.4](#) shows the inverse relationship between the cost of disruption and the cost of recovery. Earlier in this book, we discussed the fact that any BC/DR plan had to be tailored to the unique needs and constraints of the organization. This is particularly true when it comes to the financial costs involved with disruption and recovery.

**FIGURE 5.4**

Relationship between cost of disruption and cost of recovery.

You can see that the longer you allow a disruption to go on, the more expensive it becomes to the business. Conversely, the longer you have to recover, the less expensive recovery itself becomes. This makes sense when you understand that the longer a business disruption goes on, the more lost revenues, lost sales, and lost customers you accumulate. At the same time, if you need to recover your systems immediately, it's going to cost more to implement things such as zero downtime solutions and hot sites. If you can afford to take a bit more time to recover you have more options, and these options are typically less expensive. If you start plotting these points, you will find an optimal point between these two costs, shown in [Figure 5.4](#) by point A. Each company's intersecting points (point A) will be different based on your company's financial constraints and operating requirements.

LOOKING AHEAD . . .

Making the Business Case Makes Your Life Easier

During the assessment and implementation of IT systems over the course of the past few years, you may already have addressed (and invested in) some of the elements needed to reduce the time to recover or to reduce the cost of a disruption. If so, be sure to make note of these systems or investments and be sure to include them in your planning. One way to help make the business case for continued investment is to show how the systems already implemented have made an impact or have contributed to your BC/DR plan. For example, suppose you implemented a mirrored site to allow users to gain access to key data more quickly. That mirrored site also serves as a backup and reduces the cost of disruption to a single site. It also reduces the amount

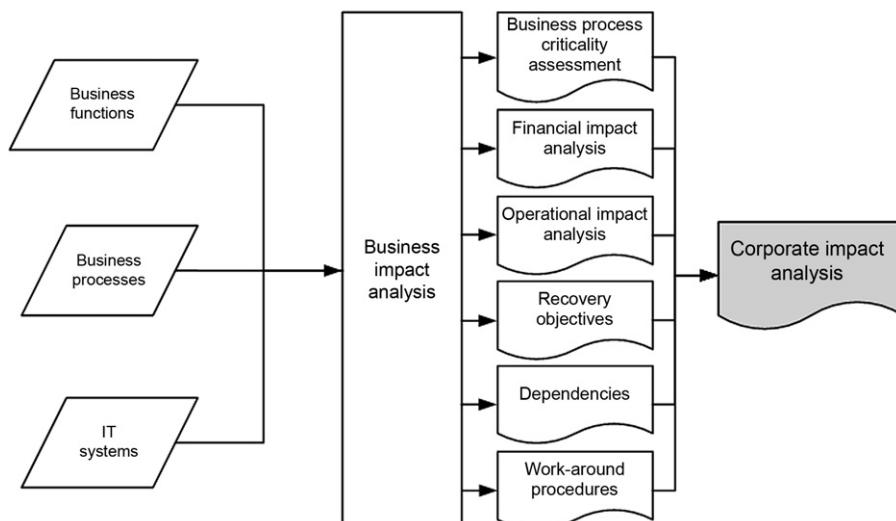
Continued

LOOKING AHEAD...—cont'd

of time it takes to recover, thereby pulling point A ([Figure 5.4](#)) down and to the left (toward lower cost and less time). This investment, then, has contributed to optimizing your balance between cost of disruption and cost to recover while also improving user productivity. Being able to establish and articulate these kinds of IT benefits within your organization will help you win support for your BC/DR plan and create a solid foundation for future investment decisions.

Next, let's look at what the entire analysis process looks like, as shown in [Figure 5.5](#). After we explore this, we take a look at the specific data required for inputs and outputs to this process.

In this segment of BC/DR planning, we're looking at business functions, processes, and IT systems to determine criticality. Business functions can be defined as activities such as sales, marketing, or manufacturing. Business processes can be defined as *how* those activities occur. How are sales or revenues generated? How are orders processed? How are services delivered? How are employees hired? How is payroll paid? These are business processes; they describe how the functions get done. By first identifying business functions, you then can focus on the key processes in each function to develop a comprehensive view of your company. The third input area, shown in [Figure 5.5](#), is IT systems. In most companies, the business processes are carried out in part through computer systems, applications, and other automated systems. Identifying mission-critical business functions and processes and how they intersect with IT systems will help you map out your BC/DR strategies.

**FIGURE 5.5**

End-to-end business impact analysis.

Once you have compiled that data, you'll perform the analysis to generate the needed outputs, including the criticality assessment, the impact assessments (financial and operational), required recovery objectives, dependencies, and work-around procedures. The work-around procedures will enable you to get critical business functions back up and running as quickly as possible. These work-around procedures may be used during the RTO and WRT periods discussed earlier and shown in [Figure 5.3](#). As you can see, the output is a comprehensive corporate impact analysis. This is the same output shown in [Figure 5.2](#) and is the end of the larger risk assessment phase in our overall BC/DR planning process. The impact analysis will be used as input to the risk mitigation planning segment of the BC/DR project and we'll discuss that in [Chapter 6](#).

IDENTIFYING BUSINESS FUNCTIONS

In this section, we're going to walk through some of the more common functions found in business today. It's not a comprehensive list but it's intended to do two things. First, you can include these in your BIA and you'll know you've got the major items covered. Second, you can use this to spur your thinking to include other areas that might be related to the items listed. You should begin by listing all the business functions that come to mind unless it's clear they should *not* be included. As with your risk assessment, it's best to begin by scanning the wide horizon and narrowing your focus later on. It's always easier to cut than to try to fill gaps later.

When possible, it's advisable to create a list of all the functional areas of the business and gather SMEs from each area to discuss the critical business functions. Although it's more time consuming to get everyone in a room together, you will more quickly discover interdependencies in this manner. If SMEs sit quietly by themselves and come up with the critical business functions alone, they might miss the elements that are vital to other areas. An alternate method of gathering these data is to have the SMEs generate a list of questions to ask others in their area and compile the results. When the compiled results are ready, the SMEs from all areas of the company can meet to go over the results with the specific mission of finding interdependencies. How you manage this aspect of the project will have everything to do with how your company runs on a day-to-day basis.

The common business functions include those shown here. They're listed in alphabetical order, not necessarily in the order in which you would review these areas. The order in which these are reviewed will be dictated by the project management processes you've defined, the data gathering methods you choose, and the structure of your company. Following this section, we discuss the specific data points you need to gather from each of these areas.

1. Facilities and security
2. Finance
3. Human Resources

4. Information technology
5. Legal/compliance
6. Manufacturing (assembly)
7. Marketing and sales
8. Operations
9. Research and development
10. Warehouse (inventory, order fulfillment, shipping, and receiving)

As we look at these business functions, keep your business in mind and think about the key processes that occur in each functional area. After you've documented your key business processes, you will assign a criticality rating to them, similar to the ones discussed earlier. As a reminder, you may also want to document key positions, skills, and knowledge in these functional areas. For example, what would the impact be if your head of facilities was injured in a building collapse and your company needed to operate from an alternate location? Who would head that up? What skills or knowledge would be needed in order to temporarily (or permanently) replace your facilities manager in the aftermath of a business disruption? These human factors should be assessed in conjunction with the major business functions.

TIP**Visually Mapping Your Business**

One activity you can use with your team is both engaging and enlightening. Gather your team in a room with a large white board. Give each functional area their own color paper (small pads the size of sticky notes). Have each one write down functions in their area. On the white board, create several columns by drawing vertical lines and at the top of each column put a functional header. Next, have the teams put their functions under each of those headers. The result will be a visual map of how the business operates. You could turn this into a swim lane map or a process map to represent the output from the sticky note session. If you have the luxury of leaving that up for a while in place, you may wish to review it periodically over the course of a couple of weeks to ensure it accurately reflects how business is conducted. Then, translate it to an electronic format that works for you. There are numerous tools available, including Microsoft Excel or Visio, which will capture the structure. It may take a few iterations to get it right, but it could be a powerful tool to help you ensure you're looking at the entire scope of work. If this concept doesn't work for you, it may spark ideas on other creative and visual ways to engage your team of experts in mapping out core business functions. Once done, you can map those to enterprise applications, databases, and servers to identify core infrastructure for Tiers 1, 2, and 3 recovery objectives.

Remember, though you're looking at the broad business environment, you want to continually pull your findings back into an IT-centric view to understand what steps you'll need to include in your BIA for IT.

Facilities and security

Your company may be located in a single office in a small office building or it may span several continents. Regardless of how many physical locations your company operates, you need to understand the critical processes performed by facilities and

security management with regard to your business operations. If a business disruption were to occur, what processes and procedures would be needed in order to get your business up and running? For example, if the building is damaged or destroyed, physical security of the building will be disrupted. Employees won't be able to just swipe their badge at the front door. Is this a critical business function or not? It depends. If the building is destroyed, it doesn't matter that they can't get into the building. You don't just need an alternate process, you need an alternate location. Once an alternate location is established, you need facilities support. So, the critical business function, in this example, is having a place of business (facilities). Security and access are secondary. Notice how it helped to think of a specific scenario—it focused our thinking so we could see the key areas. Is having a place of business a critical business function? Not in the formal definition of a business *process*, but it's certainly important. Security usually involves a process—adding employees to access lists, providing employees with badges, IDs, or other identification, and granting them appropriate access to company resources. This might be highly important during normal business functioning, but does it impact the company's mission-critical operations? It depends on your business. If you work in a secure research environment, facilities and security may be mission-critical. If you work in a software development firm where employees could check code out of an online library and work from home, facilities and security may not be mission-critical at all. Facilities and security, though, may have some critical business functions beyond these macrolevel functions just mentioned. For example, is your facilities team involved with the receiving or shipping of products, inventory, or other tangible goods? If so, these may be critical business functions to be included.

Finance

By definition, the financial workings of the company are critical business functions, but not all financial functions are mission-critical functions. For example, tracking receivables and payables are critical business functions because without the ability to keep track of what others owe you and what you owe others, you have no idea about the financial status of the company. Employee payroll is another critical business function (which is a financial transaction that might fall under the purview of the HR department). If employees are not paid, if appropriate withholding and other taxes and deductions are not taken, your company faces serious problems, with employees and with state and federal authorities.

TIP

Check Your Assumptions at the Door

Don't allow assumptions by end-users to go completely unchallenged. One large employer was able to determine that if the payroll system was down due to a disaster or major outage (hardware, software, etc.), they could simply contact the bank and have them resend the same paychecks the following pay period. This could be done for up to 2 months without any really

Continued

TIP—cont'd

serious problems for staff or the company. Therefore, though payroll should be considered a mission-critical *function*, it is not a Tier 1 *application* from an IT perspective. This is a key distinction and one that you can help your users understand as you move through this process. Part of the goal throughout this process is to really understand what is vital to the organization and part of it is to legitimately limit the number of Tier 1 applications that are defined. Reducing the Tier 1 footprint will make your BC/DR activities more focused, allowing you to bring up just the truly critical applications first. End-users typically see their function as vital, so your job will be to help balance this equation.

If your company has legal obligations to pay back a loan from a bank or make payments or reports to investors, these also might be critical business functions to be included in your analysis. In some cases, you may have some leeway with regard to repayment if you experience a natural disaster, but don't count on it. Your financiers don't care, they just want payments on time and in full. Therefore, keeping track of these kinds of financial and legal obligations may be considered critical business functions, depending on the nature of your company and its financing structure. With electronic banking services, companies can largely look at external systems to determine certain payments made and can (in some cases) make payments based on those payment histories. While not ideal, these kinds of work-arounds can keep the business running in an interim state.

Accounting, finance, and reporting functions within finance should be reviewed and analyzed. There are many interdependencies in financial functions that cross over into HR, marketing, sales, IT, and operations. If key IT systems were to go down, which business processes would be impacted? Which processes and functions would have to get back up and running first in order to keep the business going?

Human Resources

If your firm experiences some sort of natural disaster, your HR staff will be busy trying to fulfill a number of roles. Employees will usually contact HR for information on the status of the building, the status of the company, whether they should report to work, where they should report to work, and so on. Employees may also use HR as a clearing house for information about the well-being of other employees or information on the broader community. Finally, employees will be looking to HR for information on how, when, and where they'll get paid. In fact, this will likely be the first question many employees ask, especially if the business disruption happens just prior to or on payday. The staff in HR will be in the best position to provide guidance on the kinds of issues for which employees come to them. From there, you can compile a list of critical business functions. Remember, create a list of all business functions and prioritize them later. If IT systems were to go down, which HR functions and processes are mission-critical? How would they be accomplished in the absence

of IT systems? How would this impact other areas of the company? Are the functions or the applications critical? Are there viable work-arounds that no one has yet defined?

Information technology

Critical business functions for IT? It seems like almost all of them are critical most of the time, especially if you judge by the phone calls, hallways pleas, and e-mails begging for assistance when one of the applications, servers, or hardware goes down. However, ultimately, the hardware and software should support the critical business functions, so the IT functions, in large part, will be driven by all the other departments. HR might say, “We have to have our payroll application”; marketing might say, “Without our CRM system, we can’t sell any products”; manufacturing might say, “Without our automated inventory management system, we can’t even begin to make anything.” All those statements may be true and many of these systems are interdependent. Going back to a concept mentioned earlier in this chapter, upstream and downstream systems need to connect in a logical and distinct manner, so there must be an order to which critical systems are addressed. Therefore, the IT department’s critical business functions are driven externally, to a large degree.

There are also business functions that occur *within* the IT department critical to the company’s ability to recover and continue doing business after a disaster. For example, the IT department needs to create, manage, and store backups of all data that changes after a disaster. If a disaster happens on a Tuesday and you’re able to get some systems up and running by the following Monday, backups need to start on Monday, as soon as data begins being generated, saved, or changed. Therefore, backup processes can be viewed as critical business functions from the IT perspective. However, you may have a hybrid environment where some systems are still being restored while other systems are in production, generating current data. Managing this environment is extremely critical, which is why we discuss how to restore systems later in this book.

Managing security is another critical aspect. In the aftermath of a major event or disaster, there’s a tendency to “just get it done.” However, ensuring the confidentiality, integrity, and availability of critical business data must still be a top priority. As with all information security functions, you’ll need to balance security with operational needs. Still, these are areas to consider as you develop your BC/DR plan and topics to discuss during the BIA process.

Legal/compliance

There are numerous mission-critical business functions related to legal and compliance areas of your company. If your firm is subject to legal or regulatory statutes and requirements, you’re already well aware of these constraints. You need to view these constraints and requirements in light of a potential business outage to determine which of these are mission-critical, which are vital or important, and which are minor

in nature. For example, if your firm deals with private or confidential personal data, it must be protected at all times, even if you move to a manual system for the duration of a system outage. Which systems, then, should be recovered first? Which business processes are mission-critical? Those related to remaining in compliance, both in terms of business process and business data, should be ranked very high on your list. The legal and financial consequences, as discussed earlier in this book, can be enormous. There may be reporting requirements with set timelines that cannot be reasonably moved or renegotiated and those constraints must be noted in the BIA and addressed accordingly.

Manufacturing (assembly)

If your company is involved with the manufacturing, assembly, or production of tangible products, you obviously need to scour this area for mission-critical functions since your ability to produce your products is the engine that drives your company. There may be some systems that can come online later, but there are likely to be certain systems that must be up and running in order for any manufacturing, assembly, or production to occur. Identify these business processes and systems by understanding what would happen if the production equipment were to be damaged or destroyed. Next, understand what would happen if the production equipment was left intact but upstream or downstream events impacted your customers or vendors. The impact analysis needs to include both internal and external elements. What business processes should you put in place to deal with the potential loss of a key supplier? We look at risk mitigation strategies in detail in the next chapter. For now, you should be identifying the potential impact of various business disruptions to your manufacturing operations, keeping both internal and external (upstream/downstream) disruptions in mind.

It's also important to understand the interaction between any manufacturing/assembly automation equipment and IT systems. If IT systems go down, how are automation systems impacted? If automation systems go down, how are IT systems impacted? What manual processes can be implemented in the absence of either automation systems or associated IT systems?

Marketing and sales

Marketing activities help create demand for the company's products and services by establishing or expanding knowledge of the company and its products/services. Sales activities are those actions that actually create a sales transaction and bring revenue to the company. Some companies may determine that marketing activities in the aftermath of a business disruption can be put on hold while sales activities should be a top priority. Other companies may see marketing activities as mission-critical in the aftermath of a business disruption because they are businesses that need to stay in touch with customers, keep their products/services in front of customers, and cannot afford to let rumors and erroneous information about the company's status float

around, especially in today's world of instant, on-demand news. How you approach marketing and sales functions in your firm from a BC/DR standpoint will depend largely on the size of your company, its market visibility, and other internal factors. Clearly, activities that support the company's ability to perform sales transactions will most often be considered either *vital* or *mission-critical* activities/systems.

Operations

If your company doesn't manufacture, assemble, or produce tangible products, it probably develops and sells intangible products such as service, software development, research, analysis, and others. Whatever it is your company does, it sells something in order to generate revenue. Therefore, your operations are what end up generating those goods and services that are sold to customers. As with manufacturing and assembly, operations are what generate sales and therefore are almost always part of the most urgent mission-critical business functions. Some companies have a Chief Operating Officer, under whom responsibility for all operations fall; other companies have a General Manager or Operations Director; still others have operations distributed across other business functions. Although "operations" is a rather broad and vague term, each company knows exactly what its operations are and how these operations contribute to revenue generation. It is within that scope of knowledge that these activities should be assessed for criticality.

Research and development

Some companies or organizations are funded through investors, through grants, or operate as nonprofits. They may be dedicated solely to research and development and may not generate revenue in the traditional sense of the word. However, every organization needs funding and that funding almost always comes with some sort of expectations and requirements about what is to be achieved with that funding. Therefore, you can view activities that bring in funding as your sales activities and can assess their criticality in that light. For example, if your organization does biochemical research and you're funded by federal or state programs, you still have business functions related to deliverables to consider. Is the next round of funding predicated upon the successful delivery of the results of current development or testing? If so, you have several mission-critical systems to consider along with assessing the impact of a business disruption to your research. Do you have live cultures growing in a lab that need to be tested and assessed? If so, what would happen if the research building was destroyed by fire or by an earthquake or tornado? How would your research be impacted and how would you recover? Though these are a bit different from traditional business functions and are not related directly to IT systems, these are questions that should be asked and answered if you're in this type of business. From an IT perspective, these are questions operational and process owners should be asking and answering, but where they intersect with IT systems, they become part of the IT BIA domain.

Warehouse (inventory, fulfillment, shipping, and receiving)

If your company deals in tangible goods of any kind, you have processes for handling inventory, order fulfillment, returns, shipping, and receiving. In some companies, these functions are handled by outside firms. For example, you may manufacture or assemble a product that is sent out daily on trucks or trains to some other company that handles the remaining inventory processes. Nonetheless, your company has to keep track of what it makes and what it ships out at minimum. So, there are two elements here, the actual manufacturing or assembly (covered earlier) and the tracking, storing, and moving of these products. These two functional areas are closely tied together and the interdependencies in these areas should be given special attention. If IT systems go down, how are these activities impacted? If the building is ravaged by fire or flood, how are these activities impacted? Systems automation and controls are not typically considered IT assets and are therefore outside the scope of our discussion. However, with the continuing integration of systems across the continuum of business, these systems likely have interfaces (upstream or downstream) to IT systems and must be included in the scope of the BIA assessment.

Other areas

There may be other functional areas not listed here that exist in your company. If so, be sure to explore each functional area and determine the various business processes used in each area along with their relationship to the business's IT systems.

REAL WORLD

Flaws Exposed

It's important to understand that a BIA is a thorough business assessment that involves an unbiased study of the entire organization. When you start looking at the workings of the company in a very close and detailed manner, things may start to look less than stellar, like when you shine a very bright light on something and you suddenly see all its flaws quite clearly. Your corporate executives might take one of two positions. In the best case, they will appreciate the opportunity to closely examine the company's operations and find ways to improve it along the way. In the worst case, they will hesitate, stonewall, or misdirect you in order to prevent you from uncovering business processes that are broken, inefficient, or worse, illegal. So, be prepared for a variety of reactions from the top to the bottom of your organization. Also, if you're so inclined, you might begin preparing your organization for this level of scrutiny, being sure to communicate the positive aspects of this process.

Ideally, you can double your mileage from this project by using it as an opportunity to perform your BIA and to streamline business operations. Just be prepared for a few bumps in this road, especially if you suspect that the business processes are not too pretty in some areas of the company. Remember, too, that a well-executed BIA can help you garner more support for your BC/DR planning project as people in the organization begin to understand the undesirable effects a disaster or disruption would have on the business. Sometimes seeing the flaws is motivation enough to fix them.

GATHERING DATA FOR THE BUSINESS IMPACT ANALYSIS

As we discussed in [Chapter 4](#), there are four primary ways of gathering information: questionnaires, interviews, documents, and research. This holds true for the BIA as well. Before you can develop questionnaires or interviews, however, you have to know what you're looking for. You may choose to gather SMEs who then create questionnaires or interview questions. As a project team, you may create a number of very specific questions or scenarios to be presented to SMEs in the form of questionnaires or interviews. The additional information will come from either the project team or SMEs reviewing documents or performing targeted research.

What's the best way to conduct a BIA? First, understand that your organizational leaders are busy, *really busy*, with other critical work. Don't expect an enthusiastic response to meeting invitations, interviews, assessments, or questionnaires. Assume just the opposite. If you do your homework and come prepared with data the operational owners can *respond* to, you are much more likely to make progress in this process.

You should have prepared, at minimum, the following data:

1. Detailed description of key systems, databases, and information processes, organized by functional area. *Note:* If you do not have this, work on completing this before talking with your operational owners. This is a significant IT deficiency if it does not yet exist. If you have it, ensure it is current and up-to-date.
2. Identification of IT application owners and their operational counterparts. In other words, you probably have a manager in the IT department responsible for your enterprise's financial system. Who do they consider their key customer for finance to be? Both the IT and the organizational owners of that system need to be involved in BIA discussions. *Note:* One way to break up your BIA is by IT manager application list. Each could be responsible for ensuring the completion of BIA activities for their key applications and customers, with guidance from an expert or project manager overseeing the BIA.
3. Clear description of system interdependencies, interfaces, and upstream/downstream systems. It's often helpful to have the IT managers responsible for critical applications to create a map of their systems and interfaces. These can be used in discussions with operational owners and can be used by the IT department to validate current knowledge about configuration and dependencies.
4. Qualitative and quantitative cost descriptions of downtime. Each IT manager and correlating business process owner should be able to quantify, in some meaningful way, the cost of downtime to that particular area of the business. It most likely will begin with a discussion of "what if" scenarios to help business process owners to understand what IT means by various BC/DR terms. You can help your operational owners by putting BC/DR terminology into plain language. How long can you afford to be without this system? What would you do to process if this system was not available? What would that cost?

As previously discussed, asking questions and providing scenarios to consider can help people focus on specific business issues and generate better responses. Some questions you might ask of your SMEs to help them focus on the key aspects of the impact analysis include these:

1. How would the department function if desktops, laptops, servers, e-mail, and Internet access were not available?
2. What single points of failure exist? What, if any, risk controls or risk management systems are currently in place?
3. What are the critical outsourced relationships and dependencies? What are the upstream and downstream risks to your business function?
4. If a business disruption occurred, what work-arounds would you use for your key business processes?
5. What is the minimum number of staff you would need and what functions would they need to carry out?
6. What are the key skills, knowledge, or expertise needed to recover? What are the key roles that must be present for the business to operate?
7. What critical security or operational controls are needed if systems are down?
8. How would this business function in a backup recovery site? What would be needed in terms of staff, equipment, supplies, communications, processes, and procedures? (This crosses into the DR element, which we'll discuss more in a [Chapter 7](#).)

Data collection methodologies

For the BIA, it is advisable to collect data through questionnaires, interviews, or workshops, which are in many ways group interviews. Additional data can be gathered using documents and research, but these data should be gathered only to support or supplement data gathered through direct contact with business SMEs. The reason for this is fairly obvious. Only those who actually perform various business functions can assess the criticality of those business functions. You could sit down and read documents all day long and never get a clear picture of what's really mission-critical and what's just important. Therefore, you should rely primarily on questionnaires, interviews, and workshops for this segment of your data gathering. Let's look at methodologies you can use for these three data gathering methods.

TIP

Don't Start with a Blank Page

The BIA interview process can be challenging enough as it is—from developing an approach to getting SMEs on board to actually getting on people's calendars—you'll have your hands full. To expedite this process, do as much prework as possible. While you don't want to slant the results by guiding it too narrowly, if you don't provide end-users with data with which to work, you will spend endless cycles trying to get everyone on the same page. Start with something and let your process owners respond. If you hand them a blank paper, you'll most likely get blank stares in return.

Questionnaires

Questionnaires can be used to gather data from SMEs in a fairly efficient manner. Though it takes time to develop a highly useful questionnaire, SMEs' responses will be consistent, focused, and concise. They can fill out the questionnaires regarding their business units, business functions, and business processes at a time that is convenient for them (within a specified time frame), thereby increasing the likelihood of participation. On the downside, questionnaires that are sent out may be ignored, pushed aside, or forgotten. In order to generate a timely and meaningful response to your team's questionnaire, you can create a methodology that will increase your response rate.

First, it's important to appropriately design the questionnaire. If it's full of useless questions, if it's visually confusing or overwhelming, you'll decrease your response rate. The questionnaire should be clear, concise, easy to understand, and fast to fill out. If you want to use a Web-based questionnaire that records data in a database, that's fine, but it's even easier to ignore an e-mail with a survey link in it. You can send out reminders with a link to the questionnaire as frequently as needed. With a paper-based questionnaire, there's a lot of moving of paper and the increased likelihood that the paper will be misplaced, lost in a pile, or simply thrown out. You should select the best method based on the culture in your organization.

It's also important to explain the purpose of the questionnaire to the participants in a manner that helps them buy into the process. Focus on what's in it for them, not for you. They probably don't care that *you* need these data, but they will care that these data could help prevent some problem in *their* jobs. Ideally, you should hold a kick off meeting where the questionnaire is introduced and explained, the purpose of it is clearly articulated, and the process for completing the questionnaire is explained. For example, you might let people know that the questionnaire is available at a particular location, that it takes a total of 3 hours to complete per department, but that it can be completed in segments and the questionnaire-in-progress can be saved for later completion. You should let people know who the contact person is if they run into problems and when the questionnaire must be completed. If you have a project manager assigned to this project, he or she should follow up routinely and offer assistance to ensure accurate and timely completion.

If your company is the type of company that likes to have a bit of fun in these kinds of meetings, you can also announce small prizes that will be awarded to departments or individuals who first complete theirs correctly, who are most thorough, and so forth. Be careful, though, you don't want to leave the impression that this is a race to the finish (where important details can be lost) or that "cute" answers are appropriate. You can, however, announce that any SME that submits a complete and thorough questionnaire by the deadline will be entered into a drawing for the chance to win some prize such as a tablet device, a new phone, or dinner for two at a nice restaurant, among others. Sometimes small incentives to do the right thing can go a long way in getting people to participate in the manner expected and needed. Considering how vital these particular data are to your entire BC/DR plan, it's usually worth a small investment to get people to participate appropriately, if this type of activity

fits in with your corporate culture. Be sure to provide information on how respondents can get assistance with the questionnaire—either from a technical standpoint (if it's an electronic or Web-based questionnaire) or an administrative standpoint. If they don't understand exactly what a question means, who should they contact? How should they contact them? What is the contact person's e-mail, location, phone number, and work hours? Be sure to provide this information so you don't inadvertently create roadblocks for yourself.

Finally, let the team know how they'll learn about the results of the questionnaire. Most people dislike spending time filling out a form only to never hear about it again. If they are willing to take the time needed to provide these data, there should be some reciprocity. For example, if these data are all pumped into a database, a report on each respondent's data should be provided back to them for verification. Once the data are reviewed by your team, there may be additional questions. Respondents should be told, in advance, about the process for following up with them regarding their responses to the questionnaire.

Once questionnaires are completed, you and your team should review them to ensure they are complete. In some cases, you may choose to create a process whereby certain questionnaires are followed up by an interview. This might be in the case of the most critical business functions or where questionnaire data indicates there may be confusion, conflict, or incomplete data. Any follow-up interviews should follow a specific format as well so that targeted data can be collected.

Interviews

If your team has decided that data will be gathered through interviews, you'll still need to create a questionnaire type of document that will provide the interviewers with a set of questions to which they gather responses. Free form or informal interviews will yield inconsistent data across the organization and you'll have a wide array of meaningless data. Develop a questionnaire and use it as the basis of the interview process. You may choose to send the interview questions in advance for those process owners who want to give some thought to the topic. Each interview should follow a predefined format and the questions asked of each respondent should be the same. Develop a questionnaire, interview, or question sheet from which the interviewer will work and also develop a corresponding data sheet onto which the interviewer can record responses. Look to find methods to speed up the interview process. For example, don't use a rating system of elements that use 1 as NEVER and 10 as ALWAYS with eight other word/number combinations. This will be cumbersome for the interviewer to describe and will be almost impossible for the interviewee to remember. If you choose, you might say, "On a scale of 1 to 10 with 1 being never and 10 being always, how often would you say you access the CRM database on a telephone sales call?" This sort of sliding scale can be used because the respondent does not have to remember 10 different descriptions—*what does three mean again?* However, the danger is that each respondent is going to give you a different sliding scale number if the range is 10. Instead, you might use a three-element scale without numbers. "How often do you use this system during a telephone

sales call? Never, sometimes, or always?" That's much easier for the respondent to remember and evaluate and it's also more likely to generate a more consistent response across all respondents.

If you're going to use interviews, you need to find the right person or team to conduct the interviews. Sometimes it's helpful to have one person interview and one person record answers or take notes. That can speed up the process and you can send out results almost real time for the process owner to review, validate, and amend as needed. You also need to ensure that the team isn't one that's too technical, that they don't talk too much or too little. We all know the stereotype of the IT person who would rather watch paint dry than talk to people (an antiquated stereotype, but helpful in steering you away from the wrong team members). We all can also conjure up an almost instant picture of someone we know or work with who just talks too much. They're enthusiastic and engaged and you not only can't get a word in edge-wise, you can't stay on the topic at hand. Avoid these two extremes and land somewhere in the middle with a team of interviewers who are knowledgeable, efficient, and skilled at facilitating meetings. Project managers often have these skills and you may tap your PM team for assistance with these interviews. Our goal is not to go into the pros and cons of various data gathering methods, but to point out that there are unintentional problems you can build into a questionnaire or survey that can skew your results. If your organization has a group that develops market surveys or questionnaires, you may ask them to review your questionnaire before rolling it out. They might spot something you missed and help you gather better data. We all know the output is only as good as the input, so making sure your data gathering methods are clean will help on the other side of this assessment process.

Once an interview is conducted, the data need to be reviewed and verified by the interviewee. Due to the nature of an interview, it's possible one of the people (interviewer and interviewee) misunderstood the question or response. Therefore, once the data are prepared, it should be reviewed by the interviewee before being finalized. You want to avoid having the interviewee rehash their previous responses, but you do want to provide an opportunity for additional insights and information that clarify previous responses. Follow-up interviews, if needed for clarification, should be scheduled as quickly after the initial interview as possible so that the data, response, and topic are still fresh in the interviewee's mind.

Workshops

Data collection workshops can be an effective method of gathering needed data. If you choose this method of gathering data, you might still choose to create a questionnaire so that you can be sure you cover all the required data points. Here are some elements to consider:

- Identify the appropriate level of participating personnel and gain agreement as to participants.
- Choose an appropriate time and place for the workshop, ensure the appropriate amenities will be available (white boards, refreshments, etc.).

- Develop a clear agenda for the meeting and distribute this, in advance, to meeting participants. Identify the workshop facilitator and clearly define his or her role in the process.
- Identify workshop completion criteria so the facilitator and participants are clear about what is expected, what the required outcomes are, and how the workshop will conclude.

The facilitator's job is to ensure the workshop objectives are met, so these objectives must be clearly articulated prior to the start of the workshop. Develop or utilize an appropriate process for dealing with issues during the workshop so that participants stay on topic and focused on the key objectives. Some companies use the concept of a "parking lot," where issues are written up on note cards and collected or written on sticky notes and posted on a white board or an empty wall. Use an issue-tracking methodology that allows you to stay on topic but make note of issues. Also identify the method you'll use for addressing those issues that cannot be (or should not be) resolved during the course of the workshop. Finally, ensure that the results of the workshop are written and well documented and that participants have the opportunity to review the results for errors and omissions before they are finalized.

TIP**Align with What Is**

Select the format for data gathering that is least intrusive on people's time and that is most aligned with how you normally work. BC/DR planning are often very low on people's priorities and anything you can do to reduce the effort it takes to provide the data you need will pay off.

DETERMINING THE IMPACT

We've delineated some of the more common business functions. Now, let's turn our attention to some of the specific impacts to a business. As with other lists, this one is extensive but not necessarily exhaustive. Be sure to review this list, remove any items that do not pertain to your business and add any elements that are not included that do relate to your business. Remember, too, that a business disruption can run the gamut from a hard drive failure to an earthquake that levels your building, to a pandemic that impacts an entire region or nation. Once you've looked at all the potential impact points, we'll discuss specific data points to collect and analyze, as well as how to put those together with your risk assessment data. The impact of any business disruption may include:

1. *Financial.* Loss of revenues, higher costs, potential legal liabilities with financial penalties.
2. *Customers and suppliers.* You may lose customers and suppliers due to your company's problems or you may lose customers or suppliers if they experience a business disruption or disaster.

3. *Employees and staff.* You may lose staff from death, injury, stress, or a decision to leave the firm in the aftermath of a significant business disruption or natural disaster. What are the key roles, positions, knowledge, skills, and expertise needed?
4. *Public relations and credibility.* Companies that experience business disruptions due to IT systems failures (lost or stolen data, modified data, inability to operate due to missing or corrupt data, etc.) have a serious public relations challenge in front of them. These kinds of failures require a well-thought-out PR plan to help support business credibility.
What impact would system outages or data losses have on your public image?
5. *Legal.* Regulations regarding worker health and safety, data privacy and security, and other legal constraints need to be assessed.
6. *Regulatory requirements.* You may be unable to meet minimum regulatory requirements in the event of certain business disruptions. You need to fully understand these regulations and their requirements related to business disruptions, both natural and man-made.
7. *Environmental.* Some companies may face environmental challenges if they experience failures of certain systems. Understanding the environmental impact of system and business failures is part of the BIA phase.
8. *Operational.* Clearly, operations are impacted by any business disruptions. These must be identified and ranked in terms of criticality.
9. *Human Resources.* How will staff be impacted by minor and major business disruptions? What is the impact of personnel responses to business operations? What are the qualitative issues to be addressed (morale, confidence, etc.)?
10. *Loss exposure.* What types of losses will your company face? These include property loss, revenue loss, fines, cash flow, accounts receivable, and accounts payable.
11. *Social and corporate image* (strongly tied to public relations). How will employees, customers, suppliers, partners, and the community view your company? How will its image be altered by a minor or major business disruption?
12. *Financial community credibility.* How will banks, investors, or other creditors respond to a minor or major business disruption? If the cause is a natural disaster, the challenges are different than if the cause is man-made. If the company failed to secure or protect data or resources, there are additional consequences both to the corporate image and to the company's credibility in the marketplace.

Adapted from [Disaster Recovery Institute \(2013\)](#).

After you've compiled a list of your business functions and processes, you should assign a criticality rating to them. Payroll, accounts payable, and accounts receivable

usually qualify as mission-critical business processes. Furniture requisitions for new employees usually fall to the bottom of the list as minor. Rate all your identified business processes and sort them in order of criticality. You might end up with a table or matrix that looks something like that shown in [Table 5.1](#).

Table 5.1 Business Function and Criticality Matrix

Business Function	Business Process	Criticality
Human Resources	Payroll	Mission-critical
	Employee background checks	Important
Finance	Debt payments/loan servicing	Vital
	Accounts receivable	Mission-critical
	Accounts payable	Mission-critical
	Quarterly tax filings	Mission-critical
Marketing and sales	Customer sales calls	Mission-critical
	Customer purchase history analysis	Vital

BUSINESS IMPACT ANALYSIS DATA POINTS

The number and type of data points you collect in your BIA are largely a function of the size and type of company in which you work. Smaller companies will have fewer data points, larger companies will have many more. However, you can also inundate yourself with too many data points if you don't take a focused approach. Some companies are extremely slow moving, analytical types of companies in which all data must be collected and assessed. Other companies move at the speed of light (typical in start-ups) and want to grab just the high points and move on. The plan you devise needs to find a balance between information overload and superficial data. Be sure to include enough detail so that you can actually develop strategies that will help your company survive a serious business disruption, but don't allow the information floodgates to open and overwhelm you with minutiae.

[Table 5.2](#) shows various data points you can consider collecting along with a brief description of the purpose or focus of that data point. Feel free to modify this to suit your unique needs.

Once you've collected all these data points for all your business functions and processes, you have a comprehensive understanding of your business, its key functions, and what would happen if those functions were disrupted. In [Chapter 6](#), we'll discuss how to develop risk mitigation strategies based both on the various risks your company faces and on the criticality of the various business functions as defined in this phase of the assessment.

Table 5.2 Business Impact Analysis Data Points

Data Point	Description	IT Dependencies
Business function or process	Short description of the business function or process (we'll use "function" from here on)	Describe primary IT systems used for this business function
Dependencies	Description of the dependencies to this function. What are the input and output points to this function? What has to happen or be available in order for this function to occur? What input is received, either from internal or external sources, that is required to perform this business function? How would the disruption of this business function impact other parts of the business? How and when would this disruption to other functions occur?	Describe IT systems that impact or are impacted by this business function. Are there any internal or external IT dependencies?
Resource dependencies	Is this business function dependent upon any key job functions? If so, which and to what extent? Is this business function dependent upon any unique resources? If so, what and to what extent (contractors, special equipment, etc.)?	Describe secondary/support computer/IT systems required for this business function to occur
Personnel dependencies	Is this function dependent on specialized skill, knowledge, or expertise? What are the key positions or roles associated with this function? What would happen if people in these roles were unavailable?	Describe key roles, positions, knowledge, expertise, experience, and certification needed to work with this particular IT system or IT/business function
Impact profile	When does this function occur? Is it hourly, daily, quarterly, or seasonally? Is there a specific time of day/week/year that this function is more at risk? If there a specific time at which the business is more at risk if this function does not occur (tax time, payroll periods, year-end inventory, etc.)?	Describe the critical timeline related to this function/process and related IT systems, if any
Operational	If this function did not occur, when and how would it impact the business? Would the impact be one time or recurring? Describe the operational impact of this function not occurring	Describe the impact on IT if this business function does not occur. Describe the impact on operations if this business function does not occur
Financial	If this function did not occur, what would be the financial impact to the business? When would the financial impact be felt or noticed? Would it be one time or recurring? Describe the financial impact of this function not occurring	

Continued

Table 5.2 Business Impact Analysis Data Points—cont'd

Data Point	Description	IT Dependencies
Backlog	At what point would work become backlogged?	Describe how a backlog would impact IT systems and other related or support systems
Recovery	What types of resources would be needed to support the function? How many resources would be needed and in what time frame (phones, desks, computers, printers, etc.)?	What resources, skills, and knowledge would be required to recover IT systems related to this business function?
Time to recover	What is the minimum time needed to recover this business function if disrupted? What is the maximum time this business function could be unavailable?	How long would it take to recover, restore, replace, or reconfigure IT systems related to this business function?
Service level agreements	Are there any service level agreements in place related to this business function? What are the requirements and metrics associated with these SLAs? How will SLAs be impacted by the disruption of this business function?	How would IT service levels be impacted by the disruption or lack of availability of this business function? How do external SLAs impact IT systems?
Technology	What hardware, software, applications, or other technological components are needed to support this function? What would happen if some of these components were not available? What would be the impact? How severely would the business function be impacted?	What IT assets are required to support/maintain this business function?
Desktops, laptops, and workstations	Does this business function require the use of "user" computer equipment?	What is the configuration data required for computer equipment?
Servers, networks, and Internet	Does this business function require the use of back-end computer equipment? Does it require connection to the network? Does it require access to or use of the Internet or other communications?	What is the configuration data required for servers and infrastructure equipment?
Work-arounds	Are there any manual work-around procedures that have been developed and tested? Would these enable the business function to be performed in the event of IT or systems failures? How long could these functions operate in manual or work-around mode? If no procedures have been developed, does it seem feasible to develop such procedures?	Are there any IT-related work-arounds related to this business function? If so, what are they and how could they be implemented?

Remote work	Can this business function be performed remotely, either from another business location or by employees working from home or other off-site locations?	Can this business function be performed remotely from an IT perspective? If so, what would it take to enable remote access or the ability to remotely perform this business function?
Workload shifting	Is it possible to shift this business function to another business unit that might not be impacted by the disruption? If so, what processes and procedures are in place or are needed to enable that function?	Are there other IT systems or resources that could pick up the load should a serious disruption occur?
Business/data records	Where are the business records related to this function stored or archived? Are they currently backed up? If so, how, with what frequency, where?	How and where are backups stored? Based on data provided, is the current backup strategy optimal, based on the risks and impact?
Reporting	Are there legal or regulatory reporting requirements of this business function? If so, what is the impact of a disruption of this business function to reporting requirements? Are there reporting work-arounds in place or could they be developed and implemented?	Are there other ways reporting data could be generated, stored, or reported if key business functions or systems were disabled?
Business disruption experience	Has this business function ever been disrupted before? If so, what was the disruption and what was the outcome? What was learned from this event that can be incorporated into this planning effort?	Has IT ever experienced the disruption of this business function in the past? If so, what was the nature and duration of the disruption? How was it addressed and what was learned from the event?
Competitive impact	What, if any, is the competitive impact to the company if this business function is disrupted? What would the impact be, when would the impact occur, when would the potential loss of customers or suppliers occur?	
Other issues	What other issues might be relevant when discussing this particular business function?	Are there other IT issues related to this specific business function that should be included or discussed?

REAL WORLD**Data Overload**

The difficulty with the BIA is that it can generate huge volumes of data that need to be sorted, assessed, and analyzed. There is no shortcut to getting this done, but it might help to keep the outcome in mind. The result you're looking for is an analysis of the critical functions and processes used in your company to conduct your company's business. Using the scenario approach can really help you focus in on the end result. If servers go down, if power goes out, if fire rages, if tornados strike, what are the most important things your company needs to accomplish to get business going again? We'll address the DR elements in an upcoming chapter—the things you need to do to stop the impact of the disruption or emergency before business can resume. For now, you need to understand what is absolutely essential to keep your business running. If you can keep this in mind as you go through this process, you're likely to be able to tune out the irrelevant and extraneous data more effectively. Once you've completed your BIA, you'll bring it back to your stakeholders (or end-users) for validation to ensure you have captured the key elements.

Understanding IT impact

As you can see from [Table 5.2](#), the IT functions can be correlated to the business functions and processes at each step. As you gather these data, you will need to continually correlate the business functions/processes with the IT systems used to carry out or facilitate those functions in order to avoid gaps in your planning. In most cases, the SMEs and participants in this analysis will discuss the relationship of the IT systems to these functions. However, it's important to continually look at the intersection of IT systems to these business functions since the SMEs and departmental representatives may not fully understand the interdependencies of data or systems across the enterprise. For example, an SME might understand that use of the CRM system is vital to her job, but she may not have a clue that the CRM system resides on a server on the fourth floor and requires data updates from three other external interfaces. From an IT perspective, you'll see this vital CRM function as a series of servers, applications, and data flows. As you work with the BC/DR team to map out the business functions and processes, you'll need to develop a parallel map of how that information intersects with IT equipment and functions.

CRITICAL CONCEPT**Developing Data and Business Function Maps**

Depending on the maturity of your IT shop (from a CMM type of perspective), you may or may not have your systems, databases, applications, and interfaces cleanly mapped out. If not, there's no time like the present. This is critical to a successful BIA, but more importantly, it's information you should have on hand for a myriad of purposes. When you patch, upgrade, replace, and repair—how do you know what you're impacting up and downstream? Without these data, it's guesswork. In businesses where IT is mission-critical, it's really irresponsible not to have these data mapped out, documented, and continuously updated. If you don't have it, get started on creating it internally in advance of meeting with your business process owners. You'll have your work in order and you'll not only look organized, you'll be organized.

In addition, you'll need to develop an understanding of how long it would take to replace or repair IT equipment based on the assessment of criticality. When you move into the risk mitigation phase, you might decide that the most optimal solution is to implement a fully redundant system for three key functions because the replacement or repair time for these systems exceeds the MTD. The analysis of the data gathered in this phase must include IT-specific data so that you can optimize your risk mitigation strategies (coming up in [Chapter 6](#)).

The impact of IT on business functions (and the impact of business functions on IT) is usually already pretty well understood by the IT department through normal IT activities. However, the information gathered in this BIA phase will bring to light new priorities, new gaps, and new challenges to be addressed through the IT department. Understanding how these data impact IT and how IT impacts these data is key to developing a solid BIA and a comprehensive BC/DR plan.

TIP**Business View of IT**

You may want to encourage your SMEs to include their assessment of the impact on IT systems and the impact of IT systems on their critical business processes. By having them include these data, you can see IT from their perspective. You might learn something new about how they use IT systems or what you can do to mitigate risk to key business processes using IT technologies. At the very least, it will help flesh out your IT impact analysis.

Example of BIA for small business

Let's look at an example to help make this entire process a bit more tangible. We're going to focus on a small business so we can keep the example relatively simple. You can then expand the concept to apply it to a business of any size.

A company of about 125 employees works out of a single location. They're situated in a light industrial area surrounded by warehouses and wholesalers. They sell a variety of specialty building hardware such as hard-to-find latches, fasteners, locks, and more. They purchase products from a variety of manufacturers and distributors and sell to a high end, niche market in their region. These customers call in orders periodically. The company also runs a Web site that has seen sales grow significantly in the past 3 years so that Web sales are now equal to non-Web sales. They are looking to modify their business processes to hold less inventory using a better just-in-time ordering system. This will also let them expand sales without expanding their physical location, which is important because they are running at maximum capacity for the building. They don't want to move into a larger facility, so they are relying on changes to their business process and technology to help them improved revenues and the bottom line while cutting costs.

The company, which we call ABC Hardware, does about \$20 million a year in sales, about half of that online. Their facility is a large space comprised mostly of warehouse space with some office space. They ship and receive packages daily for Web operations and they ship weekly for their non-Web customer orders.

This company's risks include:

- Risk of fire in the building
- Risk of flooding in the area
- Risk of chemical spill in the area
- Risk of upstream/downstream losses by suppliers, vendors, and customers

Let's focus on the risk of a fire in the building. If a fire started in the building, the damage might be contained to one of the areas, either warehouse or office. If the warehouse experienced a fire, inventory would be damaged and the ability to process inventory (receive, pick, pack, and ship) would be impaired. If the office area were to have a significant fire, computer systems, including the inventory management system, would be damaged or destroyed.

So, what are the critical business functions impacted by a fire in the warehouse? First, we have the sales function because inventory would be damaged. Second, we have the inventory function because physical systems for managing inventory would be damaged.

What are the processes impacted by a fire in the warehouse? The company has processes in place for the following:

1. Picking orders
2. Packing orders
3. Staging orders for shipment
4. Tracking shipments
5. Receiving new inventory
6. Stocking new inventory
7. Updating inventory systems with shipping and receiving data
8. Managing damaged or missing inventory
9. Processing returns of damaged or wrong items
10. Inputting inventory data into inventory system
11. Replenishing packing materials
12. Repairing warehouse equipment
13. Cleaning warehouse areas

You can see from the list that items 11 through 13 are not critical processes. Other items on the list may not be mission-critical either, but we started with a full list of what goes on in the warehouse. If a fire engulfed the warehouse area, it's possible the building would be off-limits due to safety concerns, the offices might be filled with smoke and unusable, and the inventory might be smoke and water damaged by the fire suppression systems or by the water the fire department would hose in to put the fire out. Therefore, let's assume that a fire would impact all these processes listed. The company has no inventory it can ship to customers. What are the most important processes that have to get up and running in order for the company to generate revenue and continue operations? Remember, we're not looking at any mitigation at this point—we're not looking at fire suppression systems or any fire insurance the

company may carry. We're simply looking at the impact of a fire on operations. (Fire is the most common disaster to strike businesses, so it's a worthwhile example.)

Remember, there are probably 14 other companies out there that are waiting for ABC Hardware to falter so they can swoop in and steal ABC's customers. ABC cannot afford to wait around for the water to dry and the smoke to clear before getting back into business. So, let's look at these first 10 items, along with criticality and comments, shown in [Table 5.3](#).

As you can see from this example, what normally might be high-priority processes shift to lower priorities in the aftermath of a fire. The key to recovery for this company is to sort out its inventory quickly so it knows what it can and cannot sell to

Table 5.3 Example of Business Process and Criticality for Small Business

Business Process	Criticality	Comment
Picking orders	Mission-critical	Orders cannot be picked if inventory is damaged
Packing orders	Mission-critical	Orders cannot be packed if they are not picked
Staging orders for shipment	Mission-critical	Orders cannot be shipped if not picked and packed
Tracking shipments	Mission-critical	Orders cannot be shipped if not picked and packed
Receiving new inventory	Important	New inventory can be added to inventory system
Stocking new inventory	Minor	New inventory cannot be stocked until damaged inventory is addressed
Updating inventory systems with ship/rec data	Mission-critical	No shipments going out, but incoming inventory should be added so the company knows how much good inventory they have. Damaged inventory should be removed from stock as quickly as possible
Managing damaged/missing inventory	Mission-critical	Normally, managing damaged inventory is a minor process. In the aftermath of a fire, damaged inventory should be processed as quickly as possible to enable the company to dispose of it as quickly as possible
Processing returns of damaged/wrong items from customers	Minor	Normally, processing damaged and returned items from customers would be a high priority. In the aftermath of a fire, this falls to a lower priority
Inputting inventory data into inventory system	Mission-critical	In order for the company to sell its products, it needs to know, very quickly, what inventory it has that is sellable and what inventory it has that is damaged and must be discarded

customers. The IT systems are not damaged (though a few warehouse computers might need to be replaced) and order processing can still occur. This includes taking phone and online orders, processing orders, comparing orders to inventory levels, charging customer accounts or credit cards, and recording customer data (address, phone, etc.). Thus, the sales function for the company is relatively unharmed, but the ability of the company to process and fulfill those sales is impacted.

The BIA for this company now has identified the critical functions in the warehouse with regard to sales, inventory management, and shipping/receiving. The list is not exhaustive. For example, it does not include shipping supply replenishment. In the immediate aftermath of the fire, perhaps no shipments can go out, so this may not be a problem. However, it's likely that shipping supplies have been destroyed either by fire, smoke, or water, and need to be replaced before *any* shipments can go out. If the entire warehouse is impacted, there may be no saleable inventory and shipments will have to wait. In other cases, there may still be saleable inventory and the lack of shipping supplies would actually become a major problem. Therefore, replenishing shipping supplies as a process in the aftermath of a disruption might be mission-critical. This is how walking through scenarios helps you see the mission-critical processes more clearly. Remember, too, that as you walk through these scenarios for your own company, keep notes because great ideas about how to improve processes might pop up along the way.

Next, what is the MTD for these critical business functions and processes? Some of this company's customers are custom homebuilders who are working on tight timelines. They will not wait for a delayed order from ABC Hardware and will look elsewhere for these products. Therefore, ABC believes that with most of their orders, they have 1 week to recover operations before they begin losing serious revenue. In the risk mitigation phase of their assessment, this company's staff can devise a number of strategies to deal with this scenario either to prevent a fire from occurring or to create alternate fulfillment strategies in the event a fire does occur. This may include working with suppliers to drop ship, setting up an alternate warehouse location temporarily, and hiring a fulfillment house to take on the work in the interim and more. These are not IT functions, but this should give you the idea of how to approach your own company-wide and IT-specific BIA.

You can continue to expand this example to include other data. For example, you can include the expected financial impact, as shown in [Table 5.4](#). The example is not complete but shows the beginning of this process as a sample of how you might capture financial impact data.

The first function, the sales function, in this example, is not immediately impacted by the fire in the warehouse. Sales are still generated through the Web site and sales people may still be able to access CRM systems and other sales tools to generate sales. The problem is not on the sales generation side but the order fulfillment side. At some point, the company's inability to process inventory and orders will affect sales. Customers whose orders are delayed may cancel, rumors may cause other customers to order from your competitors. If you can't receive new inventory or ship out existing orders, these will eventually impact sales, but not immediately. If

Table 5.4 Small Business Financial Impact Example

Business Function	Business Process	Financial Impact
Sales	Generating new orders	Delayed impact
Warehouse	Picking orders	\$2000 per day
	Packing orders	\$2000 per day
	Shipping orders	\$10,000 per day
	Receiving inventory	\$4500 per day
Customer service	Handle customer problems	\$3000

you can forecast the delayed financial impact, that's great, but if you can't, just make a note that there is one down the line. We've also included an increased cost for customer service. If you have a fire and word gets out, customers may call about their orders, call to change or cancel their orders, or call to get assurance their order is in process. This may generate more work for customer service, which may require bringing in temporary help to staff the phones or existing staff to work overtime to handle the increased volume.

So far, we've seen little or no IT impact. The damage was contained to the warehouse and other than three computers used at the shipping and receiving stations, there was no other impact to IT. However, there are other IT tie-ins. For example, how will the company know the exact status of the inventory? When was the last inventory count performed? What is the status of the orders that were picked and packed—were they shipped or not? Which customer orders went out and which were on the dock awaiting shipment? Which returns were on the dock when the fire started and which were already processed? In this case, the company needs to quickly figure out the current status of its inventory as well as the status of customer sales and returns. It needs to know exactly what the status of everything is so that it can figure out what to do and in what order. IT may need to run special reports, print out inventory, shipment, or order lists in order to help warehouse functions get up and running again. These are DR tasks that the warehouse and IT staff will have to work together on to determine what might be needed.

Let's extend this scenario and ask, what if the IT systems were located next to the warehouse and the server room was partially destroyed by fire? What if the fire started in the server room and spread to the warehouse? Now the scenario has changed significantly because not only do you have damaged inventory and uncertain status of shipments but also you don't have IT system data immediately available to help sort things out. Sales data, inventory status, payables, and receivables are all unavailable. The server room is charred, all systems are unusable. Now what?

Let's extend this just a bit so you can get the bigger picture. **Table 5.5** shows some of the other operational impacts that might occur as a result of a warehouse fire. The impact on operations shows, for example, that customer perception is not impacted in the sales function.

Table 5.5 Operational Impact—Warehouse Fire Example

Business Function	Business Process	Cash Flow	Investor/Market Confidence	Market Share	Competitive Position	Customer Perception	Employee Impact
Sales	Generate new orders	Medium	Medium	Medium	High	N/A	Low
	Warehouse pick orders	High	Medium	Medium	High	N/A	High
	Pack orders	High	Medium	Medium	High	N/A	High
	Ship orders	High	Medium	High	High	High	High
	Receive inventory	Medium	N/A	N/A	N/A	High	High
Customer service	Handle customer problems	Low	Low	Low	Medium	High	High

Customers may or may not know about the warehouse fire and if they can still place their order via the phone or Web, there is no immediate impact to customer perception. The same holds true for the customer perception of picking and packing orders. Customers usually don't know how their order shows up at their door (nor do they usually care); they care that the right products show up on time. Therefore, we begin to see a customer perception impact in the processes of "ship orders" and "receive inventory." If inventory can't be shipped, customers don't receive their orders as promised and this impacts customer perception. If inventory can't be received, it isn't available for sale and the customer sees that products are out of stock. We won't go through every cell in the grid, but you can use this to understand how various operations are impacted by a warehouse fire. The employee impact, in this case, is focused on warehouse staff, who are highly impacted by the warehouse fire. Though we did not do it in this example, you could also document the key knowledge and expertise needed to carry out these functions. For example, the key skills needed in this case are people who know how to manage inventory so that orders are properly filled and inventory levels are properly tracked. These data can be added, as appropriate. The same can be done for the IT side of the process. If IT systems were down, which processes would be impacted and how would other operations be impacted? What skills and expertise would be needed for work-arounds and recovery?

As you can see, this scenario focused on the warehouse department. The warehouse manager or someone designated by the manager should participate in this BC planning process. Only someone working in the warehouse is going to be familiar enough with the various day-to-day processes to generate a realistic view of the impact of various business disruptions. Once they have walked through all the risk scenarios (we mentioned fire, flood, chemical spill, and upstream/downstream impacts earlier), they can assign the criticality, the MTD, the operational impact, financial impact, and the employee impact.

You may also choose to include additional columns in your impact table (or in your analysis if you choose not to use a tabular format) such as the financial impact and the legal impact. In this scenario, we also could have included the dependencies. Sales are impacted by the availability of inventory data. Receivables are impacted by the ability to pick, pack, and ship inventory. Payables are impacted by the ability to receive inventory and manage missing/damaged inventory. Payroll is impacted by having to work additional hours to manage inventory damage from the fire as well as to perform work outside the normal scope of warehouse operations. Expenses go up because additional supplies must be purchased to replace the supplies lost in the fire. Sales are down because shipments cannot go out until inventory is adjusted and some customers have purchased elsewhere. The building has to be cleaned by a professional company that specializes in recovering from fire damage and that impacts operations and increases the company's expenses with an unplanned expenditure. If the costs of the fire are covered by insurance, you still have deductibles that cause increase expenses at a time sales are down, or you may have delays in getting needed repairs waiting on the insurance process to complete.

What you'll discover from this exercise is that as you walk through these scenarios, you'll begin getting ideas about how to mitigate the impact of these disruptions. In [Chapter 6](#), when we discuss mitigation strategies, you'll find that one mitigation strategy might be helpful for three or four different risk scenarios. Thus, what would reduce your risk in the event of a fire might also be an excellent strategy for mitigating the risk of flooding or a chemical spill in the area. These economies are found only by thoroughly assessing risks and impacts so you can see the big picture and develop optimal mitigation strategies.

Now that you have identified the critical business processes for the warehouse department, you can also look at the impact a flood would have. For example, if employees cannot get to work, if trucks cannot come in to deliver inventory, if trucks cannot pick up shipments, many of these activities are impacted. If the warehouse area is flooded, you have a similar problem as you did with a fire. If the area surrounding the building is flooded but your inventory and IT systems remain intact, you have a different set of challenges.

By identifying the critical business functions and processes, you can clearly see the impact various risk sources would have on the business. You can assign criticality and MTD in preparation for developing effective strategies for addressing these risks.

If you were to continue with this example, you would define specific recovery objectives based on criticality, you would identify organizational and system dependencies, and you would define work-around procedures that could be used. This would comprise the impact analysis for the warehouse department for the risk of fire. If you expand it to include the same assessments for each threat source identified in your risk assessment, you would have a comprehensive impact analysis for your warehouse department. Each department in the company would complete this process and you'd have the risk assessment and impact analysis for the entire company. As you can see from just this small example, it's a large undertaking and may well take more time than any other part of your project. Allow enough time to get this completed but don't let it get long and drawn out. Most of this can be completed by departments in a reasonable amount of time, though the more complex the business systems, the longer it will take to perform this assessment.

PREPARING THE BUSINESS IMPACT ANALYSIS REPORT

There is no standardized format for a BIA report and, as with many other processes, this document will likely follow your company's standard format. At the minimum, the report should include the business functions, the criticality and impact assessments (see the list in [Table 5.2](#)), and the MTD assessment for each. Dependencies, both internal and external, should be noted and the correlation to IT systems should be delineated. It may help to organize the data by business unit or business function.

TIP**Useful Format, Useful Data**

Since much of the data can be captured in tables, using a table format in your report, along with brief explanations and notes as text, may help keep the data organized. The report serves two purposes: to capture and record data for further IT planning and to reflect back to stakeholders or end-users the information they have provided about the criticality of IT assets. Regardless of the format you use, the data must be well organized and meaningful to your audience.

This report should be prepared in draft format with initial impact findings and issues to be resolved. The participating managers, SMEs, and BC/DR team members should review the findings. Revise the report based on participants' feedback to the draft document. If needed, you can schedule a review meeting to discuss the finding in the draft. Often this is helpful (and needed) to resolve conflicts with regard to the criticality and MTD ratings, since there is a correlation between these ratings and the cost of mitigating the risks and reducing downtime. Once the feedback has been gathered, revise the draft and finalize the document. This document, depicted at the outset of this chapter in [Figure 5.2](#), is used along with the risk assessment as an input to the risk mitigation process. To assist you in preparing your final report, we've recapped the elements you may choose to include.

- Key processes and functions
- Process and resource interdependence
- IT dependencies
- Criticality and impact on operations
- Backlog information
- Key roles, positions, skills, knowledge, and expertise needed
- Recovery time requirements
- Recovery resources
- Service level agreements
- Technology (IT and non-IT technology)
- Financial, legal, operations, market, and staff impacts
- Work-around procedures
- Remote work and workload shifting
- Business data and key records
- Reporting
- Competitive impact
- Investor/market impact
- Customer perception impact
- Other (business-specific data not already included)

As you close out the BIA phase, it's vital to collect feedback from your end-users to ensure you captured the data correctly. This is not a time to revisit every line item or rehash every decision about the criticality of data; it is, however, the time to ensure

you and your end-users are in agreement about what's needed to run the business in the event of a disaster. This will become the "document of record" and will be the basis for how you and your team develop risk mitigation strategies, so it needs to be as accurate as possible. It's also important that you have stakeholders both informed and aligned with the outcome so there are no surprises and no gaps down the road.

SUMMARY

Performing the BIA requires you to look at your entire organization from top to bottom. You can begin by gathering SMEs, whether division heads, departmental managers, or designated staff, from various parts of your company. These people should be those in the company best able to answer the questions related to critical business activities. This relates to how your company generates revenues, tracks customers and sales, and other key business processes.

Data can be gathered using questionnaires, interview, workshops, documents, and research. There are pros and cons to each approach, so be sure to select the method most appropriate to your organization. Since each company is unique, there is no "one size fits all" template you can use to delineate all critical business processes for all companies. However, throughout this chapter, we have discussed a wide variety of business functions, processes, and approaches that can help you develop a comprehensive list of your company's critical processes as well as the key roles, expertise, and knowledge needed to carry out those critical processes.

Once these data are collected, each process must be assessed for criticality. In the big picture, how critical is each business process to your company's ability to continue operating? Using a three- or four-point rating system will help you look across the depth and breadth of your organization to understand which processes and functions are mission-critical, which are vital or essential, which are important, and which are minor. Your risk mitigation planning efforts will focus first on mission-critical processes and then to vital or essential processes.

You'll also need to develop your RTOs for each critical function. In some cases, you might choose to associate a recovery time with criticality ratings. For example, mission-critical functions might need to be recovered within 24 hours whereas vital or essential functions might need to be recovered within 72 hours. Alternately, you can assign criticality and then assign RTOs to each process individually. This might make more sense in companies where there are numerous mission-critical processes that cannot be simultaneously addressed. Again, this is a decision you and your team have to make regarding recovery objectives. Input from division or departmental experts is key to understanding required recovery time frames as well as key inter-dependencies that exist among departments, processes, and systems.

There is a relationship between the cost of recovery and the cost of downtime. Each company has to assess these costs and make decisions regarding the optimal point of intersection. The longer the company goes without a key process, the more

expensive it becomes due to loss of sales and increase in costs associated with the outage. However, recovery costs go down the longer you have to recover. If you need to recover within hours, your costs to provide this type of recovery capability will be significantly higher than if you need to recover within days. The point at which downtime costs and recovery costs intersect is the optimal point for planning, though in the real world, it can be difficult to determine the exact point of intersection. Keeping this concept in mind, however, will help you find the best solutions for your company.

The BIA uses business functions, business processes, and IT systems as the input points. The analysis is performed so that each process is identified and analyzed. The output for each process and function includes criticality assessment, financial impact analysis, operational impact analysis, recovery objectives, dependencies, and work-around procedures. When this is documented for each business function and key business process, you have a comprehensive look at your company and a solid BIA.

KEY CONCEPTS

BIA overview

- After identifying risks and threats to the company, the business impact must be evaluated. Key business functions and processes are viewed in light of risk assessment data.
- The impact of disruptions not only to your business but to upstream and downstream partners needs to be considered.
- Consider the impact on corporate employees including physical or emotional injuries in the aftermath of a serious event or natural disaster. People respond in many ways to disasters and your plan must have the flexibility to allow for a variety of responses.
- For each key business process, critical objectives, timelines, dependencies, and impact must be understood and analyzed.
- The impact of the disruption of key business functions is assessed and prioritized so that risk mitigation strategies can be developed.

Understanding impact criticality

- Not all business functions and processes are mission-critical. Your risk mitigation strategy planning usually is limited to those functions and processes that are vital to the ongoing operations of the company.
- You can use a three- or four-point system of rating criticality. The four-point system ratings are mission-critical, vital (essential), important, and minor. If a three-point system works better for you, you can use mission-critical, important, and minor. Define these clearly so they are used consistently across the organization.

- All processes should be assessed for criticality. Recovery objectives must also be assigned. Some companies assign the recovery time with the criticality. Therefore, mission-critical would have a recovery objective of 0-4 hours, for example. Other companies choose to set recovery objectives separately.
- The total time it takes to recover from a business disruption includes the RPO, which is the lag between the time of the last good backup and the business disruption, the time it takes to recover systems, the time it takes to recover data, and the testing and verification of repaired systems. This is often called the MTD or MTO.
- There is an optimal point between the cost of downtime and the cost of recovery. The longer systems are down, the more expensive it is for your company. The shorter the required recovery time, the more expensive it is for your company. Therefore, the intersection of the cost of downtime and the cost of recovery is the optimal point. This is not always easy to determine but the concept helps in your planning efforts.

Identifying business functions

- Business functions are areas of the company that have specific roles or purposes such as sales, operations, finance, or HR. Business processes are the defined methods and actions used to achieve those purposes. Both functions and processes must be assessed in order to fully understand the company's critical work.
- The most common business functions include facilities, security, HR, IT, legal, compliance, manufacturing/assembly, marketing/sales, operations, research/development, and warehouse/inventory.
- The most common business processes include sales, invoicing, inventory management, and payroll, to name just a few.

Gathering impact data

- Gathering data for your BIA is a significant undertaking. Enlisting SMEs from around the company is vital to your success.
- Using scenario-based questions, you can help SMEs understand what you're asking of them and help them envision potential problems. The more realistic your scenarios, the better data you'll gather.
- The data you gather should include the business function, process, criticality, time to recovery, dependencies, financial and operational impact, and other relevant data.
- You can use questionnaires, interviews, workshops, documents, and research to gather data. There are pros and cons to each approach; use the one that best fits your organization's way of doing business.

Determining impact

- Determining the impact runs the gamut from financial to legal to operational to environmental and beyond. It's important to understand the impact to the company from these various perspectives, even if your focus is on the impact related to IT systems.
- The impact of a business disruption may have serious legal, financial, or regulatory consequences. These typically come from outside the organization and should be included in your planning. It's sometimes easy to miss these external elements when focusing solely on internal business impacts.
- The company's reputation in the community, region, or marketplace can be greatly impacted by a business disruption, especially if that disruption has to do with data security, data loss, or other sensitive areas. This should also be taken into consideration as you look at the impact analysis.

BIA data points

- There are numerous data points that can be collected about business processes across the organization. A comprehensive look will include these data points along with the interdependencies and impact on/with IT systems.
- For each critical business process, the impact on and impact from IT systems should be mapped out. In some cases, the disruption of a business process impacts IT systems. In other cases, the disruption of business processes does not impact IT but the disruption of IT systems, either primary or secondary, can impact key business processes. These interdependencies must be clearly understood and documented.
- External elements such as regulatory compliance, reporting, and corporate reputation must also be addressed. Again, the IT relationship must also be addressed. Often there is no leeway in meeting financial or legal obligations, regardless of the nature of the business disruption. There may be a bit of flexibility if a large natural disaster impacts the firm, but an isolated event such as localized flooding or fire will not alter regulatory, legal, or financial requirements on the firm.
- Review the final BIA document with stakeholders to ensure there are no gaps, oversights, or misunderstandings. The BIA forms the basis for risk mitigation and BC/DR plan development, so your inputs must be comprehensive and accurate.

References

Disaster Recovery Institute. Home page; 2013. <http://www.drii.org>, [Retrieved May 26, 2013], from Disaster Recovery Institute.

Swanson M, Bowen P, Phillips AW, Gallup D, Lynes D. Contingency planning guide for federal information systems; 2010. <http://csrc.nist.gov/publications/nistpubs/800-34-rev1/>

[sp800-34-rev1_errata-Nov11-2010.pdf](#), [Retrieved May 26, 2013], from National Institute of Standards and Technology.

The Business Continuity Institute. Good practices guidelines; The Business Continuity Institute; 2005, p. 21.

The Business Continuity Institute. Home page; 2013. <http://www.thebci.org>, [Retrieved May 26, 2013], from The Business Continuity Institute.

Business Continuity and Disaster Recovery in Healthcare

IN THIS CHAPTER

- Introduction to healthcare IT
- Regulatory requirements
- Healthcare IT risk management
- Technical needs—Healthcare IT architecture
- Operational needs—Ensuring confidentiality, integrity, and availability of medical data
- Interoperability among disparate systems—Integration in healthcare IT
- Current environment and new technology
- Healthcare IT business continuity best practices
- Summary
- Key concepts

INTRODUCTION TO HEALTHCARE IT

Enter any modern emergency room in the United States and you'll instantly be barraged with technology. From the clerk who checks you in on the computer, to the nurse who takes your temperature with a digital thermometer, to the tech who measures your oxygen saturation reading with another electronic device, to the heart rate and blood pressure monitor the nurse attaches to you, to the nurse and physician who assess and record their findings on a tablet or computer—technology is utilized in just about every aspect of delivering healthcare in the United States. Some of this technology integrates into the electronic medical record (EMR) through interfaces; some of it is read and results are manually recorded into the medical record. Ultimately, it all ends up in your medical record if it's measured or noted during an Emergency Department (ED) visit. This gives you some visibility into the complex and dynamic world of healthcare information technology (IT).

In the past decade and more than ever before, technology has been deployed, used, and integrated in the healthcare setting. Whether it's at a rural doctor's office or an urban trauma center, technology has made its way into every corner of healthcare. Technology is employed in order to provide a higher quality of care with the ultimate objective of improving the clinical outcome for the patient. When routine processes can be automated, when alerts can prevent errors, and when information can be stored for instant retrieval and later analysis, technology can make a positive

difference in the quality of healthcare delivery. But technology is not the reason that better care is delivered; technology is simply an enabler. If technology is not deployed in a thoughtful and useful manner, it simply gets in the way of the end user trying to deliver patient care. Every year, more healthcare organizations—from physician offices to community clinics to regional hospitals to trauma centers to surgical centers—deploy more technology in hopes of simultaneously improving patient care and clinical outcomes while driving down cost through efficiency, accuracy, and timeliness.

The current environment is challenging on many fronts, as well. Healthcare providers face patient safety issues, variable clinical quality, complex administrative and regulatory requirements, rapidly increasing costs, and a more educated patient (better educated about healthcare, higher expectations around that care). In order to address these challenges, organizations must integrate data from a variety of internal and external sources and present those data in some meaningful way. That is the work of healthcare IT departments. The IT investments are huge. According to a report from the Center for Information Technology Leadership (CITL), needed investments in healthcare IT in the United States are estimated in excess of \$275 billion ([Center for Information Technology Leadership, 2004](#)).

On the flip side of this equation are increasing costs of doing business from higher costs for insurance to supply costs to specialty treatments that did not exist even a decade ago. The cost of doing business for many healthcare organizations is the cost of providing care to those who cannot afford to pay. During the recent economic downturn, many people lost their jobs and their health insurance coverage. Community organizations were strapped with burgeoning bad debt from individuals who needed care but could not pay. That care is never free—staff still need to receive paychecks, vendors still need to be paid for supplies—someone has to absorb those costs.

The drive in healthcare and in healthcare IT, in particular, is to find ways to use technology to reduce the cost of care while simultaneously improving the clinical outcomes. It's reasonable to assume that if the results of laboratory blood tests are in the EMR within 30 minutes of the results occurring in the lab, the physician can make faster clinical decisions with accurate lab data. Giving the right antibiotic as early as possible after surgery could improve the recovery time and enable the patient to return home to their family a day earlier. That reduces the cost of care while improving the clinical outcome.

There are many examples that demonstrate this potential, but as with so many things, the devil is in the detail. How healthcare IT is implemented and utilized is largely determined by healthcare leadership. Some hospital executives understand the strategic importance, some do not. Regardless of where the healthcare organization is on that continuum, there is a drive to utilize and integrate technology from all sides. Physicians are demanding new clinical technologies, many of which have databases, patient information interfaces, server and storage requirements, and network connectivity. Nursing and clinical leadership want tools to automate routine tasks, such as being able to automatically enter patient vital signs (heart rate,

oxygen saturation, respiration rate, temperature, etc.) into the EMR. This frees up clinical staff to pay attention to higher order tasks that can make a difference in the clinical outcome. Legal and risk management want more data for reporting purposes. Quality wants universes of data built so they can extract and extrapolate data to correlate initiatives and events with trends. Hospitals are held to metrics surrounding the management of certain clinical results and the folks in quality are always consuming the latest data in order to generate the chart that shows the data in exactly the way it's needed for the auditor or the report out or the next meeting. The buzz in the IT industry these days is "big data," and healthcare IT has terabytes and petabytes and exabytes of data that can be sliced and diced a million different ways.

In this chapter, we're going to look at a broad swath of healthcare and healthcare IT. The intent is not to be exhaustive, comprehensive, or complete in any of these areas. That would not only be next to impossible, but it's far outside the scope of this book. The intent of this chapter is to simply act as a tour guide and point out features along the way. It's not based on any particular healthcare organization nor on any type of healthcare IT solution. If you had everyone in your healthcare organization read this chapter, some of them would no doubt say "but what about . . .?" This chapter is intended to help you get smarter about healthcare and healthcare IT, even if you work in this field. Even if you don't work in this field, this chapter will help you think about how to dissect complex IT environments for business continuity and disaster recovery (BC/DR) planning purposes, where IT supports varied business and operational functions and where the implementation of IT includes communication and integration between closed proprietary systems as well as open systems. Many healthcare IT staff, like IT staff in other industries, have a pretty limited view of their overall organization, how it operates, where its challenges lie, and how those systems interact. This chapter will help connect the dots and provide an overview that will help you develop a better, more comprehensive, and more manageable BC/DR plan. All good BC/DR plans start with a strong understanding of the organization, the industry, and the overall IT environment in which you're operating. This chapter will be useful for those in healthcare IT, as well as those outside healthcare IT, in understanding complexity and BC/DR planning. Along the way, you'll learn a bit more about healthcare IT in the United States, which can be useful no matter where you work.

Types of healthcare organizations

Before we delve too far into this topic, let's take a few paragraphs to define some of the types of healthcare organizations. This list is by no means exhaustive, but even if you work in healthcare IT, this list may remind you of some of the other types of providers out there. For the rest of you, it will be a good round up of the major players. We're not going to differentiate by level of care or ownership; we'll keep it pretty simple.

Hospitals

Hospitals are, of course, the most visible types of healthcare providers in the community. Hospitals can provide various levels of care but are primarily focused on higher acuity patients (people who need more clinical care). Once a patient's acuity reaches a certain lower threshold, they are discharged from the hospital. They may not be ready to go home (i.e., discharge from the hospital does not mean they are "well"), but they no longer need the level of care provided in a hospital. Hospital services can run from trauma centers to labor and delivery, surgery to respiratory therapy, emergency care to neonatal intensive care units, and everything in between.

Skilled nursing facility

A skilled nursing facility is often a "step down" for patients leaving the hospital. Skilled nursing facilities (SNFs) offer care to lower acuity patients, typically those who need rehabilitation services of some sort. SNFs may provide long-term, intermediate-term, or short-term care for patients. Home healthcare, where care is delivered in the patient's home, also falls into this category. From an IT perspective, many SNFs lack strong IT infrastructure and much of the documentation is on paper. However, as EMRs make more and more in-roads, many of these facilities are now considering implementing an EMR. In a later section, we'll look at how all these data may all come together someday soon through health information exchanges and regional health information organizations (HIE/RHIO).

Physician offices

Physician offices range from sole practitioners to large, multispecialty offices. Regardless of the size or specialty, physician offices are where primary and specialty care occurs. From family practice to every specialty you can think of (and probably many you would never think of), physician practices are located throughout the United States in rural, suburban, and urban settings. With recent governmental incentives (and upcoming penalties), more and more physician practices are looking to implement an EMR. In some cases, they are purchasing, installing, and managing a stand-alone system. In other cases, they are implementing an extended version of an EMR installed and managed by another entity—most often a hospital or hospital system.

Regardless of the source of the EMR, physician practices are going electronic. However, many lack the staff and the IT know-how to manage data and systems at what might be termed "enterprise" level. From an information security and BC/DR perspective, many physician practices are ill-prepared to conform to best practices and industry regulation. This is where your IT shop may intersect with these practices. Whether your organization is the entity selling the EMR to a stand-alone physician practice or a hospital extending its ambulatory EMR module out to local (or remote) physician practices, you may be responsible for ensuring the confidentiality, integrity, and availability (CIA) of their data. When you provide a service at a contractual level, you may have legal and/or contractual obligations with respect to service levels, support boundaries, information security, guaranteed uptime

(information availability), and more. If your IT shop is involved in this side of the business, you will also need to ensure you have included physician practices in BC/DR discussions. If you're a service provider, understanding the requirements for EMR, Meaningful Use, and ICD-10 (diagnostic code changes occurring in the next couple of years) may be a significant competitive advantage to your shop and may enable you to create an area of expertise to sell into your local marketplace. Even if you are not in healthcare IT, you may well be involved with providing both internal and external IT services, which creates unique BC/DR challenges.

Ambulatory clinics

Ambulatory clinics are sometimes called outpatient clinics or ambulatory centers. They are medical facilities that perform procedures that do not require an overnight stay in a hospital or care facility. They may include preventive, diagnostic, or treatment services. For example, some minor surgeries are performed as outpatient procedures as are pain management, chemotherapy, wound care, physical therapies, and more. With the advancement of many medical technologies and techniques, more procedures can be safely performed on an outpatient basis than in the past.

Ambulatory centers offer a form of primary care and are similar to physician offices or long-term care facilities in that they may or may not be part of a larger healthcare organization. Depending on size, location, and affiliation, the ambulatory clinics may or may not have implemented an EMR. As with physician offices, if these types of entities are in your healthcare IT world, you need to address BC/DR functions with them to ensure they can continue to safely see patients if IT systems are unavailable (or worse, destroyed).

Pharmacies

Many hospitals have both inpatient and outpatient pharmacy functions. Inpatient pharmacies supply drugs and pharmaceutical products to patients admitted to the hospital or having outpatient surgeries or procedures in the hospital. Outpatient pharmacies provide services to those who are not patients in the hospital, whether that means people having been discharged with a prescription to be filled or people from the general population who have a prescription from their primary care provider and need it filled.

Pharmacies generally all have electronic systems these days, if for no other purpose than tracking patient demographic data (home address, phone number, primary care physician (PCP), insurance, etc.) and for inventory management. Federally controlled substances must be tightly controlled and accounted for, so pharmacies have long had electronic systems to assist with this function. Over the past decade or so, pharmacies have begun integrating with EMRs. Again, if your organization has a pharmacy function, your IT shop may be responsible for ensuring downtime data are available for pharmacy staff. For inpatient pharmacies, that might mean having access to EMR downtime data; for outpatient pharmacies, it might mean having alternate solutions. Regardless, your BC/DR plan may include pharmacy functions.

Other types of organizations

In addition to hospitals, ambulatory clinics or centers, physician offices, and SNFs, other types of HCOs include, but are not limited to:

- Radiology providers
- Lab providers
- Specialists' offices
- Short-term or long-term care facilities
- Behavior health facilities.

Let's look at a behavioral health facility as an example. What are the healthcare IT needs related to BC/DR for a behavioral health facility? You are still responsible for ensuring the CIA of patient data. You are responsible for ensuring medical notes, test results, and other medical data recorded in the EMR are available for patient care. Regardless of the healthcare setting you work in (or interact with), you need to think through how you will ensure the CIA of patient and financial (i.e., all business) data.

We're not going to review an exhaustive list of all possible types of organizations in healthcare today, but this should provide a useful overview. As you look at your healthcare organization and begin to assess your BC/DR needs, you also need give some thought to the organizations in your community with whom your healthcare IT may connect. Your job is to take a look at your organization and ensure that all the places your IT intersects with others, you have an understanding of whose data they are, who is responsible for it, and what happens if those data are not available.

Summary of healthcare organizations

As you can see, there is a wide range of healthcare organizations. In your IT organization, you likely have visibility in some manner to these functions. For example, you have servers that host discrete applications used by some of these types of healthcare organizations such as physician offices, ambulatory centers, or pharmacies. However, you may not have been thinking about the implications of these applications and business entities on your BC/DR planning. The net of it is this: if you believe there is an application or function that runs through your data center, your servers, your storage, or your network, it should be on the list of items to explore during your BC/DR analysis phase. It's fine if you assess it and decide it's out of scope for now, out of scope altogether, or not relevant, but be sure it's a conscious decision and not simply an oversight.

The rising cost of healthcare

The cost of healthcare in the United States continues to climb as our population ages and people live longer with more chronic conditions. The good news is our healthcare system can treat more types of ailments than in the past resulted in death. The bad news is that the cost of healthcare is growing exponentially and if it continues on its current trajectory, none of us will be able to afford healthcare in the future. Current

governmental initiatives are designed to help drive quality up and cost down. It can be done and technology, while not the cure-all, certainly can play a big part in this initiative. It's an exciting and dynamic time for people working in healthcare IT because of the opportunities and challenges that lie ahead. Since most people who work in IT are natural problem-solvers, the current environment presents opportunities to be creative and innovative in the use of healthcare IT. Due to this dynamic atmosphere, BC/DR planning in a healthcare environment presents specific challenges, which we'll discuss in this chapter.

Healthcare technology is not just centered around servers and storage in the data center, however. The integration of medical equipment data into the medical record is increasingly seen as both desirable and necessary to deliver high-quality, integrated care. If you get a CT scan or an MRI, it's really useful to have a note about the results of that scan in your EMR, but it's even better to have immediate access to that image and the notes in almost real time. That way, your PCP at your next office visit or your hospital physician during an emergency room visit can view those images, see those test results, and have more information at their fingertips in mere seconds than would be possible even 5 years ago. While a discussion of how healthcare is evolving across the continuum of care is outside the scope of this book, it's important to understand how healthcare is evolving because it both drives and is driven by changes in technology, which ultimately inform and impact your BC/DR plan.

Governmental incentives and penalties

We won't go into detail in this chapter on governmental incentives and penalties, but we will touch on it here because it influences what happens in your healthcare IT organization. The most influential piece of legislation to impact healthcare in the past 30 years was the HITECH Act passed in 2009. The Health Information Technology for Economic and Clinical Health Act, or HITECH, was enacted under Title XIII of the American Recovery and Reinvestment Act of 2009 ([U.S. Department of Health and Human Services, 2009](#)). Under this Act, the U.S. Department of Health and Human Services is spending about \$25 billion to promote the adoption of health information technology (HIT), including EMRs or Electronic Health Records (EHRs). The Act also included provisions for federal spending of over \$35 billion on creating a nationwide network of EHRs.

The intent of this spending was not only to provide financial incentives to adopt an EMR but to eventually enable the use of electronic data toward overall population management. With the ability to store and manage more and more data (these days, referred to as "big data"), healthcare organizations should also be able to analyze those data and find ways to positively impact the overall health of the community. While this is one of the tenets of the HITECH Act, the reality is still forming. Many organizations are beginning to use their EMRs in meaningful ways—in other words, actually using the technology and the data to improve clinical outcomes.

Title IV of the HITECH Act provides incentive payments for physicians, hospitals, and other providers (who provide care to Medicare recipients) who adopt EMRs before 2015. However, in 2015, those incentives become penalties for not adopting an EMR (1% in 2015, 3% by 2018). The ultimate goal is meaningful use of these systems, and HIEs (see next section) will play an increasingly important role as data become available across the continuum of care.

Meaningful Use has numerous stages of participation, and organizations wanting to participate in incentive programs must demonstrate they are using their EMR in ways that contribute to better clinical outcomes. The government has defined a universe of metrics and/or capabilities that organizations must select from to demonstrate this capability. The intent is to provide economic incentives for the effective implementation and ongoing use of EMRs to ultimately improve clinical outcomes and reduce costs.

Let's look at a specific example. Suppose a patient, Julian, goes to his PCP. The PCP orders blood work and in a subsequent visit, prescribes a medication for him. He goes to the pharmacy and fills the prescription and begins taking the medication. A few weeks later, he feels horrible and ends up in the ED of a local hospital. Without an integrated EMR or HIE, the triage nurse in the ED admitting area has no idea that he just had blood work done 3 weeks ago, doesn't know what prescriptions he is taking (other than what he might accurately or inaccurately report), and doesn't have the PCP's diagnosis or notes. The ED physician is likely to order the same set of blood work (depending on presenting symptoms) and provide a medication to him that potentially causes side effects due to medication for another condition the ED staff don't know about because he didn't feel great and forgot to mention it. The cost of time and rework (blood work, labs, other tests) impacts not only his health but the cost of his care. When the EMR and HIE are in place (we are describing a future state), the triage nurse can see that he was at his PCP 3 weeks ago complaining of the same symptoms he's presenting with today. The triage nurse can see the tests that were ordered and their results along with the prescription prescribed and the current list of medications. The nurse can now ask him about each of the medications to ensure the list is complete and accurate. The nurse also sees other data such as additional conditions, test results, and notes that inform the current assessment. The ED physician can also see those test results and the current list of medications. Rather than ordering more tests and prescribing more medications, the physician can use the existing data as a starting point. This potentially helps the physician make a diagnosis sooner, but it certainly reduces the need for duplicate lab work and tests. This reduces both the cost and the turnaround time, enabling faster, more effective care. At least, that's how it's supposed to work in theory.

In the United States, we still have a way to go before this desired future state is a reality. In the interim, though, more electronic data do translate into faster access to key information, even if that means that the vitals the nurse took in the ED triage area are now available to the physician when the patient is examined.

Those are the basics behind the HITECH Act and Meaningful Use—there's a lot more detail and it's a rather complex topic. If you're interested in learning more, you

can start off on the U.S. government's Health and Human Services Web site and take it from there [Source: www.healthit.gov or the more specific www.healthit.gov/policy-researchers-implementers/health-it-rules-regulations] (HealthIT.gov., 2013a,b).

HIEs and Accountable Care Organizations

Health Information Exchanges (HIE) are a more recent development within healthcare IT. HIEs share patient (or member, where insurance companies are involved) clinical and financial information among participating organizations. Some HIEs are formed by a coalition of healthcare organizations to facilitate this exchange of data. These are often referred to as Regional Health Information Exchanges or RHIOs. HIEs are usually geographically defined and may link numerous healthcare organizations in a region. HIEs also exist on smaller scales such as the sharing of lab or test results among hospitals and local physician practices.

Health information exchanges

The overarching challenge for HIEs is described well in an Information Technology Laboratory (ITL) Bulletin published by the Computer Security Division of ITL, a part of the U.S. Department of Commerce's National Institute of Standards and Technology (NIST):

Improved, more effective healthcare is a high priority in the United States today. While the U.S. healthcare system is widely recognized as one of the most clinically advanced in the world, costs continue to rise, and often preventable medical errors occur. Government and private sectors are collaborating to improve the healthcare infrastructure and to facilitate the secure exchange of electronic health information through electronic health records (EHRs). These efforts are expected to lead to better patient care, fewer medical errors, and reduced costs of healthcare in the United States.

Health information technology (HIT), especially the development of electronic health records for use in both inpatient and ambulatory care settings, has the potential for providing reliable access to health information. Currently, health information is scattered among healthcare providers and payers. Patients have limited control over the collection, access, use, and disclosure of their health information.

The goal of storing, moving, and sharing health information in electronic formats raises new challenges for ensuring that the data is adequately protected. Better management of electronic health information will depend upon its secure exchange between consumers, providers, and other healthcare organizations in ways that safeguard the confidentiality, integrity, and availability of the information.

The sharing of healthcare information can take place in many ways, including through health information exchanges (HIEs). HIEs can involve exchanges between two organizations in a community, or between several organizations in a region, in several regions, or nationwide. Exchanging organizations need

a structured approach to security, which will enable their information systems to protect health information before, during, and after the exchange. All aspects of data usage, including collection, storage, modification, and destruction, will require security and privacy protection (Radack, 2010).

If you manage the IT department for a healthcare organization that participates in an HIE or RHIO, what are your BC/DR obligations? To answer that question, you'll need to look closely at the legal documentation describing your organization's participation commitments. Since an HIE is a technology arrangement, there typically are requirements on the part of providers (whoever is hosting the data) and participants (consumers and source of the data) as to service levels, information security, connectivity, and more. As a result, your first step in your BC/DR discovery around HIEs or RHIOs is to understand your legal obligations. This includes the information exchange requirements as well as requirements around HIPAA (CIA).

For example, if your EMR system goes down and you are unable to provide information to the HIE, do you have a method of retrieving information from that HIE? If so, how do the data sync up? Are your data fully available via the HIE (which may be an acceptable short-term DR solution), or are just a fraction of your data available and, as such, it would not be an acceptable solution of any kind? Most HIEs share some, but not all, data. Is it enough to provide care while your DR alternatives come online? That's worth looking at, but in today's environment, that's not likely to be the solution. HIEs are relatively new and are still evolving dynamically. For an IT department, the nature of that change drives uncertainty as to availability (more than anything), and understanding what your HIE/RHIO data are and are not is vital to your assessment.

Accountable Care Organizations

According to the U.S. government's Center for Medicare and Medicaid Services (CMS),

Accountable care organizations (ACOs) are groups of doctors, hospitals, and other health care providers, who come together voluntarily to give coordinated high-quality care to the Medicare patients they serve. Coordinated care helps ensure that patients, especially the chronically ill, get the right care at the right time, with the goal of avoiding unnecessary duplication of services and preventing medical errors. When an ACO succeeds in both delivering high-quality care and spending health care dollars more wisely, it will share in the savings it achieves for the Medicare program (Centers for Medicare and Medicaid Services, 2013a,b).

To make things just a bit more interconnected, ACOs often initiate, create, or participate in HIEs and RHIOs. We'll leave it at that for now—if you're interested in learning more, you can begin with the CMS Web site (<http://www.cms.gov/Medicare/Medicare-Fee-for-Service-Payment/ACO/index.html>) (Centers for Medicare and Medicaid Services, 2013a,b).

The key question for healthcare IT, again, is how does this impact BC/DR planning? By definition, an ACO is a group of participating entities. Anyone who has worked in healthcare IT knows that the list of providers potentially included in an ACO runs the gamut from a sole physician provider practice to a hospital. As such, the technological capabilities also span a wide range from paper to all electronic.

If your healthcare organization participates in an ACO, the legal paperwork is a good starting point for understanding your role and responsibilities. Even if your organization's legal representative does not wish to provide you a copy of the document, you can discuss the contents of the document to understand the impact on your healthcare IT BC/DR obligations.

Typically, each entity is responsible for its own data. So, whether you're in a small ambulatory physician practice IT team or a multihospital IT shop, you must ensure that patient data are available in a timely (and accurate) manner.

Integration of healthcare IT and medical equipment

If you work in a healthcare IT organization today, you have probably already been involved in the integration of your IT systems with medical equipment in some manner. Medical equipment is typically managed through a clinical engineering department (though it varies, a physician office may contract for that service from a local vendor). Medical equipment is defined as equipment used in the diagnosis, monitoring, or treatment of medical conditions. Medical equipment is used directly on or with a patient. This can include diagnostic, therapeutic, monitoring, life support equipment and medical laboratory equipment.

Diagnostic equipment includes diagnostic imaging such as X-ray, CT, MRI, PET scans, ultrasound, and more. Diagnostic imaging typically generates images that are stored in systems that share data with EMRs. Systems can include picture archiving and communication systems (PACSs), radiology information systems (RIS), and cardiovascular imaging systems (CVIS), all of which are designed to help healthcare organizations manage the massive amount of specialized imaging data that come from medical imaging departments. These images are often referenced in the medical record via a link to an external storage system (PACS or other). This is vital to understand when planning your BC/DR initiative. Where are these images stored, how are they linked to the medical record, and how will they be recovered and sync'd up if a disaster occurs?

Therapeutic equipment includes devices like infusion pumps that control the flow of therapeutic medications to a patient via a specialized medical pump. Other types of therapeutic device are ventilators (see “life support equipment”), respiratory therapy devices (nebulizers, for example), and neonatal warming devices. There is a wide range of therapeutic medical devices; these are all used to support patients in a variety of ways.

As you can surmise, *monitoring* equipment is any equipment that monitors the status of some patient function whether that's heartbeat, oxygen saturation, pulse rate, or blood pressure, to name just a few. Monitors can measure vital signs as well

as other types of data including electrocardiograms (ECG, sometimes referred to as an EKG, the K coming from the Greek *kardia*, meaning heart) and electroencephalography (EEG), which measure and monitor heart and brain functions, respectively.

Life support equipment includes any equipment that supports and sustains the life of a patient. This can be equipment like medical ventilators, which help a patient breathe. It can also include devices used in surgery such as heart-lung machines and anesthesia machines. These devices are critical to supporting the life of the patient in a variety of situations.

Finally, *medical laboratory* equipment includes equipment used in medical labs to automate the testing and/or analysis of blood, other bodily fluids, or genes. This equipment is used for diagnostic purposes and often is managed by laboratory information systems (LIS).

The reason it's important to understand the general categories of medical equipment for a healthcare IT professional is because the integration of medical equipment and information systems is accelerating every year. Whether your EMR is pulling in lab results (LIS), pharmacy orders (PIS), imaging results (PACS, RIS, CVIS, etc.), or monitoring data for a patient, it's all converging in your data center (or will be soon).

These disparate systems can be challenging to manage, especially from an IT perspective. More importantly, however, is the need to ensure these data handled in a manner that ensures their CIA. These are the requirements for HIPAA and HITECH (discussed in the Regulatory Environment section). As these technologies continue to converge, the onus of ensuring these data are secure (CIA) will fall to IT professionals. If you have not yet included medical equipment in your BC/DR planning, you should give it some thought. Whether the medical equipment department rolls up through your Facilities department (as part of environment of care) or through your IT department, you will ultimately have to work to ensure the data collected by these various systems are safe, secure, and available after a disruption or disaster.

Consumer-driven healthcare

You might ask what consumer-driven healthcare is and, more importantly, how it impacts your BC/DR plan. One of the requirements of the HITECH Act (see next section) is that patients have the ability to interact with their medical record in some manner. For example, many physician offices today have a secure patient portal that allows their subscribed patients to log on, check or make an appointment, and check their prescription list or test results. Some physicians use this as an interactive communication tool with patients, allowing basic questions and answers to cross this forum. For example, if a patient is prescribed a medication and wonders if he/she should take it in the morning or the evening (or if it matters what time of day), the physician may choose to communicate via this secure forum with the patient to quickly answer these kinds of questions.

Other types of consumer-driven healthcare trends include use of smartphone applications to track wellness (exercise, weight, etc.); secure portals to create a personal health record (which may or may not interface with an EMR) to track personal data such as blood pressure, medications, exercise, weight, lab or test results, health history, and more. Many payers (health insurance companies) are offering these kinds of wellness or personal healthcare sites to subscribers as both a value-added service and a way to help continue to improve health while reducing cost. Naysayers are concerned about medical privacy and the use of these data by insurance companies, but taken at face value, these portals can be valuable sources of trustworthy health, wellness, and medical information along with a secure place to record and manage your personal health data.

Coming back to your BC/DR plan, you'll need to understand what personal health data you may be storing and what the expectations are for access and availability. If a portal is hosted on a Web site and it's hacked, that's both an information security event and a business disruption. You'll have to shut down the portal, determine the impact to the organization, the data, and the patients, and have a plan for remediation. If your data center goes offline due to a fire or more catastrophic event, what is the expectation (and/or legal, contractual, or organizational requirement) regarding the availability of these data? Add this to your BC/DR list if your organization interacts with these types of data.

Real-time data

One of the key characteristics of this healthcare IT environment is the rise in the demand for and use of real-time data. Clinical staff record data in EMRs and they are instantly available. This means that real-time data can be used in the diagnosis, monitoring, and treatment of patients. This enables the anesthesiologist to have vital sign data automatically entered into the EMR via an interface from the patient monitoring device. Those data can be instantly available to the surgeon in the OR on a large monitor overhead or to the nurse assisting with the case. The data are error free because they were captured from the device and not entered manually. They are available to anyone who needs them at that moment and available later for review. The surgeon can look at prior images, whether X-ray, CAT, PET, MRI, or ultrasound, as reference before or during a surgery. A radiologist can read an image remotely to assist in diagnosis. A pathologist can view an incision site remotely to collaborate with a surgeon in real time.

The rise of the use of real-time data is enabling faster, more collaborative work and often better clinical outcomes as a result. However, this puts an additional layer of complexity on the healthcare IT organization. Managing real-time interfaces such as HL7 or X12 (medical data or healthcare administrative functions such as claims management, respectively) requires constant monitoring of the status of these interfaces and plans for managing them in the face of a business disruption.

The most notable impact of this is how the IT organization architects the BC/DR solution. With so many upstream and downstream applications and interfaces, it can be daunting to determine the best solution for BC/DR. In less complex environments, systems are backed up, servers are established at remote locations (cold, warm, or hot sites), and data can be restored to an alternate location, synced up, and the organization is off and running (granted, that's a very simplified version, but that is the workflow for many IT shops). In healthcare IT, not only must the medical data be highly available, the flow of data in and out of other systems is often real time. How do these systems get managed in a downtime event? Is there local redundancy? Do those data get stored and synced up later? Do those data get entered manually? Is there a local system that functions as a “store and forward” device that would drop into local mode if the server went offline? The answers are sometimes straightforward, sometimes complex; but healthcare IT departments must ask and answer these types of questions to develop a useful BC/DR plan.

Summary

If you work in healthcare IT, you have probably given some thought to many of these topics and answered many of these questions. If you’re in an IT leadership or management position, you might be losing sleep over this topic. Many healthcare organizations are just beginning to implement these new technologies and none does so straight across the board. One organization will integrate PACS while another might focus on interfacing patient monitoring data first. You may be facing various clinical leaders championing integration with their systems (CVIS, LIS, PIS, RIS) simultaneously leaving you to wonder how to pull it all together into a coherent roadmap to your future state. As a healthcare IT professional, you’re going to have to address these and many related questions when you develop your BC/DR plan, regardless of where your healthcare organization is on the continuum of EMR adoption, medical device integration, or HIE. As we proceed through this industry spotlight, we’ll continue to point out potential challenges and offer suggestions for how to pull all of this together. If you work outside of healthcare IT, there are many parallels you can draw to other complex IT environments.

There is no one-size-fits-all approach to developing a solid BC/DR plan for your healthcare IT organization. However, by reviewing the data in this chapter, you will be spurred to ask more questions of a wider audience, challenge assumptions, and generate checklists to ensure you’ve at least considered areas for BC/DR planning, even if you eventually deem them out of scope. As we’ve discussed in [Chapter 5](#), your risk assessment includes looking at whether you want to address a risk or not. If you choose to address it, you may choose any number of mitigation strategies, which are discussed in [Chapter 6](#). As you embark on these aspects of planning, if you have a list of items to include from this chapter, you’ll be far more prepared than many of your counterparts. The data here are not intended to be exhaustive or authoritative; instead, they are intended to be thought-provoking and eye-opening. Be curious, ask questions, and look around.

REGULATORY ENVIRONMENT

According to a November 2010 white paper on Health Information Security,

Health information technology (HIT), especially the development of electronic health records for use in both inpatient and ambulatory care settings, has the potential for providing reliable access to health information. Currently, health information is scattered among healthcare providers and payers. Patients have limited control over the collection, access, use, and disclosure of their health information (Radack, 2010).

This new environment requires oversight to ensure providers across the healthcare spectrum guarantee the CIA of patient data. The goal of storing, moving, and sharing health information in electronic formats raises new challenges for ensuring that the data are adequately protected. Better management of electronic health information will depend upon its secure exchange between consumers, providers, and other healthcare organizations in ways that safeguard the CIA of the information.

Throughout this healthcare IT chapter, we'll keep bringing current information about healthcare IT back to BC/DR. Some information about the current state is context for healthcare IT work; some directly impacts it. One key example is the regulatory environment. Healthcare companies of all shapes and sizes are regulated in one form or another. The purpose of this section is not to give you specific information on regulations in these subject areas that you can use to attain or retain certification or compliance. Rather, it is to discuss the types of requirements you need to include in your BC/DR plan. Chapter 2 also reviews the broader legal and regulatory environment and you should review that chapter as well.

Centers for Medicare and Medicaid Services/Joint Commission on Accreditation of Healthcare Organizations

As you can surmise, the healthcare field is highly regulated, primarily due to the risk to human life. As such, there are many regulations defining how healthcare organizations must manage their business. In this field, organizations that received government funding must be accredited by an accrediting organization. The Centers for Medicare and Medicaid Services (CMS) is the governmental entity which oversees these two federally funded programs (Medicare and Medicaid). Any healthcare organization which bills for services to patients on Medicare or Medicaid must be accredited to receive reimbursement. One accrediting body is the Joint Commission on Accreditation of Healthcare Organizations (JCAHO, pronounced JAY-co). JCAHO is an independent, not-for-profit organization that accredits and certifies more than 20,000 healthcare organizations and programs in the United States. JCAHO is one of several accrediting bodies in the United States. If you want to learn more about CMS or JCAHO, you can find out more on their Web sites (www.cms.gov and www.jointcommission.org/).

Accreditation from CMS through any of the accrediting bodies is intended to ensure patient safety through defining, measuring, and monitoring the entire environment of care. Medical devices come under the auspices of CMS. Healthcare IT is not directly regulated by CMS. Patient safety elements of the EMR, such as medication administration, medication reconciliation, allergy alerts, clinical best practices, etc., may be reviewed as part of the overall environment of care to ensure patient safety. With the continued deployment and reliance on electronic medical systems in the delivery of healthcare, IT systems may be included in regulatory requirements in the future. For now, healthcare IT is primarily impacted by HIPAA regulations with respect to the CIA of personal health information.

U.S. Food and Drug Administration

Medical devices that are used to treat patients are regulated by the Food and Drug Administration (FDA). A vendor's product, whether it's an intravascular ultrasound machine or a patient cardiac monitoring device, must go through rigorous testing. It's vital that the machine be highly reliable, accurate, and safe. As devices become more sophisticated and leverage the latest computer technology, they also become more vulnerable to modern computer threat sources. In many instances, FDA-regulated medical device vendors are not actually leveraging the latest computer technology; they are leveraging technology that was modern about a decade ago. Why? Every time they need to make any change to the device, they must go through a rigorous (sometimes onerous) FDA approval process. That takes time and money. So, vendors are reluctant to make changes that require FDA approval until they are ready for a major new release.

Contrast that with how computer technology evolves. A vendor, say a PC hardware manufacturer, sees a trend toward touchscreen monitors or dual processors in a PC, etc. That manufacturer can spend as much time and money in research and development as they want, produce a new product, and put it in the marketplace. They are constrained by how quickly they can design, manufacture, and produce units for sale. Thus, we see the trend to ever-increasing release cycles, pushing consumers to buy the latest innovation.

Medical equipment vendors, on the other hand, look at the current state of technology when they are developing a new product and decide what to leverage. Once their design team is finished, it goes through numerous vetting cycles; once the product is ready to be sold, it must meet final FDA approval. This entire process, from end to end, can take years. So, what was new (but well established enough to be considered reliable) in computer technology when the medical device was being designed is no longer new. In fact, it may be verging on obsolete by the time it is released for sale. Keep in mind that the FDA approval extends across the technical solution—meaning that the approval for a solution includes not only the end device (used on the patient) but also the interconnections and possibly the server software, server hardware, or server appliance, as the case may be.

Many medical equipment vendors are, even today, running a cobbled-together version of an embedded Windows mobile OS.

TIP**Windows Embedded vs. Windows CE vs. Windows Mobile**

Windows Embedded CE (otherwise known as Windows CE) is a small footprint modular operating system. It contains many different components that developers put together and embed into their overall device design to meet their specific needs.

Windows Mobile, on the other hand, is based on Windows CE and is a mobile device operating system released by Microsoft. Windows Mobile contains selected elements of Windows CE along with some additional capabilities. In essence, Windows Mobile is a proprietary cobbled-together collection of Windows Embedded CE components chosen by Microsoft internally to meet its own development needs.

The challenge with IT shops dealing with medical devices based on Windows Embedded CE is that once it's developed, it's pretty much locked and loaded. Any vulnerabilities discovered for any components of the Windows CE operating system are pretty much locked into the device into which Windows CE is embedded. From an information security standpoint, this is concerning as medical devices make their way onto the network. From a BC/DR standpoint, there is likely little impact other than to understand that if there is a disaster event and you need to repurchase new devices that use embedded or mobile Windows versions, they're likely to contain different sets of components (and therefore capabilities) than earlier versions. For example, handheld devices used to scan and track inventory might not work with the installed software you have if the software or the handhelds are replaced independent of one another. In other words, if the server on which that scanning software resides is demolished and you have to replace it, you might be fine (most applications have some backward compatibility). If you have to replace all the handhelds because they were all in a charging station in a room that caught on fire, you may have issues with new handhelds having the same features and working with the older software. This is one more thing to consider if your organization relies on devices using the Windows CE technology. You might be surprised to read about Windows CE, but this is widely deployed in healthcare, despite advances to mobile operating systems in recent years.

You are probably already beginning to piece together how FDA-approved devices may or may not impact your BC/DR plan. Here's a scenario to consider. You have a patient monitoring system that includes end user devices (attached to patients), which transmit their data through a medical device interface into a server in the data center. Those data are formatted and managed by that server and then sent through another interface into the EMR. The patient device and the server to which it attaches are FDA regulated. This entire system costs over \$5 M over a 5-year period and, except for periodic updates, the system is as it was when purchased starting 8 years ago. The vendor hardware architecture is not sophisticated enough to include virtualization, redundancy, or any high availability options. You can back up the software, but that's about all you can do to manage the system.

A fire in the data center is discovered and extinguished before it impacted the entire data center. Unfortunately, the quadrant in which the fire started involved those database servers. You contact the vendor, who politely tells you that you

can purchase new servers, but they come with updated software, you cannot use your old software on new hardware and, oh, by the way, the new server software does not work with the revision of software on the patient devices.

From a DR standpoint, you have a real problem. The server hardware is provided by the vendor, preloaded with the software. They will not sell you a previous version. You can't afford to purchase a second server and keep it up-to-date with each update (support costs for medical equipment are exceptionally more expensive than standard server hardware or software maintenance costs). So, how do you incorporate this into your BC/DR plan?

There's no easy answer. You could choose to create a disaster plan whereby you purchase the upgraded server and software and some number of newer end user devices, knowing that it will barely meet clinical needs, but might suffice the most critical areas (post-op, ICU, etc.). Your plan might be that all devices are moved into local mode, and clinical staff will have to enter data manually (which will require extra staff and which will cost in terms of labor, productivity, and potential errors) until a new system can be purchased that addresses new and existing devices, revision levels, and software. That's likely to cost millions of dollars—will your insurance cover that? Will your organization be able to absorb that? How long will it take you to recover from that?

The take away is this: integrated medical devices that utilize any sort of back-end technology beyond end device (network connectivity, interfaces, servers, storage, databases, etc.) require a special review during your business impact analysis (BIA) and your BC/DR planning. Sometimes solutions are suboptimal, but having thought through what your options are and what steps you might take is important. Doing so in advance could save countless hours of “spin” in the aftermath of an event. Medical devices and their associated infrastructure should be reviewed and discussed as part of your BIA process. Recovery solutions should be discussed and documented and updated periodically as your medical device technology changes. And, going forward, you may be more engaged with your clinical leadership in the development of technical requirements for any new or replacement systems to ensure they can be more easily rolled into your BC/DR plans.

Health Insurance Portability and Accountability Act

If you work in healthcare IT, you are likely very familiar with the Health Insurance Portability and Accountability Act of 1996, commonly referred to as HIPAA, and its associated requirements. In this section, we'll talk about HIPAA as it relates to your BC/DR plan. A thorough discussion of HIPAA requirements is beyond the scope of this book. In addition, a discussion of specific actions you'll need to take to remain HIPAA compliant through your BC/DR planning is outside the scope of this book as well. However, we will list the major elements and discuss frameworks for ensuring compliance as you develop, implement, and manage your BC/DR plan.

TIP**HIPAA Compliance and Your Organization**

As a reminder, nothing in this book is intended to be a substitute for your own independent legal review and counsel. You and your organization must take action to ensure you understand all regulatory requirements pertaining to your organization and that you develop BC/DR plans that are compliant with those requirements. The information in this section will point you in the right direction, but the expectation is that you'll do independent research and pull in your own risk management and legal experts to review your plans.

The basic tenant of HIPAA is that health information be private and secure. There are two rules that relate to this area—the Privacy Rule and the Security Rule. The Privacy Rule created national standards to protect the *privacy* of individuals' protected health information (PHI). The Security Rule establishes national standards for electronically *securing* PHI. With the rapid adoption of EMRs, patient privacy and information security are of utmost importance. Privacy and security are also impacted by disaster events; therefore, there are requirements related to creating a BC plan that provides for the CIA of personal health information.

The Security Rule is divided into three categories: Administrative Safeguards, Physical Safeguards, and Technical Safeguards. According to CMS HIPAA Security Series:

- *Administrative Safeguards:* In general, these are the administrative functions that should be implemented to meet the security standards. These include assignment or delegation of security responsibility to an individual and security training requirements. (For more information, see 45 CFR §164.308 and paper 2 of this series titled “Security Standards—Administrative Safeguards.”) ([U.S. Department of Health and Human Services, 2013](#))
- *Physical Safeguards:* In general, these are the mechanisms required to protect electronic systems, equipment, and the data they hold, from threats, environmental hazards, and unauthorized intrusion. They include restricting access to EPHI and retaining off-site computer backups. (For more information, see 45 CFR §164.310 and paper 3 “Security Standards—Physical Safeguards.”)
- *Technical Safeguards:* In general, these are primarily the automated processes used to protect data and control access to data. They include using authentication controls to verify that the person signing onto a computer is authorized to access that EPHI, or encrypting and decrypting data as they are being stored and/or transmitted. (For more information, see 45 CFR §164.312 and paper 4 “Security Standards—Technical Safeguards.”) ([U.S. Department of Health and Human Services, 2007](#))

As you can see, the HIPAA Security Rule requires you to safeguard data, including off-site backups. While HIPAA does not require the use of specific technologies, it does require that you protect electronic data from threats, environmental hazards, and unauthorized intrusion. These are all address in a BC/DR plan. Conducting a

BIA, conducting a risk assessment, and maintaining a current BC/DR plan all come under HIPAA Security Rule requirements.

REAL WORLD

The Reality of Information Security in Healthcare Today

A recent headline read “Patient data revealed in medical device hack.” The article went on to describe how hackers had found a way to exploit critical vulnerabilities in a popular medical management platform. That’s technical language for hacking a system that runs medical devices. That’s one growing reality in today’s integrated world.

According to HealthITNews.com, the top five largest healthcare data breaches in 2012 were, in order:

1. Utah Department of Health—780,000 records
2. Emory Healthcare—315,000 records
3. S.C. Department of Health and Human Services—228,435 records
4. Alere Home Monitoring, Inc.—116,506 records
5. Memorial Healthcare System, FL—102,153 records

And it’s not just the number of records compromised, it’s the number of organizations and the times there are multiple incidents at the same organization, as well. For example, Stanford University Hospital & Clinics had to notify 20,000 patients in 2010 that their PHI had been posted to a student Web site. That same year, Lucile Packard Children’s Hospital (part of the Stanford system), reported a breach involving more than 500 patients. Just 2 years later, Stanford University Medical Center notified another 2,500 patients of an HIPAA breach.

The point is not to call out any one healthcare organization; the point is to drive home the challenge of protecting electronic data and to understand that these breaches are business disruptions. These breaches may also be caused by hackers or malicious software, which can not only expose protected health information but also cause an organization to have to perform some sort of event recovery.

We often think of a disaster or a disruptive event as a fire or flood, but it’s becoming increasingly clear that disasters from a malicious attack or inadvertent breach must also be considered in BC/DR planning ([Healthcare IT News, 2012, 2013](#)).

Health Information Technology for Economic and Clinical Health

As discussed earlier, the HITECH Act is focused more on securely implementing EMRs and using those records in a meaningful way (Meaningful Use) to have a positive impact on clinical outcomes. There are numerous aspects to HITECH, but they are focused on using EMRs and the financial rewards (and penalties) related to that.

According to CMS, HITECH is described this way:

On February 17, 2009, President Obama signed the Health Information Technology for Economic and Clinical Health (HITECH) Act, as part of the American Recovery and Reinvestment Act (ARRA). Administered by the Office of the National Coordinator (ONC), the Act contains specific incentives designed to accelerate the adoption of health information technology (HIT) by the health care industry, health care providers, consumers, and patients. Its goal is to enable improvements in health care quality, increase affordability, and improve health care outcomes for all Americans ([HealthIT.gov., 2013a,b](#)).

As you can see, the focus is on using EMRs, not on the privacy, security, and availability of patient data, as is the case with HIPAA. If you're managing a healthcare IT shop, what you need to know about HITECH comes in the form of increasing demands for reporting, interfaces, and application modification to meet Meaningful Use requirements. If you oversee the applications side of the house, HITECH has probably already had a significant impact on the work you do. If you're on the infrastructure side, you may have seen increase requests for reports, databases, extracts, testing regions, interfaces, and perhaps storage.

From a BC/DR perspective, your key takeaways are that whatever you put in place for Meaningful Use (whatever stage you may be attesting to), you must make available for auditors. In other words, if you implement a feature, begin using it, and collecting data, and then have a business disruption, you must still be able to demonstrate the ability to use these features once you've recovered your systems. Therefore, you must ensure all systems are backed up and dependencies, both upstream and down, are accounted for in your BC/DR planning. If recovering System A before System B causes the data to be out of sync, you need to specify that you must recover System B first. These are the kinds of details your application teams or your cross-functional project teams can attend to, but it's helpful when you understand the overall environment so you can ensure these elements are included in your risk analysis, BIA and eventual BC/DR plan.

Payment Card Industry

Organizations that accept credit card payments must be compliant with the Payment Card Industry Digital Security Standards (PCI DSS). PCI DSS is a set of requirements developed to ensure the adoption of consistent data security methods. Almost all healthcare organizations accept credit card payments, whether for co-pays or payment in full for services render. As such, those organizations must be PCI compliant. While a discussion of PCI compliance is outside the scope of this book, it is important to understand how PCI compliance dovetails into your BC plans. For example, if you have point-of-sale (POS) systems throughout your facility (gift shop, cafeteria, cafes, vending machines, flower shops, etc.) which accept credit card payments, those data must remain safe. If there is a downtime of these POS systems, is it an IT responsibility to address these systems? How much of a disruption will it be to the organization and what risks are there with manual credit card processing methods?

According to AuthorizeNet, there are 12 requirements to PCI compliance, as outlined below. As you can see, these are elements you are already addressing in HIPAA as well as in information security best practices. However, information security, HIPAA compliance, and PCI compliance are not redundant. There are unique aspects to PCI compliance worth investigating.

Build and maintain a secure network

1. Install and maintain a firewall configuration to protect cardholder data.
2. Do not use vendor-supplied defaults for system passwords or other security parameters.

Protect cardholder data

3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data across open public networks.

Maintain a vulnerability management program

5. Use and regularly update antivirus software.
6. Develop and maintain secure systems and applications.

Implement strong access control measures

7. Restrict access to cardholder data by business need-to-know.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder data.

Regularly monitor and test networks

10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.

Maintain an information security policy

12. Maintain a policy that addresses information security ([AuthorizeNet, 2013](#)).

These elements may be outside the scope of your direct responsibility, but many healthcare IT professionals focus on HIPAA and forget about PCI compliance, especially during a risk assessment or BIA. A chat with your Finance folks should help bridge the gap, but don't be surprised if your Finance folks are not up to speed on PCI. They look at sources of revenue and may not be looking at the technical aspects like payment gateways, authorizations, and PCI compliance. It will be your job to get smart about these items, discuss them with Finance, assign an operational owner, and then bring these data into your BC/DR plan, as appropriate.

State and local requirements

Regardless of whether you're in a small physician practice IT organization or a large, multistate hospital system's IT organization, you will need to be compliant with state and local regulations. It's unlikely there are state or local regulations related to BC/DR, but it never hurts to discuss this with our organization's legal counsel. Each state does have different laws regarding protected health information (PHI), especially around breach notification laws, but this is outside the scope of this book. Suffice it to say it's important to understand your state and local requirements to ensure you don't overlook a critical item.

HEALTHCARE IT RISK MANAGEMENT

The American Society for Healthcare Risk Management (ASHRM) looks at risks in healthcare, but their specific focus is not on healthcare IT. That said, there are

numerous areas of risk management that are important to understand, if even at a high level, to ensure your BC/DR plans are comprehensive. As we discuss each of these sections, you'll see how healthcare IT systems impact each of these areas. By extension, then, your BC/DR plans will impact each of these areas as well.

Patient safety

The sole purpose of any IT department is delivering service to the organization. In healthcare, the ultimate end user is a patient. While all healthcare organizations work toward health and healing, the number one objective is always patient safety. As we saw during various super storms over the past decade, patient safety when a hurricane is bearing down on a hospital is a dire situation. At times like those, all efforts are focused on ensuring every patient is safe.

How does healthcare IT have anything to do with patient safety? Without going into deep detail, one of the most often-cited examples is barcode medication administration. A patient wears a bar-coded wristband. Medications have bar codes. The nurse logs into the patient's medical record, scans the patient, scans the medication, and administers the medication. With this relatively simple workflow, the nurse has verified the patient getting the medication, verified the medication is the right medication ordered for that patient, and verifies that the right dose of the medication was administered at the right time. So, the right medication for the right patient at the right time using current technology. While it's not 100% error proof, it has reduced medication administration errors exponentially in most organizations where it's been implemented. Keep in mind that medication errors can be relatively benign—administering a dose after a meal instead of on an empty stomach or administering a dose after an order had been stopped—or an error can be life-threatening such as giving a drug that the patient is allergic to.

The next question is then how does BC/DR have anything at all to do with this? How is medication dispensed when your EMR is down or your network storage is down? How does that impact patient safety if your downtime is an hour, a day, or 4 days? Clearly, your EMR will be defined as a Tier 1 application, most likely *the* most important application you have. You've likely virtualized your servers and your storage to assure high availability, high redundancy, and low probability of downtime. Still, things happen. Common components fail, staff enter in the wrong command, software has a critical bug—it happens to the best IT shops in the world.

Understanding the nature of patient safety and the interaction with IT systems in your facility is critical to both understanding the problem and helping devise downtime alternatives. For example, if the EMR is down but you have key patient data stored locally in an encrypted file on a PC in each clinical unit, you may be able to get by with a few hours of downtime without a patient safety issue. But what if that PC can only be logged onto using cached credentials (say you have a partial network outage)? What if the people on duty have not logged into that PC and the credentials are not cached? How else can those data be provided to clinical staff? During your BIA, you'll need to help clinical leadership understand what it means

to have no network or no storage or no servers or no application. They don't understand the differences between these technologies; they understand their clinical work. Understanding how the technologies you manage impact patient safety is the most important task you can undertake in your healthcare BC/DR planning.

Patient care

Patient care goes beyond basic patient safety and encompasses every workflow associated with every clinical task your organization performs. From radiology to surgery, nuclear medicine to pain management, vascular interventions to orthopedic rehab, neonatal intensive care to hospice, primary care to lab work, your organization cares for patients in a variety of settings using a myriad of technologies.

Clearly, risk to patient care related to BC/DR is a large topic, one we've been discussing throughout this chapter. The primary risk to any healthcare organization is around patient care (patient safety being of the most important facet of patient care). The key deliverable for IT organizations is how that technology assists in, contributes to, or facilitates patient care. Understanding each application, each server and its backend storage, each interface, and how they all interact to enable patient care is imperative for anyone in healthcare IT.

Your BC/DR plan needs to account for patient care to the extent that IT systems intersect with patients and their care givers. You are not expected to deliver systems that never go down or won't ever be offline due to a major business disruption. You are, however, expected to do the lion's share of the work in helping the organization understand what the impact would be if those systems went down and what workarounds, alternatives, and solutions you have to recover quickly and effectively.

Organizational solvency

Appropriately, we've focused on patient safety and patient care as primary risks related to IT system downtime. Second to patient safety and care is financial solvency. The facts about the number of businesses that fail after a disaster or business disruption are dramatic. The vast majority of businesses that don't have a BC plan in place fail after a major disaster or disruptive event. It's that simple. They fail primarily because they are unable to get their systems back up and running in a timely manner and whether they fail because they are unable to manufacture goods, deliver services, or bill and collect revenue, they fail financially.

A serious downtime for a healthcare organization's financial systems, such as their supply chain management (purchasing, receiving, inventory management, asset management, etc.) or their financial systems (payroll, accounts receivable, accounts payable, capital assets, etc.), can cause the organization to be unable to fulfill its basic functions. If supplies for surgeries are not on hand, cases are cancelled and likely rescheduled elsewhere if the problem persists. This has a ripple effect on the organization and solvency can quickly become questionable if a

lengthy downtime occurs. Addressing financial systems in your BC/DR plan is about more than money—it's about being able to care for patients in a safe and effective manner.

Facility management

Most healthcare organizations have integrated facilities management systems such as fire, alarm, or HVAC systems. Many of them are now running on virtualized servers in the data center. Whereas before, when systems failed it was a facilities' problem, it's now also an IT problem. If an electrical failure disrupts your data center, how are facilities management systems running? How are they impacted? How would the downtime of these systems, individually, impact patient care? If the fire alarm system is running on a server that fails, what happens? If it's virtualized, it may just fail over to another virtual server and continue on. However, many building automation systems are not quite as sophisticated as other IT systems. You may find that the system needs to run on a physical server; or worse, the vendor supplies the box and it doesn't support dual power supplies, has no redundancy, and is built on a legacy platform. These are all risks to your facilities management systems and to your facility. Ultimately, they're risks to your patients. Therefore, your BC/DR plan needs to look at the risk to facilities with respect to systems in the data center (and how they impact your data center itself) and ensure you have your bases covered.

TECHNICAL NEEDS—HEALTHCARE IT ARCHITECTURE

Healthcare IT storage is one of the fastest-growing areas of storage demand. In fact, according to a 2008 study by The Ponemon Institute, 30% of the world's storage was found in healthcare ([Ponemon Institute LLC, 2008](#)). In the intervening 5 years, that number may well have grown to exceed 40%. Naturally, storage vendors are clamoring to get a foothold into healthcare IT due to the estimates for ever-increasing storage demand. Storage, though, is not the only element of a robust healthcare IT architecture.

The protection of data is important in any business, but it's even more critical for HCOs with the massive amount of data being generated and stored in healthcare. Electronic data in healthcare include digital medical images, clinical documentation, and stored scans of paper documents such as consents or paper charts from other organizations. The move toward a HIMSS Stage 7 EMR implementation (see sidebar “Real World” for more information) has created an upsurge in demand for servers, storage, interfaces, applications, and end user technologies. In this section, we'll review some of the basics of healthcare IT to provide you an overview of systems and technologies you should be thinking about for your healthcare IT BC/DR plan. If you don't currently have these technologies in-house, you may well be in the analysis or planning stages of acquisition. These will need to be incorporated into your BC/DR plans as you review and refresh in the future.

REAL WORLD

HIMSS Analytics EMR Adoption

The Health Information and Management Systems Society, or HIMSS, is a nonprofit organization dedicated to providing global leadership “for the optimal use of information technology (IT) and management systems for the betterment of healthcare.” [Source: <http://www.himss.org/about>.] HIMSS Analytics is a wholly owned subsidiary dedicated to utilizing the data within healthcare information and management systems to improve the quality of care. HIMSS Analytics developed an EMR Adoption Model that tracks the progress of a healthcare organization toward a fully integrated EMR. There are eight stages, from zero through seven, with seven being defined as “Complete EMR; CCD transactions to share data; Data warehousing; Data continuity with ED, ambulatory, OP” (and a more comprehensive set of requirements located here: www.himssanalytics.org/home/; [HIMSS Analytics, 2013](#)).

Many healthcare organizations in the EMR adoption process have used the HIMSS Analytics framework as a method of defining adoption outcomes and tracking progress toward those goals. Many healthcare organizations worldwide have adopted some technology to facilitate patient care; fewer than 2% of healthcare organizations in the United States have achieved HIMSS Analytics Stage 7. As healthcare organizations continue to reach for incentive dollars available through 2015 (and later, avoid penalties), EMR adoption rates will climb. Integrating systems to achieve Stage 7 is a daunting, but achievable, task. Healthcare IT departments are both driving and being driven by these requirements.

Clinical systems

Clinical systems, by definition, directly or indirectly support patient care. Most notable among these is the EMR or EHR. The EMR contains patient demographic information such as name, address, age, as well as patient history, orders, test results, medications, medical history, admission, and discharge data. These data may be input directly by a nurse or they could be automatically entered through interface data from another system or a patient monitor, an anesthesia machine, or other medical device attached to the patient.

In addition, clinical systems often interface with one another in either a one-way or two-way information flow. For example, the EMR may send basic patient demographic data to the lab system, and the lab system may then send back associated lab results to the EMR. This is also true for radiology systems, pharmacy systems, and food services, among others.

There are often hundreds of applications in use throughout a healthcare organization. Some reside on servers in the data center; some reside on stand-alone PCs in clinical areas. Getting your arms around all clinical applications and systems can be a daunting task if a current list does not exist. It’s a great time to get a full inventory of systems in use while performing your BIA interviews. Often asking clinical leaders (or staff) to name the vendors they work with or the names of the programs they work with daily can be more enlightening than asking, “What systems do you use on a daily basis and are those data being backed up?” Clinical end users are notorious for overlooking systems—primarily because IT folks often ask questions from the wrong perspective. If you are unsure if you have key systems that are not accounted for, spend a few hours at the clinical location in question and watch them work. Make

note of the programs they’re firing up and using. You might be surprised to find there are many little applications living in the wild that are actually critical to the daily operations of that department.

TIP**Going to Gemba**

Borrowing from a Lean concept, *going to gemba* means going to the place where work happens. (*Gemba* is the westernized version of the Japanese word *genba*, which means “the real place.”). It’s got a specific definition and set of actions in the Lean world, but it’s a useful concept that pops up in different ways at different times. The concept “management by walking around” is also related to going to gemba—a manager walking around and seeing what’s going on is more likely to pick up on how the business is really running, far more enlightening than a status report. In the context of this chapter, going out to where your customers are and seeing how they use systems can be eye-opening. If you work on the infrastructure side of the IT shop, it’s often the case that you or your staff spend the vast majority of your time heads down with a couple of computer monitors in the back corner just outside the data center. If you really want to get smart about your healthcare organization, put an appointment on your calendar every week for 60 minutes and just walk around the facility. Talk to folks; watch them work. You’ll learn a lot and build valuable relationships that may help when it comes time to nail down DR plans.

Quality systems fall somewhere in the middle of clinical care systems (EMR) and business systems. For example, quality analysts need access to clinical data in order to analyze trends and track improvements based on discrete actions taken. These data are often organized into a data universe in order to provide a way for end users (in this case, quality analysts) to slice and dice data from a data warehouse. Is this a clinical or a business system? In the end, it doesn’t matter how you define it as long as you address it in your BC/DR plans. For example, Meaningful Use requires the ability to provide reports on a number of metrics. Where are those data stored? How are the reports generated? How long do they need to be archived? Can they be pulled and filed or do you need to have the ability to go back to some period in time and rerun those data if audited? These are the kinds of questions you’ll have your experts answer, so you need to be sure to have those experts at the table when you’re assessing the systems and data used in this arena.

Quality is just one example of departments in your healthcare organization that may rely on data from numerous clinical and business systems. While quality data may not be at the top of your list in the aftermath of a BC/DR event, they need to be on the list so that your organization can return to normal operations should a disruption occur.

Business systems

Business systems encompass administrative and financial systems—anything needed to run the business. Administrative systems are typically used by nonclinical staff to manage the business, the facility, and the resources needed to deliver care.

One major healthcare-related business system is enterprise scheduling. Patients need to be scheduled for surgeries, cardiac procedures (Cath Lab, for example), radiological exams, and inpatient and outpatient procedures. In ambulatory settings, patients need to be scheduled for physician appointments, lab tests, or other types of exams, procedures, or appointments.

In addition to scheduling, there are scores of applications related to managing the facility itself. From automated building controls to maintenance management to cleaning and asset tracking, healthcare organizations need to manage assets throughout the facility.

Supply chain management systems are another category of application used in healthcare settings. In most hospitals, OR supplies account for the vast majority of the supply budget, so purchasing and managing supplies is a critical business function.

From a BC/DR perspective, you need to understand what systems are upstream and downstream to your EMR. As important, you need to understand how your organization would manage supplies if a critical supply chain management system was down. Remember, purchasing is often needed in the aftermath of a disruptive event because lots of things need to be purchased. If that system were to be down due to the disruption, how would supplies be ordered, tracked, and managed? Is there a viable “downtime” process in place? Understanding the relative criticality of supplies for clinical and nonclinical needs in the event of a business disruption is second only to clinical concerns.

Financial systems are, of course, critical to the business. Being able to capture charges, bill, collect, and post payments, as well as monitor financial status and generate reports is an essential business function. Personnel management systems, payroll systems, benefits administration, recruiting, capital management, cash flow management, and many other financial systems are used to ensure the business runs efficiently. In the aftermath of an outage, these key systems will need to be brought back online quickly. How do they compare to the EMR and its up- and downstream systems? Most likely, the financial systems would be second to EMR efforts, though often healthcare organizations have different teams working in different areas, so systems may be able to come back online in a semi-parallel fashion rather than a serial fashion.

Understanding the types of systems in your organization will help you understand how large a task you have ahead of you with your healthcare IT BC/DR plan. It will also help make you more informed in general and help make you a better steward of your company’s resources.

Types of data

Like any other type of business, healthcare generates a lot of data. Where healthcare diverges from other types of businesses is in the fact that much of the data in healthcare impact patient care, whether directly or indirectly. As we’ve discussed, the different clinical and business systems generate data that need to be stored, backed up,

and recovered in the event of a disaster. Understanding the types of data you’re managing is critical to ensuring you have a solid plan for restoring them, if needed. While you may understand these fundamentals we’re going to discuss in this section, it’s worth mentioning these types of data. If you’re not familiar with these types of data, this will serve as a good starting point for further research.

Structured

Structured data are data that reside in defined fields, such as within a record or file in a database; examples include name or a street number when storing a unique address record. Spreadsheets may contain structured data because each element is contained in a cell. XML files are also structured data because each element is specifically tagged and can be easily identified. In healthcare, most structured data are located in databases such as MUMPS, Cache, Oracle, and SQL. Throughout lab, radiology, pharmacy, and clinical information systems (EMRs), structured data are typically the norm because they are easily searched, reports can be generated from extracts, and the defined data elements in different types of records can be cross-referenced.

Unstructured

Unstructured data are any data that are not associated with a discrete data field. In other words, unstructured data are data that do not reside in a spreadsheet file or in a database format. Examples of unstructured data include files that reside on a file share—often text or binary files like Word, PowerPoint, audio files, video files, image files, and more.

The problem with unstructured data is that they are hard to sort, manage, and organize. If you think of the files stored on servers or network storage, you know that there may be thousands of duplicate copies (or almost duplicate copies) of data in many different formats. It’s not uncommon for medium-to-large organizations to have terabytes of unstructured data that they need to manage, backup, and potentially recover. It’s both a problem for the IT department and a significant, if not always visible, cost to the organization in terms of resources (storage space, backup space, backup time, staff resources) to manage so much unstructured data.

Semi-structured

Somewhere in the middle of all of this are semi-structured data. The most notable example in healthcare is PACSs, where a database maintains information about images that are stored (so that part is structured), but the discrete files (images) are unstructured data. PACSs usually run on top of a SQL or Oracle database and the structured part of the system is small compared to the massive size of the unstructured images. Another example of semi-structured data is an enterprise document storage system in which documents are scanned and stored and information about them is stored in a database, much like a PACS for documents (document images). As healthcare organizations move toward being paperless, more documents are stored electronically and the volume of semi-structured data is expanding exponentially.

The challenge for healthcare IT is to figure out how the data are organized and the best way to manage it—both for day-to-day operations and for BC/DR. If you have terabytes of unstructured data, how do you determine what to backup or the order in which you need to restore those data? What is critical and what is left from years of people leaving the organization and simply abandoning their data files? It's an impossible task to do during an emergency, so it needs to be undertaken in the normal course of business. If you find yourself with terabytes (or more) of unstructured data to be restored after a disruptive event, you may just have to restore them all and clean up afterward, the least efficient and more expensive course of action.

That said, you should have a very clear idea of what databases you're running and what kinds of data they are managing. If you've been with your healthcare IT department for any length of time in the systems/databases side of things, you no doubt have a pretty good handle on this. If, on the other hand, you are new to the organization or newly managing a team in the IT department, you would do well to do a bit of discovery. Understanding not only how much storage you have but how those data are organized (or not) can be immensely helpful as you develop your BIA and risk mitigation strategies. It's important to understand what data must be restored and in what order.

Types of systems and storage

The types of systems and hardware you have in your data center will largely be dependent on the roadmap the organization has had for IT over the past decade. It will also depend on the overall financial health of your organization, the size and configuration of your corporate structure, and other factors. That said, there are a few high-level facts worth discussing in this section.

First, many of your systems might be virtualized and to the extent they are, you certainly have a more robust infrastructure that can withstand interruptions—the failure of a spindle or a server becomes a non-event as software handles the migration, replication, and commissioning of a replacement. However, in healthcare IT, not all your systems will be able to be virtualized. Some clinical systems cannot handle a virtualized environment or have such strong ties to allocated memory or timing of network traffic that virtualization causes the application to behave badly. To the extent that you have physical servers running clinical applications, you'll need to have a discrete backup and recovery plan for each of those applications and servers.

Second, many clinical applications are deployed as appliances or “black boxes” that IT has no visibility to or control over. They reside in a rack in the data center and the vendor connects remotely to update, reboot, or manage the device. This poses a significant challenge to your BC/DR planning. Do you have an “as built” set of documents outlining exactly what you have purchased and are using? Do you have a vendor technical support and sales contact? Does the vendor back up the configuration files or the data? Are you supposed to be doing that? Are you backing up the data or device? How would those data be restored if the data center was destroyed? Do those systems manage life support equipment? How are downtimes handled?

Often there are systems in the data center that no one in IT “owns”—they live on their own and everyone either assumes or hopes that someone has their eye on it. Often, that’s just not the case. The solution ends up being a bit haphazard. The vendor may or may not have backups of their configuration files, they may or may not connect in a secure manner, and they may or may not be able to replace the appliance at the same hardware and software revisions as you currently have. These are all things to consider in your BC/DR planning and are somewhat unique to healthcare IT.

For BC/DR planning purposes, you may choose to duplicate servers and key applications not just to an off-site location, but to a secondary location at the same site. Depending on your specific situation, it may be wise to put core servers and applications in a secure distribution center at your location to provide an alternative to the primary data center. If the data center is offline but other areas of the organization are still online, you may be able to run critical systems from a local secondary location while you begin your assessment and recovery tasks. This is one aspect to consider as you look at your BC/DR plan. For some smaller organizations, this may not be a viable option. For mid- to large-sized organizations, this may well be a very affordable interim solution. It allows you to have local redundancy and removes the data center as the single point of failure. For that to be effective, however, you need to have core network services available as well. We’ll discuss that in a moment.

Moving on to storage, you need to ensure that your storage is configured in a manner that provides high availability as well as extensibility. As data in healthcare continue to expand exponentially, the demand to pull those data back out and analyze them will also grow. “Big data,” “data analytics,” and “business intelligence” are hot topics in IT these days and healthcare is certainly in the thick of it. If your storage platform cannot handle the data, the replication, deduplication, and growth, you should start thinking about how you handle both growth and BC/DR needs. Cloud computing is another hot topic and has its pro’s and con’s with respect to healthcare data. Most notably, concerns about security have prevented many large healthcare organizations from moving to cloud computing or storage, but that is a dynamic area at the moment and the outcome is far from certain. What is certain is that you need to ensure your storage architecture both supports growth and BC/DR. You may have opportunities to get creative and develop a solution that both provides solid BC/DR capabilities but enhances the organization’s use of storage at the same time.

Network core, medical network, and guest network

Clearly, the core infrastructure in a healthcare organization consists of servers, storage, and network connectivity both within the data center and out to end user devices. The convergence of server and network architectures is providing new capabilities that work well with the demand for high availability.

The network core is clearly the foundation for all other network capabilities. In most larger healthcare organizations, core network functions are handled by redundant systems and are usually located in physically separate locations—whether that’s a separate sector of a large data center (connected to separate power, cooled by separate systems, for example) or in different data centers or secure distribution centers

throughout the facility. If your network architecture does not have core functions distributed in a physical and logical manner, your organization is at risk. Reviewing and modifying existing architecture will be a key component in your BC/DR planning. One of the new services hitting the IT market is Network as a Service (NaaS), which may further streamline (or complicate) healthcare IT and BC/DR in the future. For a very technical discussion of NaaS, see Microsoft's research document entitled "NaaS: Network-as-a-Service in the Cloud" (Costa et al., 2012).

Some healthcare organizations have created a medical network for connecting medical devices. This is a current standard and is done to ensure the CIA of patient data as well as to prevent nonmedical data from crowding out vital data on the network. For example, as companies move to VoIP and video services, those often require a Quality of Service above many other types of data. How, then, do you prioritize audio and video compared to medical data? They both require high priorities so service levels are maintained, but they may not play well on the same network. Segmenting out medical device data onto a medical network helps solve that problem. It also allows you to segregate that traffic and maintain it in whatever way is most suitable to the environment. However, it also can create a challenge in terms of BC/DR. Replicating network infrastructure for BC/DR is expensive—ensuring you can also replicate or recreate a medical network adds a layer of complexity to the equation. In most larger healthcare organizations, this is handled through additional core network functions that manage these separate virtual networks. For BC/DR, though, this can mean additional components in your infrastructure (more cost, more maintenance, more connectivity, more complexity). It's up to you and your IT team to determine the best path forward for your organization, but if you have a medical network, you need to address downtime and redundancy in the event of a business disruption or disaster as a discrete planning phase. We've already discussed the risk and criticality with medical equipment. How you address those needs in your organization should be high on the list of priorities for BC/DR planning.

Finally, most healthcare organizations provide some sort of network connectivity for guests—whether they are patients, family members, business associates, physicians, or visitors. Many organizations provide a special, secure physician-only wireless infrastructure. Regardless of what you provide and to whom, you need to determine the criticality of that network. In many cases, guest networks are high on the list of satisfiers for patients and visitors. At the same time, there are no life safety issues with a guest network, and there is no real requirement for this network other than convenience. If you determine that guest network (including physician's) connectivity is a Tier 3 or Tier 4 need, it will be addressed as time allows after the major impact of a disaster or disruption has been addressed. That might be perfectly appropriate, but needs to be indicated in your planning and communicated to your stakeholders. The last thing you need in the aftermath of a disruption is your Chief Medical Officer or your Chief Executive Officer demanding that the visitor network be brought back online immediately because physicians need to connect remotely to a critical external asset when you have other, higher priorities...or so you thought. Think through the uses a guest network might provide in a disaster event and

determine whether some functionality available through this network might be useful in a disaster. Physicians being able to connect to the Internet to access records at their offices might be helpful if your EMR is down; it might not be. Being able to access various Internet sites during a downtime might be helpful; it might not. Think through and test your assumptions about how *you* think the guest network is being used today and how it could potentially be used if there was a major disruption. More importantly, talk with your stakeholders and ask them how this network would be used in a disaster (if available). Ask how important it would be to bring it back online as compared to other very critical tasks. Your plans might not change, but you won't be surprised by misaligned priorities down the road.

Wireless/RFID

Your wireless network no doubt carries a lot of traffic today. In most organizations, wireless devices are proliferating. In healthcare, wireless equipment provides added mobility to clinical providers and that can translate into better patient care, higher productivity, and higher job satisfaction. Wireless controllers and access points are no doubt peppered throughout your facility, and managing the wireless network is often a full-time job for a network engineer. Tuning radio signals, ensuring strong coverage in key areas, getting rid of dead zones, and dialing back signal that's spilling out into areas it shouldn't, can be a large job if you're in a facility that is growing or changing frequently. How important is your wireless network to patient care? How many critical devices communicate wirelessly and depend on that connectivity? Understanding all the wireless devices and how they are used in a clinical setting will give you a deeper appreciation for the work your clinical folks do as well as broaden your own understanding of how technology is used in patient care. You may have a partial understanding of how these technologies are used, but you'd be wise to spend a few hours a week for several months just walking around talking with clinical managers and staff and observing their work. You'll be surprised by how that alone sharpens your understanding and helps you fine-tune your BC/DR plans to address this critical need. It may be that you determine your overall network BC/DR plan adequately addresses these issues, but adding wireless devices and associated clinical areas to your checklist will ensure you've thought through the implications. If you have a significant downtime, you don't want to find yourself in a position of not being informed about how wireless devices impact patient care.

If your organization has implemented real-time location services (RTLS) or radio frequency identification (RFID) services, you may have implemented it to manage medical devices. As such, there may be interfaces into asset management systems, EMR, and other systems. Depending on whether or not you've integrated RTLS/RFID into other systems will dictate how you treat these systems in your BC/DR plan. It may be as simple as saying, if the network is offline, we will resume tracking when it comes back online. However, you need to check with your customers to understand how they're using the technology today and what the implications are if one or more components of that infrastructure go offline. You also need to understand what level of recovery is required for these systems. How do they tie into

patient safety and patient care? How do they impact supply chain? Understanding workflows and data flows will be crucial to getting this right.

Security infrastructure

As with other technologies, we’re not going to spend time getting into the details of network, server, or storage security. We are going to discuss overall infrastructure security as it relates to BC/DR in a healthcare organization. However, items that should be on your list are things like data loss prevention technologies, e-mail security and encryption, data encryption (data at rest, data in transit), access control lists, group policies, firewalls, DMZs, intrusion prevention and detection systems, and related technologies your organization has implemented to keep data safe.

From the data presented earlier, it’s clear that PHI and financial data (credit card, insurance information, patient insurance identification data, etc.) are targets for attackers. When data for your organization are compromised, you have a disruptive event that has to be addressed and remediated. Throughout, we’ve focused on physical events such as fires and earthquakes, but in this chapter, we’ve pointed out numerous logical threats that can be seriously disruptive to your business and which must be addressed in your planning. When performing your BIA and risk assessment phases, you must ask and answer questions such as:

1. What data do we have that might be vulnerable to current threats (SQL injections, for example)?
2. How would our systems and processes be impacted if we had to contain or take a system or set of data offline to investigate a malware infection?
3. What alternative systems could our clinical staff use in these events? What backup plans should patient care providers have?
4. How would we determine if the threat was addressed and stopped?
5. How would we determine if any PHI or PCI data were breached?
6. How would we determine the scope of the impact and appropriate remediation steps?
7. What other parts of the business would be impacted if any of our Tier 1 or Tier 2 applications were compromised? How would we respond?
8. What plans do we have for recovering from this type of disruption?
9. What function would our incident response team play and what would their scope of work be?
10. Who would we have to notify and in what order?

As you can see, the list can go on, but these are the same kinds of questions you have to ask in the aftermath of any business disruption or disaster event. The difference is logical threats and events are less tangible and are sometimes harder to think through. Addressing a fire in the data center is fairly well defined; addressing a malware outbreak on a virtual server running three different applications is different.

REAL WORLD

Medical Identity Theft on the Rise

An emerging area of identity theft is medical identity theft. For a variety of economic reasons, people are stealing others' medical identification—primarily to receive medical services they might otherwise not be able to receive. Stolen PHI data are often mined for medical identity information. We won't go into the political, economic, or social elements of this discussion, but it is worth mentioning this growing trend so you understand how large a target healthcare IT has become.

One form of healthcare fraud, known as medical identity theft, has its own staggering statistics: 1.42 million Americans were victims of medical identity theft in 2010, according to a 2011 study on patient data privacy and security by the Ponemon Institute. The report estimates the annual economic impact of medical identity theft to be \$30.9 billion.

(Kam and Arevalo, 2012)

Consider this—the street value of a social security number is \$1. The street value of medical identity information is \$50. You can do the math.

As an IT professional, you are tasked with securing your data—from patient data to financial data to other confidential information. The rise of medical identity theft makes your healthcare organization a more appealing target than ever before. A breach can cost hundreds of thousands, if not millions, of dollars in fines and reparations. These are disruptions to your infrastructure and should be assessed during your BC/DR planning. What if your network is seriously breached? What will you do? What steps will you take to stop the breach? What steps will you take to investigate and remediate? While these are not normally thought of as disasters, they are. They are electronic disasters and are a growing problem. Having a plan around how you'll address these is an important part of your overall BC/DR plan. Your CISO or Information Security team may have these plans in place (or in progress) and they should be rolled into your IT BC/DR plans.

End user devices

End user devices run the gamut from desktop and laptop PCs to printers, document scanners, bar code scanners, smart phones, and consumer-oriented tablet devices. These devices are typically easy to replace and inexpensive (individually; replacing 500 of them gets expensive). How do they come into play in your BC/DR planning?

First, look at how your IT department uses these devices. If the data center was destroyed or went dark, what tools would your team need to recover and are those available outside your building? Are these tools backed up? Are they living in the wild on individual's desktops and laptops? If the IT building was destroyed one night by a bomb or a plane crash, how would you manage to transition to your DR site or implement your BC/DR plan? Chances are good a lot of very key information resides on these end user devices and your IT department may be more at risk than you realize. For healthcare IT, that could mean the difference between recovering in your agreed upon time frames or missing them altogether. Do an inventory of IT systems and assets and correlate them to how you manage your infrastructure. Then, incorporate a plan for ensuring the availability of needed hardware and software in the event of a disaster. For example, you may load up a few laptops with key applications and data (encrypted, of course) and have staff or managers keep them at home or

rotate them. The challenge is keeping them up-to-date and out of harm's way. If you have multiple locations, you can certainly use those locations for redundancy. If you are a single data center facility or don't have multiple locations, you'll have to get creative and determine what will work best for you.

From a patient care perspective, end user devices are how data get in the hands of the clinicians. If the EMR is down, how would clinical staff access those data? Is something stored locally on a PC? On a laptop? Can they connect to the wireless network to access data via a remote hot site? The end devices are less important, of course, than how data are provided. However, looking at things like emergency power in clinical areas, what end user devices are plugged into emergency power, which should have uninterruptible power supplies (UPS), which should auto-login, which should auto-reboot, etc., should all be thought through. Planned power outages, whether testing emergency generators on a periodic basis or via facility maintenance activities, give your team the opportunity to ensure end user devices are assessed and understood in the scheme of BC/DR planning.

Finally, developing hardware standards and working through a trusted value-added reseller (VAR) can be extraordinarily helpful when facing a disruptive or disaster event. With a quick phone call to your VAR, you can have a swarm of hot spares, new hardware, and even preconfigured systems, depending on what's been arranged in advance. Once you have your BC/DR strategy in place, involve your VAR in discussions about what capabilities they can provide. For healthcare IT, that can save time and money in the aftermath of a disaster.

One last note on this topic—be sure your end devices do not store PHI or PCI unless local disk encryption is used. A single laptop can be the source of a breach of hundreds of thousands of names and can be a serious event for any organization—so be sure you're looking at how and where data are stored on end user devices and ensuring the security of those data in the event of theft or loss. In the event of a disaster, you won't have to wonder how many laptops are missing, whether or not they are destroyed or intact, and whether you have data exposure as a result.

HEALTHCARE OPERATIONAL NEEDS

In this section, we'll walk through various operational needs of your organization to ensure your list of stakeholders and business functions is complete. You'll need to do a survey of your own organization, but as is the case with many IT professionals in healthcare IT, you may only have a partial understanding of how business runs. Understanding the various components to the business can help you be a better steward of resources and ensure that the right priorities are set for backup and recovery objectives for key organizational data.

Admitting

If you work in a hospital setting, admitting is the first place patients enter the organization. Functions such as verifying patient demographic information (name, age,

date of birth, address, etc.) as well as insurance and payment information are gathered. Typically, this is done in your EMR system as these data are used in every aspect of patient care. Typically, these data become part of the admits, discharge, and transfers feeds that connect just about every hospital EMR-related system from imaging to lab to pharmacy and more. The admitting function also gathers insurance and payment information to establish eligibility and coverage for hospitalization and/or outpatient procedures.

Insurance verification and billing services

Though probably invisible to most IT staff, the insurance verification and billing services function is probably second only to patient care in terms of priorities for the hospital. If the hospital cannot establish eligibility and authorization for a procedure or hospital stay, it may not be reimbursed for costs. This is true whether the patient has Medicare, Medicaid, or private insurance. If the healthcare organization you work in is on this side of the equation, such as an insurance company or payer of any sort, you know the criticality of these functions in your business, which include the following:

- *Eligibility.* Determines whether a person is covered by insurance for a medical procedure or reason and to what extent. Eligibility drives reimbursement for services to providers, so ensuring things line up at this juncture is vital to patient care, patient expectations, and provider payments.
- *Enrollment/disenrollment.* Determines whether a person is part of a plan or not. A person can be enrolled or disenrolled for a variety of reasons such as being a new hire (enrollment), losing other insurance (divorce), or leaving the company (disenrollment).
- *Authorization.* After eligibility is established, authorization must be verified, especially for anything outside normal ranges. For example, visits to a physician office or an urgent care center usually don't need to be specifically authorized, but a nonemergency surgical procedure usually must.
- *Coding.* A step in the medical billing function is coding everything that was done. In order for a payer to know exactly what was performed and how much they pay for a given procedure, there must be a framework for common understanding. That framework is called International Classification of Diseases or ICD. The worldwide standard is ICD-10; the United States still uses ICD-9, though the U.S. government has set deadlines for converting to ICD-10. A discussion of the implications of this conversion is outside the scope of this book, but suffice it to say that this conversion is a massive one that all U.S. healthcare organizations are now planning and undertaking.
- *Billing.* The care provider bills the payer, whether that is the insurance company or the person or a combination. These bills are generated by gathering data from throughout the healthcare continuum. In a physician office, that might be the office visit, lab draw, medications, minor procedures, etc. In hospitals, that can

include any procedure done throughout the facility, supplies used in surgeries, supplies provided the patient (walker, oxygen, etc.) as well as the overall hospital care itself. Billing is dependent upon complete and accurate medical coding of the care provided.

- *Claims, remittance.* Submitting claims and receiving remittances to/from payers is a complex process that generates a lot of work in your billing department. It's almost never a straightforward process and because there are so many payers with vastly different plans, programs, and rules, each provider has to navigate this challenging environment to receive payment for services rendered. If any of the electronic systems that interface to billing systems is impaired, it can have a ripple effect throughout the organization that will impact revenue and bottom line results pretty quickly.

You may choose to assist your subject matter experts in assessing various systems by breaking it down into fundamental business processes. These business processes must be well defined and documented before they can be analyzed. However, once defined, you might end up with a matrix that looks a bit like the data in [Table HIT.1](#). In this grid, you can use a standard rating system (see [Chapter 5](#) for more on developing and using standardized scales) to create a semi-quantitative or quantitative assessment of the impact of disruption of information systems used for key business systems.

Table HIT.1 Operational Business Process Scoring Matrix for BIA

Business Process ^a	# 1	# 2	# 3	# 4
<i>Impact data</i>				
# Patients impacted				
# Providers impacted				
% Cost of this BP as % of whole				
% Of monthly transactions				
Regulatory requirements?				
Political impact?				
Impact on patients/beneficiaries?				
Impact on providers?				
<i>Total score</i>				

^aEach business process should be clearly defined and documented and numbers here should refer to those definitions.

Your health information management (HIM) function will typically drive this analysis and provide critical data. However, you'll need to ensure the team identifies minimum acceptable levels for:

1. Eligibility: inquiries and responses
2. Enrollment and disenrollment: self-serve or assisted
3. Authorization: requests and responses

4. Coding: ensuring procedures are documented in a complete and accurate manner
5. Billing and remittance: requesting (billing), receiving, and reconciling incoming funds
6. Claims: receipt of electronic and paper data, handling, and disposition of claims data
7. Claim status: inquiries, responses, and audits

You might be thinking this is far outside your direct area of responsibility and it may be. However, the more educated you are about how your organization runs, the more effective you can be in your role in developing an IT BC/DR plan. For example, if you don't ask these kinds of questions to your HIM department experts, they may not think about these kinds of issues. Once they begin thinking about these questions, you will more easily be able to address key elements of your BC/DR plan. You might be better able to determine the risk to various systems or processes. You may be able to assist in developing mitigation strategies or you may be able to better understand the relative criticality of various upstream and downstream systems.

For each identified business process, the HIM staff should identify workarounds in the event needed electronic systems are unavailable. Depending on the complexity and volume of work, this may be a huge challenge. Your job is not to develop their workarounds or contingency plans, but it may be expected that you help them think through what they would do if systems were unavailable. This may occur with an assigned IT project manager leading the discovery or it may be through a vendor contracted to assist in the BIA and contingency planning aspects of your BC/DR plan.

Perhaps the biggest takeaway from this section is an understanding of how your healthcare organization makes money, how it bills, and how it collects and reconciles claims and payments and remittances. Revenue management (often referred to in hospitals as the *revenue cycle*) is a complex and challenging segment of the business. You don't need to become an expert in this area, but understanding the high-level elements can help you create a BC/DR plan that ensures your organization is able to receive funds and keep the doors open in the aftermath of a serious business disruption.

Clinical care

We're not going to spend a lot of time on this area—the scope of clinical care your organization provides (if any) is likely very well known to everyone in the organization, even IT staff who may not regularly interact with clinical functions. However, there are a few areas that are worth mentioning so you include them in your thinking as you develop your risk assessment and BIA. To exclude these from consideration will leave a gap in your plans, so thinking through the impact will be a worthwhile use of your time.

Physician

If your healthcare organization is a physician practice, then all your BC/DR planning will have been around supporting and sustaining physicians, physician assistants, and nurse practitioners in that environment. However, if you work in an ambulatory

surgery center or a hospital, for instance, you might have developed plans for the EMR and for direct patient care (how nurses and patient care techs might continue to provide care if the EMR is down), but you may not have specifically looked at your physician population. You'll need to talk to your professional services staff to determine what systems they use, what they would do if those systems were down, and how the organization would be impacted both short term and longer term. For example, credentialing systems ensure that the physician has the proper credentials for the work they intend to perform—whether that's a surgical procedure in an OR, an emergency procedure in the ED, or a diagnosis—the physician must be credentialed and the healthcare organization needs to keep track of that (for many different reasons). It's vital for you to ensure that your systems related to working with physicians are addressed in your BC/DR planning.

Another angle is to think through what your physicians need in order to perform their work. Most likely these are the key systems you've been looking at already—EMR, diagnostic imaging, PACS images, lab results, pharmacy, etc. However, you might ask your professional services experts to come up with a list of systems (or at least functions) that are key to physician work at your facility to ensure you have covered necessary systems in your BC/DR plan.

Nursing

For the most part, our discussion has focused on what's needed to provide safe patient care and continue running the business in the event of a disaster or disruption. Nursing is a single term for a wide and varied set of skills and activities. There are numerous specialties within nursing and if you take a look at the diverse population of patients you treat, you'll begin to appreciate those skills. From labor and delivery to newborns, all the way to geriatrics and hospice, nursing specialties are found in every area of care. Your BC/DR plans likely already encompass the areas that would most impact nursing, but including clinical leadership in your planning will ensure you cover all the required areas and will also help educate clinical leaders about how to prepare for system downtimes. It's easy for clinical staff to become so accustomed to using electronic systems that they don't develop sound downtime processes and procedures. This is where your clinical informatics team can add tremendous value—through assisting in this disaster planning and readiness phase.

Support services

These services will vary depending on the organization type you work in. However, it is definitely worth noting support services as an area to investigate and address in your BC/DR plan. If you work in a physician office, your support services may well be external vendors with whom you have a contract, including lab, imaging, or pharmacy services. If you work in any sort of clinic or hospital typesetting, there may be numerous departments providing support, or ancillary, services. These can include (this list is not exhaustive by any means):

1. Gastro-Intestinal Lab
2. Vascular Lab

3. Cardio-Vascular Catheter Lab (Cath Lab)
4. Radiology and Diagnostic Imaging (CT, MRI, PET, ultrasound, etc.)
5. Respiratory Therapy
6. Physical Therapy and Rehabilitation
7. Pain Management
8. Wound Care
9. Pharmacy
10. Lab
11. Central Supply

In your BC/DR risk assessment and BIA, you need to not only look at your primary systems, such as your EMR, but supporting systems and systems that are used only in these support areas. How do lab systems interface with your EMR and what are their BC/DR plans for lab systems (if any)? Do they have redundancy of systems in-house? What would they do if there was a hazardous spill in the lab and that area was evacuated and sealed off for months? These are questions your organization's overall risk management team should be engaged in and planning for. They almost always fall outside the direct line of responsibility for IT professionals. Still, those systems interconnect with systems managed by the IT department and simply assuming they're taken care of would be a mistake. Rather than expanding the scope of your work beyond reasonable measure, you might give a planning checklist to each support department and ask them to work through the questions and answers. To the extent those systems impact your planning, you can actively engage and develop BC/DR plans. Using the lab example, however, it may be that all labs would be shipped off-site via courier to another lab and results would be faxed back and manually entered into your EMR. That's a viable plan and that may be all you need to complete your portion of the BC/DR plan, that is, ensuring there are no gaps even if the specific plans are outside your scope.

INTEROPERABILITY AMONG DISPARATE SYSTEMS

In this section, we'll look at a variety of systems at a high level. The objective is not to provide an exhaustive list of systems but to provide categories of systems that you can use as a checklist to look internally at your systems. A full inventory of your in-house systems, as well as all external systems you may connect to, is critical to a complete BC/DR plan. This section will give you a running start.

Electronic medical record

It's the biggest application you are likely to have and needs no further mention. One note is to get your clinical application team together and ensure you have mapped out every upstream and downstream system that connects. That will end up looking like a spaghetti map, but at least you'll have it mapped out and inventoried. Figuring out

how to architect a satisfactory DR solution will be a challenge, but it can only be solved with a clear inventory starting with your EMR.

Diagnostic imaging

This category doesn't need a lot of explanation either. However, it is worth noting that many healthcare organizations have two, three, four, or more PACSs. Some are internal; some are external (outsourced or managed by a vendor/partner). Some are integrated through interfaces to your EMR; some may be stand-alone. Talk with your PACS Administrator, your clinical application team, or your Imaging department to understand the dependencies—from storage to backups to recovery times and dependencies.

Medical equipment

As previously mentioned, more and more medical equipment is either being interfaced to the EMR or it has a server component that lives in your data center. The biggest challenge is often that these systems are FDA regulated and may “fly under the radar.” They may be managed by the vendor with remote access. They may be run as “black boxes” and you and your team may have little visibility or control over these systems. Ensuring you have a solid BC/DR plan starts with a deep discussion with your Clinical Engineering team or your Biomedical and Diagnostic Imaging teams. If the equipment can run in stand-alone mode during a disaster or business disruption, that's great. More often than not, these devices now require network connectivity and a server connection so they need to be pulled into your BC/DR plans.

Food services

Food services applications allow staff to plan menus and prepare the right number of meals for the patient population. Food allergies and dietary restrictions/needs are addressed through food services systems. An outage of these systems won't necessarily stop the chef from baking the chicken or steaming the broccoli, but the ability to prepare, distribute, and manage food services is highly dependent upon IT systems. Ensure these systems are discussed as part of your BC/DR plan and that you understand the relative priority of these systems as well as any potential workarounds.

Environmental services

Environmental services run the gamut from cleaning patient rooms, ORs, and hallways, and it also includes the ability to schedule cleaning staff in these areas and perform routine, emergency, and periodic maintenance. Though these systems may be lower priority in the clinical scheme of things, it might be easy to overlook these systems in your planning process. More and more of these systems are tied to

the EMR (so that cleaning staff are paged when a patient is discharged, for example) and/or are becoming Web based. Keeping an eye on upstream and downstream dependencies with these systems will help ensure your BC/DR plan addresses these needs appropriately.

Billing and payment systems

We've talked about financial systems of various sorts, but it's worth mentioning that the revenue cycle at a hospital is one of the most complicated financial processes you can imagine. Even if you work in healthcare IT, you may have no real understanding of the process your billing and claims folks have to use to get paid for services. There are thousands of patients with thousands of insurance plans with hundreds of insurance companies. Visits must be documented, then coded, and then billed. That process alone may involve four or five or six different systems, all interfaced, to hand data back and forth. If one link in this chain goes down, the whole line stops. Essentially, it cuts off the ability to collect revenue for services rendered. It's clearly the foundation of keeping the business solvent and is a critical business function. Make sure you bring your medical records, HIM, and finance professionals into the discussion to ensure your plans adequately cover these complex systems.

Payroll

If you ever want to see reasonable people become unreasonable quickly, just miss paying one paycheck. Getting paid for work, is fundamental to how business operates. Payroll systems typically have high visibility in IT, so there's little chance that this system would be overlooked. However, one key to note is that payroll is, in most healthcare organizations, somewhat repeatable (at a macro level). So, help your payroll folks be creative when looking at alternatives in the event of a serious downtime. One organization, when asked about how they would handle a downtime, indicated they would simply call the bank and ask them to repeat the prior payroll. This would ensure people who got paid 2 weeks ago would get paid again. While that may be a bit more cumbersome for a hospital compared to an outpatient surgery center or physician practice, for example, it's a potential solution. Hospitals also often rely heavily on temporary types of labor, which can complicate payroll activities for clinical staff. Keep your options open when looking at workarounds and Recovery Time Objectives for various systems.

Also, your organization's Payroll staff will be well aware of this, but there are typically legal requirements around timely payment for staff and timely payment of taxes and other funds withheld from paychecks (such as savings transfers, 401K contributions and garnishments, for example). Your BC/DR plan, just like any other organization, needs to address these legal requirements. These are not unique to healthcare and should be fairly easy to address in your BC/DR plan.

Human resources

Human resources (HR) systems manage all data about employees from pay rates to tenure, performance appraisals to promotions. It tracks employee credentials, which may be required for accreditation, along with employee demographic data and more. From recruiting functions (open positions, external job postings, applicant tracking) to hiring to performance management to benefits administration to terminations, HR systems contain vast amounts of confidential data that need to be addressed in a BC/DR plan. Your HR professionals or legal counsel will be able to provide guidance on federal, state, and local laws which may play into your BC/DR planning. Understanding key functions and how they may be impacted by a potential downtime will be essential to developing both a solid assessment of risks but possible mitigation strategies as well.

CURRENT ENVIRONMENT AND NEW TECHNOLOGY

Before we conclude this chapter, it's worth looking at what the current environment is in healthcare IT BC/DR. As mentioned previously, more than 30% of the world's storage is found in healthcare. Much of the data are considered mission critical and must be always available or quickly recoverable. Digital images are tied to EMRs and many organizations are, essentially, paperless. With the proliferation of electronic systems, paper backup options are simply no longer available. You can't go back to paper since paper doesn't exist. Few healthcare organizations were fully prepared for the burgeoning demand *going paperless* placed on IT infrastructure and many are struggling to keep up or catch up.

Added to the mix is the increased regulation by government, regulatory bodies, or other organizations defining how healthcare information should be secured and protected in the event of a system outage, loss, breach, theft, or all out natural disaster.

It's not all bad news, however. There are numerous positive trends in technology that can mitigate some of these pitfalls. These are not specific to healthcare IT, so we'll cover them briefly here as they are discussed in more depth primarily in [Chapter 6](#) and elsewhere throughout this book.

Advances in data storage and replication

Over the past 5 years, there have been significant changes in data storage infrastructure technologies as well as replication techniques. The ability to use higher bandwidth in the data center, especially to data storage infrastructure, has enabled faster data storage and management. Replication options such as backing up to disk, deduplication technologies, and vaulting have greatly increased throughput for organizations with large data repositories, as most healthcare IT shops have. The ability to replicate data to a remote location (DR site) and synchronize those data has become

an increasingly popular option for BC/DR planning for many organizations. The challenge in healthcare, specifically, is that the number of interconnected systems increases the complexity dramatically. It's insufficient to simply transmit your data to a remote location; you must also be able to resume operations after a disaster by bringing systems and data back online in a controlled and often prescribed sequence. Whether you choose a cold, warm, or hot site for your DR solution, you'll have to address all the interfaces that feed your EMR (we're assuming your EMR is your top Tier 1 application). All the data must be synchronized as you bring systems back online. We'll discuss recovery later in this book. For now, your organization should be looking at your data storage and replication infrastructure with an eye toward BC/DR. If you don't have a great solution in place now, you should be building your business case for upgrading your infrastructure in the coming years with solid data, including financials, return on investment (ROI), and risk management data. You may have to add to your capabilities in an incremental fashion through a multiyear capital funding plan. If you lay out your roadmap with associated financials and business impact data, you'll make a compelling business case for the investments. If you've already got a robust and up-to-date infrastructure in place, look to optimizing that infrastructure for BC/DR.

Mobile devices

Mobile devices are the bane of every IT shop at the moment because they are challenging to manage. The trend toward bring your own device (BYOD) is good news and bad news. In healthcare IT, the challenge is to safeguard protected health information (PHI) and medical identity information. As physicians use more mobile devices to connect to multiple EMRs, there's a higher likelihood that some data may reside on mobile devices, even if temporarily. For example, many physicians work at multiple hospitals and connect to their own practice's EMR as well. Where do those data reside? How long are they resident on the device? These are questions information security analysts are wrestling with daily. However, from a BC/DR perspective, mobile devices may be more good than bad.

Take a look at how mobile devices are used in your healthcare organization today and determine whether there are opportunities to define a role for mobile devices in your BC/DR plan. Many staff have laptops, tablets, or smartphones. How could you leverage these technologies in the event of a disaster? What applications would you deploy today if you knew you would have to rely on these devices tomorrow? What types of communications plans (discussed in [Chapter 7](#)) would you use if you could rely on mobile devices?

There are no solid answers to mobile device management in healthcare IT today, though most organizations have a tentative roadmap and strategy in place. That said, you can review your current mobile device applications and connectivity options and see how you might turn this challenge into an opportunity for your organization.

CRITICAL CONCEPT**Virtual Desktop Infrastructure**

One area of growing interest and utilization in IT is virtual desktop infrastructure (VDI). VDI was a term coined by VMWare, Inc. and is also sometimes referred to as server-based computing. As you're probably aware, VDI serves up the desktop operating system and installed applications from a virtual machine on a server. This abstracts the OS and application software from the physical desktop device. Clearly, the benefits are that a desktop can be standardized (good news for IT), virtualized (good news for IT), and served up anywhere (good news for end user). As organizations explore the cost/benefits of VDI, there are three key concepts worth noting specific to healthcare IT.

First, and most important, you need to assess your current state environment and determine *in which scenarios* VDI might make sense. It is not an all-or-nothing proposition and it's critical to look at ways in which VDI might add value and where it would simply add complexity. Of course, there's a minimum cost for implementing VDI and it may not make financial sense to move forward unless you're "all in." For example, in healthcare IT, serving up a virtual desktop sounds like a great idea until you look deeper at some clinical areas in which hardware devices are tied to physical locations—because of how vendor software is configured or for clinical workflow reasons or security concerns. For example, a prescription printer can only be printed to by certain groups defined by security, clinical role, and location. Due to the way in which security and clinical functionality is presented via vendor applications (most notably, the EMR), this can be a difficult challenge to work through. As more vendors are looking at virtualization (in general) as a viable and cost-effective framework, the challenges of VDI will undoubtedly be addressed. However, it's important in healthcare IT to look at the very practical workflow implications and ask how this might work and what might create problems. Don't assume VDI can or cannot be implemented, but do be aware of the challenges unique to healthcare IT.

Next, there is a cost to additional infrastructure, so to say that VDI saves money without deeper analysis is misleading. It shifts the cost from desktop to server, which may ultimately reduce the overall cost of ownership. This is especially true if your organization already has a robust virtualized server environment and the infrastructure (network, server, storage) to support this framework. Several years ago, there were blanket statements being made about the cost effectiveness of VDI without the accompanying discussion of how it impacts server and storage infrastructure. Again, without analysis, you can't make a definitive statement. Looking at VDI by today's standards and evaluating where and how costs shift will enable you to develop a solid financial analysis of VDI for your healthcare organization.

Finally, VDI potentially shifts work from your desktop team to your server team or changes the work your desktop team performs. These changes need to be assessed before making a commitment to going the VDI route. Ultimately, you may decide to do what many organizations have done—roll VDI out for specific use cases in a pilot program. You can monitor and measure results, gather end user feedback, and fine-tune your approach before rolling out more widely. The primary drawback to this approach is that you have to have or put some VDI infrastructure in place before even piloting a program. In some organizations, that alone might be cost-prohibitive or too resource-intensive for your organization. Start with a compelling ROI and thoughtful use cases before making any technology decisions.

Virtualization and cloud computing

Most larger IT organizations have implemented virtualization to some extent. The ability to run virtual servers provides redundancy, high availability, and agility to an IT organization, when well-managed. When not well-managed, it can lead to complexity, confusion, and mismanagement of the infrastructure. However, there's

mostly upside to virtualization including the ability to move data or applications around in the virtualized environments for upgrading, patching, or testing; to upgrade, patch, or repair the underlying hardware; or to create various test environments that can be used for system development, validation, or even DR testing. The ability to move environments on the fly with no disruption to end user computing is a huge step forward, especially for healthcare IT departments, where continuous access to the EMR and associated systems is a requirement. Being able to virtualize also makes DR solutions more easily developed, though the challenge remains in terms of the interconnectivity of so many upstream and downstream systems such as PACS, medical device interfaces, images of scanned documents, lab results, and even billing and coding systems.

One note regarding virtualization, mentioned previously in this chapter is that in a healthcare IT environment some clinical applications may be unable to be effectively virtualized—either because the application is a legacy application or because it is sensitive to some of the variables inherent to virtualization. The critical takeaway here is that you need to inventory your applications, especially clinical applications, and understand whether they can be virtualized or not. If you find connectivity or latency issues arising with data or synchronization of data, you may have to move back to physical. This comes into play when planning your BC/DR options. If you rely solely on a virtualized environment for DR and your applications are not all virtualized, you will have a gap that must be addressed.

Cloud computing is a hot topic in IT circles these days and has been for the past few years. With numerous large organizations offering cloud storage and cloud computing capabilities, it's an area worth investigating. Many smaller healthcare IT organizations may already be taking advantage of some cloud technologies, such as secure backup to the cloud. For smaller to mid-sized healthcare IT organizations, this may well be the best option and certainly more affordable than renting space at a remote data center, paying for dedicated bandwidth and maintaining a duplicate set of hardware and software. For larger organizations, the jury is still out—it's not clear where the cost/benefit, risk/reward lines fall.

In healthcare IT, the overriding concern is the ability to ensure the CIA of patient data. When data reside in the data center, there is an assumption that the data are secure both in transmission and at rest. Technologies are implemented to ensure the data are secure. However, when transmitting to the cloud and storing remotely on servers and data centers you can neither control nor physically access, you are abstracting security by one level. This is not necessarily a problem but most IT security professionals are, by training and necessity, control freaks. Before signing up for cloud-based storage, especially as a DR solution, healthcare IT leaders need to clearly assess the potential risk to data. There have been numerous high profile cloud-based security breaches and outages. When a provider like Amazon has an outage, you have no control over the situation, you have to sit patiently and wait for them to restore services. For small organizations, this lack of control also translates into removing the need for high end IT specialists and may therefore be a smart tradeoff. For larger organizations, the need to manage and control data is likely an overriding

factor in not moving to hosted cloud solutions. That doesn't mean all cloud solutions should be rejected; there are numerous private cloud options, including a combination of public and private (hybrid), that may make sense. This is an area of technology that is evolving rapidly and is worth keeping an eye on as a potential partial or full DR solution for healthcare IT in the future.

REAL WORLD

For Cloud Options, Start with SaaS

The most logical place to explore the viability of cloud compute or storage solutions is with service offerings that are already cloud based. Most healthcare IT organizations oversee hundreds of applications, many of which are moving toward Web- or browser-based solutions. If you want to understand how cloud technologies might benefit your organization, you might begin with looking at these applications. They're already Web based, so they're already hosted externally. This is a great starting point for exploring cloud technologies, how they intersect and interact with your internal IT systems and how they might be leveraged in the event of a business disruption.

That said, there is a new category of Web-based services now referred to as Recovery as a Service (RaaS). RaaS can help ensure secure and reliable data backups to an off-site location (public or private cloud). While RaaS is gaining momentum, most analysts don't foresee RaaS making significant inroads into large enterprise IT anytime soon. The sheer number of applications running across a range of computing platforms (Windows, AIX, Solaris, etc.) in large enterprises makes RaaS far more complicated. In addition, larger organizations typically have remote cold, warm, or hot sites established. RaaS may end up being an excellent solution for mid-tier enterprises, and it's certainly an area of growing interest in IT.

The take away here is that cloud-based storage makes sense for some organizations and not for others; it's not a cure-all. It's worth taking a look at the current state of cloud-based offerings and comparing to your IT needs. Comparing the level of investment, infrastructure, and IT expertise needed to use (or not use) cloud computing should factor in. The complexity of your systems and interfaces certainly will play into the equation as will the overall assurance (guarantee) of information security both in transit and at rest. These are big questions to answer during the course of planning your BC/DR solutions, but are worth investigating as part of your larger technology roadmap.

Communication systems

Communications systems used to mean telephone trees and handheld radios. With the proliferation of personal communication devices (aka cell phones and smartphones), the landscape has shifted significantly. When a hospital has a disruption to phone systems, it's still a huge problem, but communication can still occur through cell phones, pagers, wireless communication devices, and overhead paging systems (if not tied to telcom). This change makes business disruption communications planning a bit easier. In healthcare IT, you need to address not only the potential downtime of your internal telephone system but your external communications as

well. Physicians routinely call or fax orders or instructions; clinical staff call pharmacy, lab, or radiology to get status; purchasers call vendors to place orders—the list goes on and you’re no doubt well aware of how telephones are used in your environment today.

Ensuring you have telephony DR plans is vital for your BC/DR plan. In addition, you need to ensure you are looking at broader disaster planning and working in tandem with your risk management team. For example, most larger healthcare organizations participate in some sort of local, regional, or statewide disaster management programs. Automated notification systems, Web-based call trees, and text messaging options are part of these systems and should be leveraged as part of your BC/DR planning.

In addition, the proliferation of cell phones, whether the organization provides it or the employee does, makes cell phone communications a viable option during a business disruption. Incorporating this into your BC/DR planning will provide you additional options and flexibility as you walk through your disaster scenarios.

Current environment and new technology summary

There are just a few of the new, emerging, or accelerating changes that are helping IT departments deal with the ever-increasing demands. Information technologies are quickly evolving and healthcare IT is in the thick of it all. If you like a slow, steady pace, healthcare IT is not the place for you. If you thrive on change and finding creative solutions to difficult and complex problems, you’re in exactly the right place. Now, let’s wrap up our discussion of BC/DR for healthcare IT by looking at some final BC/DR best practices.

HEALTHCARE IT BC/DR BEST PRACTICES

The last topic we’ll cover in this chapter are some guidelines on BC/DR best practices. The intent is to help you wrap up what you’ve learned in this chapter and apply it toward your healthcare IT department’s planning efforts.

Security frameworks

There are numerous frameworks that address information security as well as BC/DR. As you no doubt understand, the two practice areas (InfoSec and BC/DR) are tightly integrated and really must be addressed in tandem. That said, the various frameworks available to organizations help address those concerns. In this section, we’ll briefly discuss three frameworks you might consider if you don’t already have a framework selected. There are many frameworks available; our discussion is limited to three that are frequently chosen for healthcare IT.

National Institute of Standards and Technology

The U.S. Department of Commerce’s National Institute of Standards and Technology, Information Technology Laboratory ([National Institute of Standards and Technology, 2013](http://nvlpubs.nist.gov/nistpubs/SP/nist.sp.800-53r4.pdf)) provides a wealth of information about IT including applied and computational mathematics, advanced network technologies, biometrics and computer security, among other things. Though the focus is on federal information systems, the framework and best practices can easily be applied to healthcare IT. The library of special publications can be found here: <http://csrc.nist.gov/publications/PubsSPs.html> (Computer Security Resource Center, 2013). It contains a wealth of information on information security. In fact, you could spend weeks reading relevant information on this site, so if you haven’t been on this site or haven’t visited recently, it’s worth exploring even if you don’t select this framework. Two relevant NIST standards which may help with your BC/DR planning efforts include:

- *SP 800-53 Rev 4*—Security and Privacy Controls for Federal Information Systems and Organizations
- *SP 800-12*—An Introduction to Computer Security: The NIST Handbook (Chapter 11 addresses BC/DR)

ISO/IEC 27000 series

The ISO/IEC 27000 series is an international standard for information security. There are numerous publications that guide information security, including (not full list):

- ISO/IEC 27000:2012—Information security management systems—Overview and vocabulary
- ISO/IEC 27005:2011—Information security risk management
- ISO/IEC FDIS 27013—Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

The ISO standard is widely recognized and this framework might be suitable for your organization. Take a look at <http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html> (International Organization for Standardization, 2013) to review the ISO standards related to information security.

HITRUST common security framework

The framework most aligned to healthcare IT is the HITRUST framework, which exists “to ensure that information security becomes a core pillar of, rather than an obstacle to, the broad adoption of health information systems and exchanges...The HITRUST CSF addresses these industry challenges by leveraging and enhancing existing standards and regulations to provide organizations of varying sizes and risk profiles with prescriptive implementation requirements” ([HITRUST LLC, 2013](http://www.hitrustcc.org/)). The primary benefit of using the common security framework (CSF) in a healthcare organization is that it is specifically designed for healthcare IT. It establishes benchmarks and requirements that incorporate best practices and standards from ISO, PCI,

COBIT, HIPAA, HITECH, and NIST. As a healthcare IT professional, you need a framework that is not only compatible with the way you manage your IT department, but one that enhances the work you do by driving improvements in areas specific to healthcare.

Throughout this chapter, we've discussed standards such as HIPAA and PCI. The CSF framework compiles these standards and addresses information security for healthcare IT. For more information on this framework, visit <http://www.hitrustalliance.net/commonsecurityframework/>. This framework is available to qualifying individuals, so registration is required to access this information.

Information Technology Information Library

One last framework to mention, though not specific to BC/DR or information security, is the Information Technology Information Library (ITIL) framework. ITIL is one source of Information Technology Service Management (ITSM) but is a widely adopted model for managing IT. It covers an array of topics and is used as a model for developing and improving IT management. It originated in the United Kingdom in the 1980s as an approach for defining how successful organizations could deliver IT service. It has evolved since then and has been adopted by organizations worldwide. One of the primary benefits to the ITIL framework is that it works well with other frameworks such as COBIT, NIST, ISO, CSF, and methodologies including Agile and Lean. It describes a wide range of best practices and can be used to guide your IT organization's efforts toward process improvement and overall service management. It's easy, then, to understand how using a framework like ITIL in conjunction with whatever IT security framework you choose can drive improvements and efficiencies in your healthcare IT organization. While it might sound duplicative, it's really more complimentary. For example, a security framework might talk about change management to avoid errors that could take entire systems down or expose them to intruders. The ITIL framework provides a process overview for how to organize change management in your organization to ensure it is a documented, repeatable process (ITIL, 2013).

REAL WORLD

Select and Implement a Framework

No matter what industry you work in, you are likely subject to some sort of regulation. In healthcare IT, the primary regulatory areas that impact your IT work are HIPAA and PCI. The best thing you can do for your organization is to select a framework against which you will measure your efforts. HIPAA and PCI have requirements that don't always intersect, but they are not at odds with one another either. Review several frameworks for suitability to the way your organization runs before selecting one. Once you select a framework, stay up-to-date on any revisions to that framework and ensure your auditing, monitoring, and remediation efforts keep your organization compliant. If a disruption, breach, or disaster ever does occur, one of the first questions that will be asked is whether the organization was following its published and approved policies and procedures. In other words, if you establish a particular framework and you follow those guidelines, you are in far better shape than if you either (a) have no framework or guidelines in place or (b) have a framework but are not following it.

Best practices

We'll close out this chapter with a checklist of items you should review for your BC/DR plan. This list should be used in tandem with the information presented throughout this book to ensure your plan addresses all areas of BC/DR planning, including elements with specific healthcare implications. Use this as a starting point, not an end point, to ensure you have looked at and addressed all major and minor systems used to provide safe, effective patient care and to maintain the operations of the business.

1. *Understand every aspect of your business, at least at a high level.* Talk with experts in your organization to develop a solid understanding of how things work at your healthcare organization. Having a clear understanding of how revenue is generated and captured, what the key cost drivers are, what clinical services are offered, what technologies they use, how the medical equipment intersects with IT, how patients are cared for, how financials are managed, how staffing and personnel is managed, and so forth can provide you a holistic view of the organization that enables better, smarter BC/DR planning.
2. *Develop current documentation showing servers, databases, applications, and all interfaces.* Use a service framework (ITSM) for managing your IT systems from change management to capacity management to availability management and beyond. You can't develop a meaningful BC/DR plan without knowing your current state.
3. *Develop a process for incorporating BC/DR aspects into equipment procurement, commissioning, and management.* Don't wait for a huge capital budget to be approved to begin improving your BC/DR capabilities. Build BC/DR into planning and design requirements, add them to procurement guidelines, and begin addressing BC/DR incrementally. For a real world look at this process, read the Energy/Utilities Industry Study.
4. *Understand the relative criticality of all applications in your data center.* Understand what data you're managing in the data center and ensure your backup and recovery strategies are aligned with criticality. Keep in mind that your users will tend to exaggerate the importance of their own systems and processes, so work to normalize your findings across the environment. Also, be sure you have awareness of all systems and applications that reside outside the data center. Develop backup and recovery plans for those systems and those data as well.
5. *Separate data from systems, where possible.* Some data can be stored or archived separately from the systems used to manage those data. When discussing systems and criticality during your BIA, find opportunities to see where periodic data extracts might be useful as downtime files. If you can separate the data from the system, you may find inexpensive and fast ways to restore key functionality in the aftermath of a disaster.

- 6.** *Select an appropriate framework and adhere to the policies and procedures you develop within that framework.* Selecting a framework aligned with your organization's goals, objectives, strategy, and size will make much of the BC/DR work easier. It will provide guidance on what to work on first as well as how to approach the work. Developing policies and procedures aligned with that framework will help ensure compliance with regulatory requirements and reduce the likelihood of gaps or serious noncompliance. Finally, ensure you work within your published standards to maintain quality and compliance.
- 7.** *Proactively look at your technology infrastructure and look for opportunities to provide better service at a lower cost with less risk.* Healthcare IT is a dynamic and complex environment. Looking for opportunities to continually improve patient care, to proactively avoid problems, and to find ways to provide innovative service to your customer base is what makes working in healthcare IT exciting. While you have to focus first on "keeping the lights on," both day-to-day and in the event of a disaster, you should also be focused on staying informed about changes in the IT market. Leveraging new technology can improve service delivery and lower cost. Whenever you can achieve both objectives, you're raising the bar.
- 8.** *Leverage your organization's risk management team.* IT BC/DR planning cannot happen in a vacuum. If the disruption is limited to your data center, you and your team are certainly the people who should develop and implement a recovery plan. However, if a flood, earthquake, pandemic, or other disaster impacts the organization as a whole, IT BC/DR will be just one aspect of an overall disaster response plan. Be sure you are tied into the organization's efforts. Better yet, look for technology you can leverage that will assist the organization's disaster response plan as well as your own IT BC/DR plan.
- 9.** *Assign owners.* Like any other duty or assignment, if it's not specifically assigned to anyone, it won't get done. Add BC/DR to job descriptions, to roles and responsibilities, and to teams. Once you've developed your initial BC/DR plan, maintain it by assigning discrete tasks to individuals. This may help prevent having to do another large project to completely overhaul and update your plan in a few years' time.
- 10.** *Don't stop.* BC/DR planning is an ongoing process. Just like many other aspects to IT, you can't just set it and forget it. Being sure that your IT organization could recover from the most likely types of disasters or disruptions is one of your primary responsibilities. This requires a plan to periodically review and revise your plans and then test them. It's almost impossible in today's healthcare IT environment to carve out time to do this, but you must. Building BC/DR considerations into your daily, weekly, and monthly standard work will help ensure you stay current. Creating an annual review process and adhering to it will also help. Gaining executive support through your IT governance process and/or your risk management team can assist greatly.

SUMMARY

BC/DR has many elements that are common across industries. Performing a risk assessment, developing a BIA, developing recovery metrics, and BC solutions are common elements. However, healthcare IT has some unique attributes that require special attention.

In this chapter, we've reviewed the elements of healthcare IT and the unique requirements, especially as they relate to regulatory requirements. Clearly, compliance with HIPAA regulations is at the core of healthcare IT information security priorities. Ensuring the CIA of personal health information, especially data residing in the organization's EMR. By logical extension, this includes a requirement to plan for data backups, data and systems recovery in the event of disruption or disaster.

Beyond regulatory requirements, we reviewed the technical, business, and operational needs of an effective healthcare IT architecture.

Overview of healthcare IT

More technology than ever before is used in the delivery of healthcare. From high tech clinical tools to EMRs to medical device interfaces pulling in diagnostic imaging, lab results, and pharmacy orders (to name a few), healthcare IT is a dynamic and changing landscape.

The environment is further complicated by regulatory requirements around patient data CIA, personally identifiable data including medical identity information, and financial data. All of these systems interoperate and intersect in healthcare. Investments in healthcare IT are topping \$275 billion and are expected to grow.

The challenge is to find ways to leverage technology to improve patient care and reduce costs. As healthcare costs continue to climb and our U.S. population grows older and lives longer, healthcare IT is challenged to come up with innovative solutions. Those solutions need to contribute to maintaining or improving patient care, but do so at a lower cost per unit.

The depth and breadth of healthcare organizations create a diverse industry filled with highly sophisticated organizations and those barely using technology; it includes practices large and small; it includes those that provide direct patient care and those that provide support services. The environment is further impacted by the increasing focus on connected care across the continuum of services and the need to interconnect health information. Understanding the impact of ACO or HIE participation to your healthcare IT will become increasingly important in the coming years. Regardless of the specific type of healthcare organization you work in, you need to have BC/DR plans in place.

Regulatory requirements

Through existing regulation and new governmental initiatives, healthcare IT is being transformed. New regulations impact the security and availability of healthcare data across the continuum of care. Ensuring patient data are secure and available to the

right clinical providers at the right time is just one aspect of the requirement. Data are also being shared by insurance carriers, third party billing firms, quality analysts, and governmental entities. Ensuring your healthcare IT department is aware of and compliant with the regulations that impact your organization and its data is a critical focus of BC/DR in healthcare. In this chapter, we looked at governmental entities including CMS and FDA and the nongovernmental entity, JCAHO. We also looked at various regulations that impact healthcare IT, most notably HIPAA, HITECH, and PCI. While there may be other regulations your organization must comply with, such as governmental (government-run hospitals, for example) or financial (publicly traded, private, nonprofit, etc.), the focus is on maintaining compliance for BC/DR purposes.

Healthcare IT risk management

There is an entire field of study related to risk management and specifically, risk management in healthcare. Their focus is not in IT systems, but instead on healthcare systems such as the environment of care, that directly impact patient safety and care. These are two areas of focus for healthcare IT as well, though from a different perspective. In your BC/DR planning you need to ensure that plans adequately address alternative systems, methods, and processes to ensure that any downtime of technology does not adversely impact the patient.

In addition to patient safety and patient care, there are other areas of healthcare risk management that should be considered as you create your plan. Two very relevant areas are organizational solvency and facility management. Organizational solvency is a risk the finance department must address. However, IT must address them to the extent that financial systems—from billing, to claims management to payment processing to vendor payments to payroll—that are impacted by a business disruption put the organization at risk. Determining interdependencies, backup, and recovery strategies, alternatives to electronic processing in a downtime, and more should all be part of your overall BC/DR plan. This is not unique to healthcare, but some of the financial implications are driven by regulatory requirements and must be addressed. Sitting down with your risk management and finance staff will help surface these requirements.

Facility management may seem like an odd addition to this discussion, but it is part of the overall healthcare risk management function. Providing a safe environment of care usually comes under the direction of the Facilities department, from ensuring heating and cooling are provided to medical gases to repairing broken doors, windows, or flooring. Many larger healthcare facilities have discrete facilities management software suites, some of which interface with the EMR or other asset management systems. Ensuring these are part of your BC/DR planning is important and an area that is sometimes overlooked.

Technical needs—Healthcare IT architecture

Healthcare IT storage needs are burgeoning due to the proliferation of interfaces pulling in large image files, including diagnostic imaging from CT, MRI, and

ultrasound to real-time laparoscopic images recorded in the OR during a surgery. Regardless of the source of the data, storage needs are growing every year and as healthcare IT becomes more interconnected, that trend will accelerate. The healthcare IT environment can be generally divided between clinical and business systems. These systems can be separated out by function, but they are inextricably linked in healthcare. From scheduling an appointment to performing a procedure, from admitting a patient to drawing a specimen for the lab and beyond, the business of healthcare is clinical care. Being able to perform both the clinical and business functions in the aftermath of a business disruption is vital to long-term success and short-term crisis management. In this chapter, we reviewed standard IT elements such as servers, storage, and wireless technologies and discussed not only how they're used in a healthcare setting but how they might be impacted by a DR event. In some cases such as mobile and cloud compute and storage resources, we looked at how these technologies might reasonably be leveraged in a disaster.

Healthcare operational needs

Throughout this chapter, we've endeavored to draw your attention to the vast array of considerations for your BC/DR planning. Understanding the operations of your healthcare organization is central to your overall ability to develop a comprehensive yet practical BC/DR plan. Understanding areas such as admitting, insurance verification, and billing services are needed in order to properly assess risk and mitigation. While we did not specifically discuss HIM or the medical records functions in this chapter, we did discuss the some of the systems needed to generate and collect revenue. Having discussions with your key business stakeholders—from HIM to professional services to quality to facilities to infection control (and others)—will ensure you have no gaps or serious deficits in your BC/DR plan.

Interoperability among disparate systems—Integration in healthcare IT

In this chapter, we discussed a number of systems that must be integrated or interconnected in order to manage a healthcare organization. While the types and numbers of these systems vary depending on the exact nature of the healthcare organization, what remains the same across the environment is the rising complexity of managing these connections. It's a relatively simple prospect to be able to backup, recover, and restore a single system or a series of systems. It's much more difficult when systems are interdependent and the availability of upstream and downstream data must be carefully synchronized and verified. We discussed the EMR, diagnostic imaging systems, medical equipment, food services, environmental services, and facilities services to name just a few. We also looked at how financial systems, scheduling systems, payroll, and HR systems all interconnect and have an impact how the business is run and therefore, indirectly, how care is provided.

Current environment and new technology

There is a plethora of new technology available to healthcare organizations today, the challenge is sorting it all out and developing a technology roadmap to leverage new and emerging technologies. Regardless of how electronic (or not) your organization is, patient data are at the core of every effort. How those data are generated, stored, recovered, and made available during a downtime are the key considerations for every healthcare IT department. With more and more healthcare organizations “going paperless,” there is no paper fallback option in many cases.

Advances in virtualization technologies, particularly in compute and storage functions, are driving improvements in redundancy and availability. Mobile devices, while still the bane of many IT organizations, are driving changes in the IT landscape. These changes, both innovative and challenging, need to be considered as part of your BC/DR planning. Cloud computing is captivating the imagination of healthcare CFOs who see large potential savings. Meanwhile, healthcare CIOs investigate ways to develop architectural designs using cloud technology that seamlessly integrate into the interconnected world of healthcare IT.

Healthcare IT BC/DR best practices

In this section of the chapter, we looked at several frameworks that can be used for developing your overall approach to information security, regulatory compliance, and BC/DR. The frameworks discussed included NIST, ISO/IEC, and HITECH/CSF. We also discussed ITIL against the backdrop of these other frameworks. The discussion was not an exhaustive review of the frameworks available, but simply a starting point and a discussion of the ones most often used in healthcare IT in the United States today. The takeaway from this is that a framework should be adopted to provide structure and guidance to your efforts and to help ensure your organization achieves and maintains compliance with applicable regulatory requirements.

The top 10 best practices we discussed were:

1. Understand every aspect of your business, at least at a high level.
2. Develop current documentation showing servers, databases, applications, and all interfaces.
3. Develop a process for incorporating BC/DR aspects into equipment procurement, commissioning, and management.
4. Understand the relative criticality of all applications in your data center.
5. Separate data from systems, where possible.
6. Select an appropriate framework and adhere to the policies and procedures you develop within that framework.
7. Proactively look at your technology infrastructure and look for opportunities to provide better service at a lower cost with less risk.
8. Leverage your organization’s risk management team.
9. Assign owners.
10. Don’t stop.

KEY CONCEPTS

- **Overview of healthcare IT**
 - Rising cost of healthcare is driving demand for better care at a lower cost.
 - Healthcare IT can contribute to better care at a lower cost through use of new technologies.
 - Increasing dependence on technology creates new challenges for healthcare IT.
 - Governmental regulations are creating an environment where healthcare IT must move forward or face penalties in the future.
 - HIEs and ACOs are driving change across the continuum of care.
 - HIEs and ACOs must be considered in BC/DR planning if there are legal, organizational, or regulatory requirements for your organization in this arena.
 - Integration of healthcare IT and medical systems is driving the need to develop BC/DR plans with respect to these interconnected devices.
 - Information security is a challenge in medical device systems both due to medical device manufacturer's sometimes lagging technical sophistication and due to FDA regulation.
 - Consumer-driven healthcare is rapidly changing the face of healthcare and will continue to impact the way care is delivered.
 - Real-time access to medical data is enabling faster, more collaborative delivery of healthcare and in many cases, driving better clinical outcomes.
 - Managing real-time data and data interfaces is a challenge for healthcare IT departments and must be considered in BC/DR planning.
- **Regulatory requirements**
 - CMS/JCAHO are focused on patient safety and improving patient care. Neither organization currently regulates or audits IT systems, but the interaction of clinical staff with systems can come under scrutiny.
 - HIPAA is at the core of most healthcare IT departments with respect to information security and BC/DR planning. Maintaining the CIA of personal health information is the top priority.
 - The HITECH Act provides a set of incentives to healthcare organizations with respect to EMR implementation, data security and Meaningful Use. The objective is to use electronic systems to capture data and for organizations to analyze and act upon findings to continuously improve patient care.
 - PCI requirements are related solely to consumer financial transactions related to credit cards. Since almost all healthcare organizations accept credit card payments, they must also be PCI compliant.
 - State and local requirements vary by locality and it's important that each organization's legal or risk management team is aware of these requirements. Some may have IT implications and must be addressed in BC/DR plans, if required.

- Business-specific requirements vary depending on the type of healthcare organization such as hospital, SNF, assisted living, outpatient clinic, physician office, lab, pharmacy, or rehab, to name just a few.
- **Healthcare IT risk management**
 - Patient safety is at the core of every activity undertaken by responsible healthcare organizations. To the extent that electronic systems and data are needed to ensure patient safety, these systems must be the highest priority in BC/DR planning.
 - Patient care runs the gamut from high acuity to low acuity and there are numerous electronic systems used in a variety of patient care settings. Understanding how these interface with IT and what the availability needs are of these systems is an important element of BC/DR planning in healthcare IT.
 - Organizational solvency is always at risk in the aftermath of a major disaster or business disruption. Healthcare organizations need to be able to capture charges, bill, collect, and post payments in order to continue to deliver care. These essential business functions are at risk in a disaster and healthcare IT professionals must address these needs in the BC/DR plan.
- **Technical needs—Healthcare IT architecture**
 - Clinical systems directly or indirectly impact patient care. Most notable is the EMR system, though numerous other systems are typically interconnected to the EMR to provide additional data.
 - Business systems are the systems used in healthcare to manage the business including financial, supply chain, payroll, and HR systems. These may not directly impact patient care but must be carefully prioritized during the BIA to ensure key systems are available for running the business in the aftermath of a disaster event.
 - Types of data include structured, unstructured, and semi-structured. Your BC/DR plan needs to address each type of data. Different solutions are appropriate for different types of data.
- **Operational needs**
 - Admitting is a function of inpatient healthcare organizations including acute care, subacute care (skilled nursing), and behavioral health.
 - Insurance verification and billing services are not often top of mind for healthcare IT staff. These systems are needed for ongoing financial operations and must be included in BC/DR planning.
 - Clinical care includes many different types of providers from physicians to nurses to patient care tech, respiratory therapists, physical therapists, pharmacists, lab techs, and more. Each area must be assessed for BC/DR requirements to ensure that your BC/DR plans support the way your organization runs.
 - Physician
 - Nursing
 - Support services include lab, pharmacy, supplies as well as other clinical support services such as GI Lab, Cath Lab, Vascular Lab, Pain

Management, and Therapies (physical, occupational, respiratory, behavioral). Each area in your healthcare organization requires special review for BC/DR planning purposes.

- **Interoperability among disparate systems—Integration in healthcare IT**
 - EMRs are at the heart of IT integration in healthcare today. Organizations have varying levels of adoption and the degree to which they are paperless.
 - Diagnostic imaging is a service offering that generates storage demands for healthcare IT. Many PACSs interface with EMR systems to provide either embedded or linked access to diagnostic images.
 - Medical equipment is a growing area for healthcare IT as more and more devices are interfaced through some sort of medical device interface technology. Pulling in device data is faster and less prone to error, though it adds complexity for IT.
 - Food services is integral to patient care in inpatient settings and there are clinical implications such as managing diets (low sodium, gluten free, low sugar) and avoiding allergens.
 - Environmental services are responsible for the health and safety of the environment including cleaning and periodic maintenance of various systems. Each organization's EVS team may have slightly different areas of responsibility but these systems often tie into the EMR as well (prompting staff to clean a room upon patient discharge, for example).
 - Billing and payment systems are vital to ongoing operations, regardless of whether you work in a local lab, a physician practice, or a multistate acute care hospital. If your organization's ability to bill and collect funds is a fundamental requirement and must be addressed effectively in your BC/DR planning.
 - Payroll is to employees what billing is to an organization; staff depend on timely payment for their efforts. There are certainly laws regarding payment of staff, but here are more pressing and practical matters that should be addressed in BC/DR planning.
 - HR systems capture data about the people in your organization from recruiting to hiring; credentialing to benefits administration; and pay to PTO and beyond. These systems are not unique to healthcare IT but some of the types of staff in healthcare HR systems are. Ensuring your BC/DR plan meets the needs of your particular organization requires discussion with both HR and clinical leaders.
 - Facilities/building automation is another fast-growing field where automation and industrial controls are intersecting with other IT systems. These systems are often not as technically advanced as other types of systems and can be challenging to create BC/DR plans around. Having awareness and working toward a solid solution is a great starting point.
- **Current environment and new technology**
 - Advances in data storage and replication technologies have both driven the demand for more storage and the more cost-effective solutions available to organizations.

- The current explosion in demand for mobile devices and BYOD is straining IT departments as they struggle to develop security standards and solutions. However, mobile devices also present opportunities to provide faster, secure access to healthcare data.
- Virtualization and cloud computing are two fast-growing areas in IT. Many healthcare organizations have virtualized compute and storage assets to gain higher availability, more resilience, and less reliance on physical infrastructure.
- Cloud computing offers many risks and benefits. Many healthcare organizations have yet to embrace cloud technologies. The most logical place to explore this is with applications that are already hosted (SaaS).
- **Healthcare IT BC/DR best practices**
 - Understand every aspect of your business, at least at a high level.
 - Develop current documentation showing servers, databases, applications, and all interfaces.
 - Develop a process for incorporating BC/DR aspects into equipment procurement, commissioning, and management.
 - Understand the relative criticality of all applications in your data center.
 - Separate data from systems, where possible.
 - Select an appropriate framework and adhere to the policies and procedures you develop within that framework.
 - Proactively look at your technology infrastructure and look for opportunities to provide better service at a lower cost with less risk.
 - Leverage your organization's risk management team.
 - Assign owners to ensure responsibility and accountability are clearly defined.
 - Don't stop, BC/DR is a continuous improvement effort.

References

- AuthorizeNet. Understanding PCI compliance. <http://www.authorize.net/resources/pcicompliance/>; 2013 [Retrieved May 24, 2013], from AuthorizeNet.
- Center for Information Technology Leadership. The value of healthcare information exchange and interoperability. https://www.ncoic.org/apps/group_public/download.php?19487/CITL%20HIEI%20Levels.pdf; 2004. Retrieved from Network Centric Operations Industry Consortium.
- Centers for Medicare and Medicaid Services. Accountable care organizations (ACO). <http://www.cms.gov/Medicare/Medicare-Fee-for-Service-Payment/ACO/index.html>; 2013 [Retrieved May 24, 2013], from CMS.gov.
- Centers for Medicare and Medicaid Services. Accountable care organizations (ACOs): general information. <http://innovation.cms.gov/initiatives/ACO/index.html>; 2013 [Retrieved May 24, 2013], from Centers for Medicare and Medicaid Services.
- Computer Security Resource Center. Special publications (800 series). <http://csrc.nist.gov/publications/PubsSPs.html>; 2013 [Retrieved May 24, 2013], from National Institute of Standards and Technology Computer Security Resource Center.

- Costa P, Migliavacca M, Pietzuch P, Wolf A. NaaS: network-as-a-service in the cloud. <http://research.microsoft.com/en-us/um/people/pcosta/papers/costa12naas.pdf>; April 2012 [Retrieved May 24, 2013], from Microsoft Research Cambridge Lab, Paolo Costa.
- Healthcare IT News. Infographic: biggest healthcare data breaches of 2012. McCann E, editor. <http://www.healthcareitnews.com/news/infographic-biggest-healthcare-data-breaches-2012>; December 12, 2012 [Retrieved May 24, 2013], from Healthcare IT News.
- Healthcare IT News. Stanford reports fourth HIPAA breach. McCann E, editor. <http://www.healthcareitnews.com/news/fourth-hipaa-breach-involving-stanford-u>; January 12, 2013 [Retrieved May 24, 2013], from Healthcare IT News.
- HealthIT.gov. HITECH programs & advisory committees. <http://www.healthit.gov/policy-researchers-implementers/hitech-programs-advisory-committees>; 2013 [Retrieved May 24, 2013], from HealthIT.gov.
- HealthIT.gov. Policymaking, regulation, & strategy | health IT rules & regulations. www.healthit.gov/policy-researchers-implementers/health-it-rules-regulations; May 24, 2013 [Retrieved May 24, 2013], from HealthIT.gov.
- HIMSS Analytics. Overview. www.himssanalytics.org/home; 2013 [Retrieved May 24, 2013], from HIMSSAnalytics.org.
- HITRUST LLC. HITRUST common security framework version 4.0. Health information trust alliance. Frisco, TX: HITRUST LLC. <http://www.hitrustalliance.net/>; 2013 [Retrieved 2012].
- International Organization for Standardization. Freely available standards. <http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html>; 2013 [Retrieved May 24, 2013], from International Organization for Standardization.
- ITIL. Overview. <http://www.itil-officialsite.com/>; May 13, 2013 [Retrieved May 24, 2013], from ITIL.
- Kam R, Arevalo C. A glimpse inside the \$234 billion world of medical fraud. <http://www.govhealthit.com/news/glimpse-inside-234-billion-world-medical-id-theft>; February 8, 2012 [Retrieved May 24, 2013], from Government Health IT.
- National Institute of Standards and Technology. Information technology library. <http://www.nist.gov/itl/>; 2013 [Retrieved May 24, 2013], from National Institute of Standards and Technology.
- Ponemon Institute LLC. Research studies & white papers: security. <http://www.ponemon.org/data-security>; June 30, 2008 [Retrieved March 2, 2013], from Ponemon Institute.
- Radack S. Computer security division | computer security resource center | ITL security bulletins. <http://csrc.nist.gov/publications/nistbul/november2010-bulletin.pdf>; November 2010 [Retrieved May 24, 2013], from National Institute of Standards and Technology | Information Technology Laboratory.
- U.S. Department of Health and Human Services. Health information privacy | security rule guidance material. <http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html>; March 2007 [Retrieved May 24, 2013], from U.S. Department of Health and Human Services, pp. 8–9.
- U.S. Department of Health and Human Services. HITECH Act. <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hitechact.pdf>; February 17, 2009 [Retrieved May 24, 2013].
- U.S. Department of Health and Human Services. Federal Register, vol. 78(17), part II. <http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf>; January 25, 2013 [Retrieved May 24, 2013], from U.S. Department of Health and Human Services.

Risk Mitigation Strategy Development

6

IN THIS CHAPTER

- Types of risk mitigation strategies
- Risk mitigation process
- IT risk mitigation
- Backup and recovery considerations
- Summary
- Key concepts

INTRODUCTION

Risk mitigation is defined as *taking steps to reduce adverse effects*. Risk mitigation is a commonly used process within traditional business risk management, but as you'll see in this chapter, there are unique aspects to risk mitigation related to IT business continuity and disaster recovery.

The mitigation strategy development phase of the business continuity and disaster recovery project plan, shown in [Figure 6.1](#), is where you develop strategies to accept, avoid, reduce, or transfer risks related to potential business disruptions.

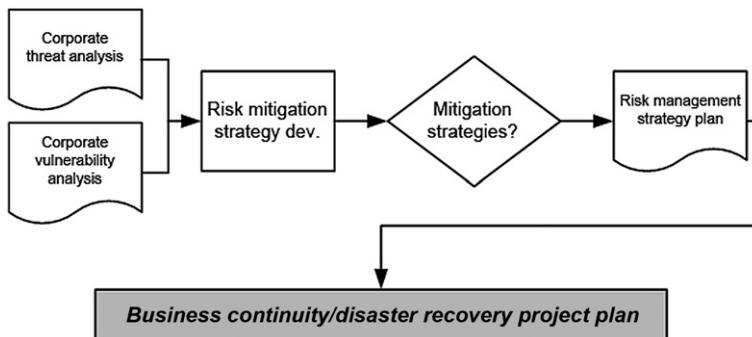
Developing the risk mitigation strategies is the last phase of risk management activities, which was shown in [Figure 4.2 in Chapter 4](#). This last segment, depicted here in [Figure 6.2](#), includes the inputs of the risk assessment and business impact analysis data. This information, along with risk mitigation data, is used to develop strategies for managing risks in a manner that is appropriate for your company. Once you have the risk management section completed, you can begin to draft your business continuity and disaster recovery plan.

As mentioned before, it's important to develop risk mitigation strategies that match your company's profile. If your company is very risk averse and wants to avoid risk at almost any cost, your strategies will need to be appropriate for that objective. On the other hand, if your company doesn't mind taking on a bit of risk, your BC/DR strategies will be different than a more conservative, risk-averse company's approach. There is no one-size-fits-all answer in the risk mitigation phase—you'll have to create a strategy that meets your company's financial, operational, and risk management goals.

According to ISACA, a nonprofit IT and information systems professional organization, IT risk is the business risk associated with the use, ownership, operation,

**FIGURE 6.1**

Business continuity and disaster recovery risk mitigation.

**FIGURE 6.2**

Risk mitigation phase details.

involvement, influence, and adoption of IT within an enterprise (ISACA, 2009). We discussed performing your IT risk assessment previously, and we covered a wide range of potential threats, the risks they pose, and the potential impact to your organization. As you probably discovered during your risk assessment and business impact analysis phases, your company has just a handful of critical applications that have the greatest impact on your business. It probably roughly follows the 80/20 rule. Twenty percent of your applications are going to require 80% of your time, effort, and resources to address appropriately. Eighty percent of your applications, then, should only consume 20% of your time, effort, and resources. It's important to keep this in mind as you're developing your strategies.

TIP

Keep It Simple

The temptation can be very strong to address every risk you encounter. However, if you define too large a project and are too ambitious in your undertaking, you're likely to fall well short of an acceptable outcome. Instead, keep your top priorities in mind as you develop your risk mitigation strategies and ensure you have the key elements covered. You will need to instill organizational discipline into an ongoing process of assessment and mitigation, so the very iterative nature of the process gives you the opportunity to triage and hit your biggest risks first. That way, you'll get the fundamentals addressed quickly and can create a more robust plan over time.

As we've discussed, IT threats come in all sizes and shapes with varying levels of likelihood to occur and impact. The importance of assessing these risks and taking steps to mitigate them increases as your company seeks to leverage its investment in technology and deliver better results, improving operations and the bottom line. In the risk mitigation phase, we're going to develop strategies for managing IT risks including determining ways to sustain critical operations, designing the appropriate IT architecture to support business continuity and develop policies and procedures that support these efforts.

TYPES OF RISK MITIGATION STRATEGIES

Let's begin with a quick overview of standard risk mitigation strategies. These will be useful as you develop your strategies. A clear understanding of your options at the outset will help you and your team make better decisions. The four standard choices are *acceptance*, *avoidance*, *limitation*, and *transference*. As you read through these four options, refer to [Figure 6.3](#), which shows the relationship between time and cost for each option and the relative cost of each option to the others over time.

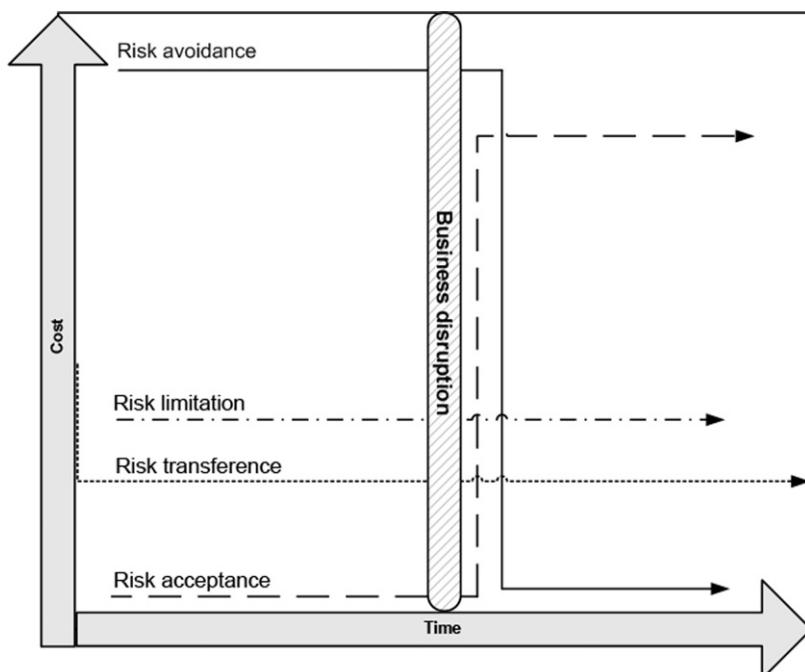


FIGURE 6.3

Relationship between time and cost for risk mitigation options.

Risk acceptance

Risk acceptance is not really a mitigation strategy because accepting a risk does not *reduce* its effect. However, risk acceptance is a legitimate option in risk management. There are various reasons why companies may choose risk acceptance in certain situations. The most common reason is that the cost of other risk management options, such as avoidance or limitation, may outweigh the cost of the risk itself. There is no benefit in spending \$100,000 to avoid a \$10,000 risk. In cases where the cost outweighs the benefit, most organizations choose to accept a risk rather than spend time or money mitigating it.

Accepting a risk is sometimes referred to as the “do nothing” option. This may be a familiar concept for those of you familiar with project management fundamentals. As you develop your strategies, you should consider the implications of “doing nothing.” This can be a way of ensuring that you’re taking appropriate actions because if you consider the implications of accepting the risk, you can see the potential consequences and weight them out against other options.

As you can see in [Figure 6.3](#), the cost of risk acceptance is very low at the beginning (it may even be zero), but after a business disruption, the cost can be significantly higher than other risk management strategies. The company may be willing to save money today knowing that it will have a disproportionately large expenditure later if a business disruption occurs. That’s key—you have to understand that you’re betting that the business disruption will not occur or if it does, it will be far enough in the distant future that you’re willing to take the financial risk.

A word of caution here: Small businesses often take the stance that they cannot afford to avoid, limit, or transfer risk, and therefore, they accept risk by default. This is a mistaken and limited view and should not be the default position going into this planning. Risk acceptance should be evaluated along with the other options to determine the implications, appropriate actions, and costs of various mitigation strategies. Risk acceptance is the least expensive option in the near term and often the most expensive option in the long term should an event occur.

Risk avoidance

Risk avoidance is the opposite of risk acceptance because it’s an all-or-nothing kind of stance. To use an insurance example, cutting down a tree limb hanging over your driveway, rather than waiting for it to fall (maybe on your car, maybe on a person), would be risk avoidance. The insurance company would be avoiding the risk that the tree limb would fall on your car, on the house, or on a passerby. Most insurance companies, in this instance, would accept the risk and wait for the limb to fall, knowing that they can likely avoid incurring that cost. However, the point is that risk avoidance means taking steps so that the risk is completely addressed and cannot occur.

In business continuity and disaster recovery plans, risk avoidance is the action that avoids any exposure to the risk whatsoever. If you want to avoid data loss, you have fully redundant data center in another geographical location that is

completely capable of running your entire organization from that location. That would be complete avoidance of any local disaster such as earthquake or hurricane. Risk avoidance is usually the most expensive of all risk mitigation strategies, but it has the result of reducing the cost of downtime and recovery significantly. [Figure 6.3](#) shows this relationship—the cost is very high early on but the cost after a business disruption is lower than other strategies. Shutting down systems is costly in advance of a hurricane, but if they are packed and shipped to another location and fired up, the cost to recover from the business disruption is minimal. This option is not feasible for many types of risks or for many types of companies. However, it is a viable option to consider as you develop your risk mitigation strategies. As you'll note, we keep coming back to the risk/reward analysis to determine whether we want to spend time and money now (mitigate) or later (remediate). There is no single right answer, and this discussion often requires a strategic discussion with organizational leaders to ensure the overall assumptions and costs are well understood and agreed upon.

Risk limitation

Risk limitation is the most common risk management strategy employed by businesses. You choose to limit your exposure through taking some action. For example, performing daily backups of critical business data is a risk limitation strategy. It doesn't stop a disk drive from crashing; it doesn't ignore the potential for disk failure. It accepts that drives fail and when they do, having backups helps you recover in a timely manner. In [Figure 6.3](#), you can see that risk limitation strategies fall between *acceptance* and *avoidance* both in terms of early costs and costs after the business disruption. In a sense, it's an average of the two. Risk limitations include installing firewalls to keep networks safe, creating backups to keep data safe, practicing fire drills to keep employees safe, and more. We'll discuss various risk limitations you can implement with regard to your key processes throughout the remainder of this chapter because this is, by far, the manner in which most businesses choose to deal with their risks.

Risk transference

Risk transference involves handing the risk off to a willing third party. Many companies outsource certain operations such as customer service, order fulfillment, or payroll services. They do this in many cases, so they can focus on their core competencies, but they can also do this as part of risk management. For example, if you outsource your payroll services, you may choose to select a processing company that is not located in the same geographical region as your firm. If you're in the southeastern United States, you may choose a company in the Northwest or one that has multiple processing sites around the United States, so it can process payroll regardless of weather events.

Another example of risk transference is purchasing insurance or other insurance types of services. In order to transfer risk, you usually have to pay some other company some amount of money to assume that risk, whether it's an IT company that will manage your security or databases for you, or an insurance company that will pay for

losses in the event of a business disruption. Figure 6.3 shows that, relative to other choices, your risk transference will usually cost more as some sort of up-front or ongoing fee, but that the overall cost usually will be somewhere in the same area as risk limitation. One important point to note, however, is that risk limitation usually has an end-point cost where risk transference can be ongoing. For example, you make insurance premium payments every month or quarter, regardless of whether or not you experience an event that requires your insurance company to step in. With risk limitation, you typically put some system in place, such as a firewall or redundant system. The cost of that implementation is finite and known and usually ends at some point in time. Of course, you then have to incur the cost of patching, maintaining, upgrading, and replacing that firewall over time, and those are ongoing costs that are sometimes omitted from the overall cost/benefit analysis. Even when those costs are included and even if they net out to the same cost as insurance, your firm may conclude that it's a more beneficial to purchase the gear and manage it than simply buy insurance. One reason is that usually there are other benefits to having the gear (in this example) that enhance business operations. Another reason is that even if the cost nets out the same, insurance doesn't address the risk in any manner, just the cost.

In the case of contracting with an external payroll processing firm that has multiple geographic processing centers, risk limitation makes sense and does, in fact, limit your exposure. Where it can become a bit convoluted is assessing what additional risks you're taking on by outsourcing your payroll function. You can't simply outsource and expect that your problems are solved.

Thus, while the near-term costs of risk limitation and risk transference may appear to be similar, it's important to understand the *duration* of the cost with regard to these strategies and the operational implications of each. It's also important to assess any new or residual risk that has developed as a result of these decisions.

REAL WORLD

Operationalizing BC/DR

Some companies don't like to discuss risk either because they don't want to acknowledge it or because they are cavalier about the risks they face. This latter stance is most commonly found in small, entrepreneurial start-ups that have their hands full just getting the business off the ground. Often the larger a company gets, the more it is willing to discuss, plan for, and mitigate various kinds of risks. This may be, in part, due to outside pressures of regulatory compliance, financial markets, or investors. If you're working in a small company that doesn't want to address risk, you may run into challenges even getting a BC/DR plan off the ground. As we discussed earlier in the book, you may be able to implement many of the BC/DR plan elements without making a big, formal process out of it. If this is the only way you can do BC/DR planning, it may be worth working in stealth mode. For example, when you look at data backup methods, you may choose to select and implement technologies and processes that not only meet your backup needs but provide an adequate level of BC/DR capabilities as well. You should certainly follow the rules, regulations, and procedures in your company, but you may find that you have a bit of leeway when it comes to implementing technology solutions that will meet the broader needs of the company, even if the company doesn't want to know about it.

THE RISK MITIGATION PROCESS

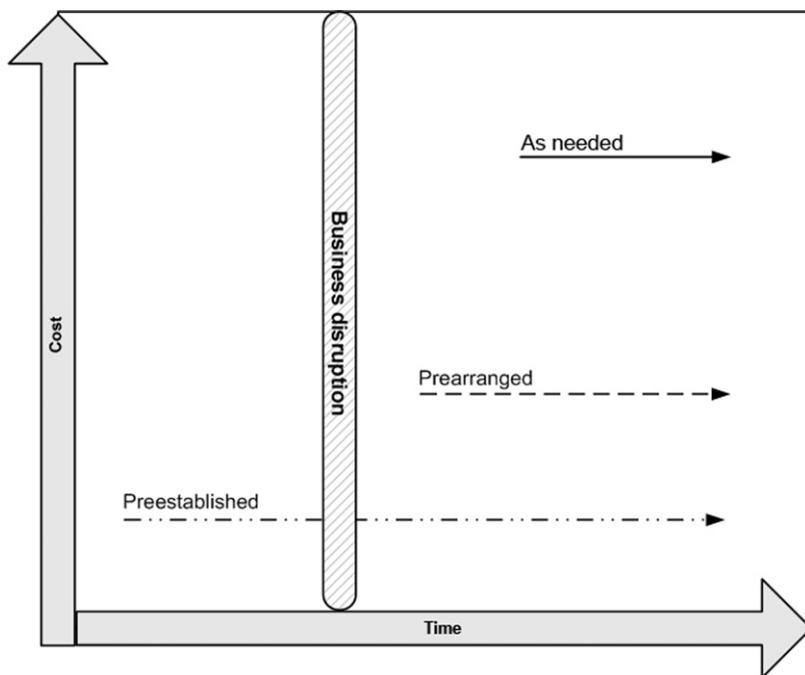
In order to develop a risk mitigation strategy, you first have to know your options. In previous chapters, we looked at the various risks, threats, threat sources, vulnerabilities, and impacts. Next, we need to look at the recovery profile including the recovery requirements, options, timeframe of options (compared with maximum tolerable downtime or MTD), and cost versus the capability of options. From there, we can select appropriate options. Once these elements are known, a comprehensive strategy can be devised. The strategy will ultimately also include identifying off-site requirements and alternate facilities and developing business unit strategies. In the following sections, we'll look at the recovery steps specifically. If this whole task seems enormous, keep in mind that you can focus on your top risks only for the first pass. Don't attempt to solve the whole problem at once. Instead, work through a prioritized list to make this process not only manageable, but actionable as well.

Recovery requirements

Recovery requirements typically are broken down by functional areas including facilities and work areas, IT systems and infrastructure, manufacturing and production (operations), and critical data/vital records. Your company may have other recovery requirements. If so, they should be included in this section. The recovery requirements are developed for the critical business processes identified in the business impact analysis. They help identify the resources that should be the focus of the recovery strategy since there is a cost involved with developing and implementing a mitigation or recovery strategy. If a process is not mission critical (or essential), it is likely not a good candidate for the expenditure of time and effort to develop mitigation strategies. Recovery requirements can be categorized even within the functional areas. For example, a recovery requirement category for facilities is alternate office space. Another category might be a crisis management center or a communications command center. Once you identify the recovery requirements, you can begin to review recovery options.

Recovery options

For each critical business function or process, you have identified the impact on the organization; the dependencies to other functions; the IT dependencies, the key positions, skills, and knowledge needed; and the time requirement for recovery (among other things). Based on these data and on the recovery requirements, you can develop a variety of recovery options. Typically, these options will come with varying timelines of their own as well as varying costs and capabilities. At this juncture, your primary concern is to develop a list of viable options based on the business impact analysis data you have. For example, if you have a requirement for an alternate computing facility, you have numerous options available including borrowing computer space from a local firm to setting up a co-location center outside your own

**FIGURE 6.4**

Comparison of three recovery approaches.

geographic area to using public or private cloud options and many other solutions in between. These options, unless absolutely outside the realm of possibility, should be listed so they can be included in the subsequent evaluation steps.

There are three basic recovery options you can consider. Each of these can also be considered part of a mitigation strategy, as you'll see. You can acquire the option *as needed*, you can *prearrange* for an option, or you can *preestablish* an option. **Figure 6.4** shows the relative cost relationship of these three approaches.

Notice that *as needed* options often take longer to implement after a business disruption and typically cost more at the time. However, the cumulative cost may still end up being lower than *prearranged* or *preestablished* options, especially if one-time setup fees or recurring maintenance fees are required for those other options. *Prearranged* options are typically less expensive than *as needed* solutions, and they often can be implemented in a more timely manner since availability should be guaranteed in the arrangement. However, these may be more costly on an ongoing basis and you need to select vendors carefully to ensure they can deliver on their commitments. Finally, *preestablished* solutions can be implemented almost immediately, but they often have a fairly significant recurring cost or a sunk cost in advance of the disruption. This can make their total cost more than other options. Clearly, *time*

is one of the major factors in each of these options; cost is another and overall utility to the organization is a third factor to explore. Let's look at each of these options in more detail.

As needed

Acquiring resources *as needed* at existing market rates and within existing market availability following the business disruption is one recovery approach. If the disruption is isolated to your company, as would be the case in a fire or building collapse, market rates and availability might be acceptable. If the disruption is broader in scope, such as an earthquake or volcano eruption, market rates may skyrocket while availability may plunge. In some cases, availability may go to zero, regardless of the price you're willing and able to pay. Some of the challenges of this approach are the risk of availability, the risk of cost, and the risk of implementation. If you clearly detail out your *as needed* requirements and develop a plan with sufficient detail, such as vendor contact information, part numbers, technical specifications, and estimated costs, this may be a workable solution in some instances.

Preadranged

Preadranged options involve making arrangements in advance for the quick shipment or delivery of materials, supplies, and capabilities later. These types of arrangements typically involve a contractual agreement with a vendor to supply required systems, products, or services within an agreed upon time frame following a business disruption. There is often a cost to creating these arrangements or a charge above existing market rates built into the contract. For example, if delivering new IT systems is prearranged with a computer maker, there may be an up-charge over the existing market cost of the systems for fast turnaround, expedited or custom system configurations, testing, shipping, delivery, and setup. However, these would all be specified in the contract so that costs would be contained and would be known in advance. In addition, availability requirements are included in the contractual agreement so your firm is not subject to the vagaries of the open market in the aftermath of a major event. The risks are both financial and operational. As stated, you also need to have a very high level of confidence in your selected vendor(s) and well-written service level agreements (SLAs) to ensure your needs truly will be met in the event you need to activate these arrangements. Your worst case scenario is needing these services only to find out the selected vendor really can't deliver on its promises while you're in the middle of handling a crisis. And remember, a contract really defines what you're agreeing to up-front. If you have to invoke contractual terms during your crisis, you don't have a very solid vendor relationship.

Preestablished

Preestablished recovery options are those that are purchased, configured, and implemented prior to a disruptive event and are used only for recovering from a disruptive event. A company-owned alternate computing site that is activated only in the aftermath of a business disruption would be considered a preestablished recovery option. Often the

cost of this type of solution is lower on a per-unit basis because the expenditures can be timed and managed. However, the cost over time may be higher, depending on the cost of these preestablished options. For instance, if you purchase IT systems in the exact configuration of existing systems and have them stored at an alternate location in the event of an emergency, those systems sit idle until (and unless) there is a business disruption. Unlike working systems, these are non-production systems and are nonproductive expenses. There is also the risk that these systems will not be properly updated and patched to remain consistent with your current operational environment. Certainly, if your company experiences a disruption, the cost of these preconfigured, preinstalled machines is suddenly a good investment. If your company never experiences a disruption, the systems become outdated and useless. Never having been in production, they must, nonetheless, be upgraded or replaced periodically, leading to additional licensing, hardware maintenance, and support costs.

Note that there are options within this solution. We're really talking about having a cold, warm, or hot site. A cold site fires up from nothing; a warm site might be used for testing environments and other nonproduction needs to provide some ongoing value to the organization beyond what is required for BC/DR. A hot site can be used to load balance production services to ensure demand is distributed across your sites. This is a more complex solution but is highly desirable in organizations where availability is an absolute must (as in the case of large financial institutions, for example).

TIP**Keep Recovery Solutions Simple**

For IT systems, preestablished and prearranged solutions are often best. Trying to get IT systems acquired, shipped, set up, configured, and online in the aftermath of a business disruption is a major undertaking. Anything you can do in advance, within the constraints of your organization, will be well worth it if your company faces a disruption. You'll have to balance the cost of preparing against the cost of dealing with the aftermath. In some companies, this cost can't be justified. In larger companies, it almost always makes financial and organizational sense to make arrangements in advance.

Recovery time of options

Once you've developed your list of recovery requirements and options, you can look at the recovery time of each option. For example, borrowing space for your computers from another local company might be prearranged, and therefore, it could be implemented within a matter of hours. A co-location facility, if preestablished, potentially could be online within minutes of a business disruption. Buying new computers and setting them up in a temporary work location such as a local hotel conference room or mobile office unit is another option but it typically would take days to get that set up. Having defined the MTD for your critical business processes, you must now compare that data to the recovery time of the options you're considering. Any option that does not meet MTD requirements should be removed from further consideration at this juncture. In this way, only options that meet MTD requirements will be assessed in terms of cost and capability.

Cost versus capability of recovery options

You should have a pared down list of recovery options based on those that meet MTD and recovery requirements. Next, you'll assess the cost of each of the remaining options and list the capabilities included in that cost. Some options may have various levels of cost/capability. In most cases, the higher the capability, the higher the cost. Since all mitigation strategies will ultimately have to meet the company's financial constraints, these data are critical to making the right decisions for your company. The attributes that can and should be included in the cost/capability assessment are:

- Cost—the cost of the mitigation or recovery option.
- Capability—the capabilities of the option.
- Effort—the amount of effort it will take to implement and manage the option.
- Quality—the quality of the product, service, or data associated with the option.
- Control—the amount of control the company will retain over the critical business process.
- Safety—in cases where physical safety is a concern, this attribute rates the safety of the solution. If setting up a few braces on a faltering ceiling over the data center is among your recovery options, its safety attribute would be about zero compared to other options.
- Security—the estimates of physical and virtual (information and network access) security the option provides.
- Desirability—the assessment of the overall desirability of an option. In many cases, this is a qualitative judgment based on quantitative data. If so, the quantitative data should be included. The reasons for rating desirability as high, neutral, or low should be documented.

You can create a matrix to review these attributes and help you make sound decisions. [Table 6.1](#) shows a grid related to various options related to acquiring critical IT systems; [Table 6.2](#) shows options of establishing alternate computing facilities. These are two different approaches to mitigating risk, and as you assess these attributes, you can make decisions as to your best options.

Remember that these options are being considered only because they met the recovery requirements including time to recover. Therefore, they're all viable options at first glance. However, additional analysis is required to understand the particular needs of your company and the viability of these various options.

Recovery service level agreements

Any agreement you enter into for recovery services should include specific metrics such as time, cost, availability, response time, throughput, bandwidth, and so on. These metrics all fall under the category of SLAs and can include a number of different elements including:

- Response time to initial request for services
- Technical capacities—computer equipment specifications, storage space, voice and data capacities, speeds, bandwidth availability, test equipment, among others
- Access to recovery facility and equipment

Table 6.1 Example: Options for Acquiring Critical IT Systems

Option	Cost	Capability	Effort	Quality	Control	Safety	Security	Desirability
As needed	High	Unknown	High	Low	Low	N/A	N/A	Low
Pearranged	Medium	Meets requirements	Medium	Medium	Medium	N/A	N/A	Medium
Preestablished	Low	Meets requirements	Low	High	High	N/A	N/A	Medium

Table 6.2 Example: Options for Establishing Alternate IT Facilities

Option	Cost	Capability	Effort	Quality	Control	Safety	Security	Desirability
Company cold site	Medium	Meets requirements	Medium	Low	High	Medium	Medium	Medium
Outsourced hot site	High	Meets requirements	Low	High	Low	High	High	Medium
Public cloud	Low	Meets requirements	Low	Medium	Low	High	Medium	Medium

- Access to adequate work area and access for staff
- Security procedures and guarantees
- Processing controls
- Access to technical and functional support (time, response time, etc.)

Another important aspect to reviewing recovery SLAs is to look at any existing SLAs you may have with external parties such as your clients or customers. If you have contractual agreements to process data or ship orders within a specific period of time, you will need to review your recovery options in light of those contractual agreements. Although these SLAs should have been identified in your business impact analysis as critical business functions, it's good to take the opportunity here to ensure your risk mitigation strategies address your contractual obligations and, in particular, any SLAs that are currently in place.

REAL WORLD

Contracts Don't Guarantee Service

While you may do a great job defining and negotiating a contract, what really matters is your relationship with and trust in your selected vendor. A contract defines your shared understanding of roles, responsibilities, and obligations, but if you have to pull it out to get the other party to perform, you have a problem. In the midst of a serious business disruption or disaster, the last thing you need is a tug-of-war over contractual obligations or terms. Be sure you develop a solid relationship with vendors you can trust in the event of a disruption. It really can mean the difference between success and failure.

Review existing controls

In some cases, you may already have all or part of these controls in place. For example, you might have a very robust data backup solution in place, and by adding an additional service or two, you can meet these recovery requirements fairly easily. The reason for reviewing these controls after you've reviewed your recovery requirements is because you want to be able to look at existing solutions with fresh eyes. If you were to begin by examining existing solutions and try to fit them into your recovery options, you might have a built-in bias toward existing solutions. This is especially true if you were the one who championed or implemented the solution or if you happen to know that it was a very expensive, high-end solution. To avoid these natural biases, it's best to review your recovery options first then compare the optimal solutions to existing solutions. In some cases, you'll find that existing solutions meet requirements. In other cases, solutions might actually exceed requirements. Finally, you will undoubtedly find areas where existing solutions do not meet requirements and you'll need to address these areas.

If you find that you have solutions in place that address various recovery requirements, be sure to include these in your risk mitigation strategy document. As stated previously, this might be an opportunity to show the value of a previous investment or at least to show how an existing investment is serving dual purposes. In addition, you want to include these existing solutions in your risk mitigation strategy so that

you keep these systems in mind as your systems and BC/DR plans change over time. For example, if you have a solid backup solution that is part of your risk mitigation strategy, that should be noted so that if you decide in the future to modify your backup strategy, you can evaluate the impact on your BC/DR plan. You may have a checklist (on paper or just in your mind) of things you consider when you look at technology investments—speed, compatibility, cost, security. Be sure to add BC/DR to your list so that any future investments can be evaluated in light of BC/DR requirements as well. Anytime you can operationalize your BC/DR solutions, you have a greater chance of making maximum progress at minimal cost. In some organizations, gaining approval for large undertakings can be so onerous that some IT staff just stop trying. That's an unfortunate cultural problem to overcome, but one that can be addressed through making incremental changes and improvements through the provisioning process.

TIP**Dragging Dead Weight**

Leverage existing assets, processes, and procedures to the greatest extent possible, but don't be afraid to rip a solution out by the roots if it doesn't meet your immediate and long-term needs. Don't continue to support a failing (or failed) solution just because no one wants to be the one to terminate it. This BC/DR planning process can help you identify areas for improvement. It may also provide you with the financial and organizational support you need to update legacy systems that have outlived their usefulness.

DEVELOPING YOUR RISK MITIGATION STRATEGY

The steps in developing your risk mitigation strategy are as follows:

1. Gather your recovery data.
2. Compare cost, capability, and service levels of options in each category.
3. Determine if the options remaining are risk acceptance, avoidance, limitation, or transference and which, if any, are more desirable.
4. Select the option or options that best meet your company's needs.

Now that you've gathered these data on various recovery options, you can review them in relation to cost, capabilities, and service levels.

These data can now be compiled into a document in whatever format is suitable for your needs. Some people like to use a grid or matrix, and others prefer an outline format. The key is to create a highly usable document that delineates the choices you've made. Let's look at two examples. In our first sample, we look at a small segment of data that might be included with regard to backups. This uses a grid or matrix style, and it should give you an idea about what data to include and how you might approach it. In our second sample, we'll use text without a grid, so you can compare which method might work better for you.

Sample 1: Section from Mitigation Strategy for Critical Data

Category Selection	Option	Cost, Capability, SLAs	Risk Mitigation
Data backup—frequency	Continuous	Expensive, zero downtime, exceeds MTD	Potential solution, depending on cost to implement
	Daily	Moderate, up to 8 hours of potential lost data, 3 hours to restore, meets MTD	Implement daily backup process to reduce likelihood of significant data loss and to reduce recovery time to meet MTD
	Weekly	Moderate, up to 5 days of potential lost data, 12 hours to restore, may meet MTD	
	Monthly	Low, does not meet MTD	
Data backup—type	Full	Longest backup time, shortest recovery time, meets MTD	
	Incremental	Medium backup time, longest recovery time, exceeds MTD	
	Differential	Medium backup time, medium recovery time, meets MTD	Differential backup meets MTDs at the lowest cost
Data backup—method	Tape backups	Longest recovery time, least expensive, may not meet MTD	
	Electronic vaulting	Long recovery time, somewhat expensive, may not meet MTD	
	Data replication	Medium recovery time, medium expense, may meet MTD	
	Disk shadowing	Fast recovery time, medium expense, may meet MTD	Based on cost constraints, this option may meet MTD. This and disk mirroring will be explored in terms of cost, time, and feasibility
	Disk mirroring	Fast recovery time, medium expense, may meet MTD	Based on cost constraints, this option may meet MTD. This and disk shadowing will be explored in terms of cost, time, and feasibility

Continued

Category Selection	Option	Cost, Capability, SLAs	Risk Mitigation
	Storage virtualization	Fast recovery time, high expense, removes localized failure risk, meets MTD	
	Storage area network	Fast recovery time, higher expense, removed single point of failure, may remove localized failure risk, meets MTD	
	Wide area high availability clustering	Fast recovery time, higher expense, removes single point of failure, may remove localized failure risk, meets MTD	
	Remote mirroring	Continuous availability, zero recovery time, highest expense, removes single point of failure and localized failure risk, exceeds MTD	

Sample 2: Section from Mitigation Strategy for Critical Data

Critical Data Recovery Options (*selected choice is underlined*)

1. Data backup frequency
 - A. Continuous—expensive, zero downtime, exceeds MTD. Not suitable due to cost.
 - B. Daily—moderate, up to 8 hours potential lost data. 3-hour recovery time.
Meets MTD. Best choice based on cost and time factors.
 - C. Weekly—moderate, up to 5 days lost data, 12 hours to restore, may meet MTD. Although cost is acceptable, the recovery time for this option just barely meets MTD and does not provide any leeway. Therefore, this option is not as suitable as daily.
 - D. Monthly—low cost, does not meet MTD. Not suitable due to time.
2. Data backup type
 - A. Full—uses the fewest tapes, takes the most time to back up, least time to recover, exceeds MTD. Not suitable due to time to back up.
 - B. Incremental—uses moderate number of tapes, takes less time to back up than full, moderate time to recover. Just barely meets MTD. Not suitable due to time to recover.

- C. Differential—uses moderate number of tapes, takes less time to back up than full, takes less time to recover than incremental. Meets MTD. Suitable due to time and cost.
- 3. Data backup method
 - A. Tape backup—longest recovery time, least expensive, does not meet MTD.
 - B. Electronic vaulting—longer recovery time, somewhat expensive, may not meet MTD.
 - C. Data replication—medium recovery time, medium expense, may meet MTD.
 - D. Disk shadowing—fast recovery time, medium expense, may meet MTD.
 - E. Disk mirroring—fast recovery time, medium expense, may meet MTD.
 - F. Storage virtualization—fast recovery time, high expense, removes localized failure risk, meets MTD.
 - G. Storage area network—fast recovery time, higher expense, removed single point of failure, may remove localized failure risk, meets MTD.
 - H. Wide area high availability clustering—fast recovery time, higher expense, removes single point of failure, may remove localized failure risk, meets MTD.
 - I. Remote mirroring—continuous availability, zero recovery time, highest expense, removes single point of failure and localized failure risk, exceeds MTD.

As you can see from both examples, you may need to do additional research before deciding on the right backup method for critical data. It's clear that a weekly backup scheme might work, but the problems inherent in a local backup process might not be acceptable. You can also see from the data that while a weekly differential backup strategy might be acceptable, disk mirroring is also an option. In some cases, these two backup objectives might be at odds, might be redundant, or might not make sense for your organization. Once you've looked at these data, you can determine the best risk mitigation strategy for that business function and, ultimately, for your entire business.

Your final strategy might be to set up disk mirroring and perform weekly backups of data that are sent to a remote data storage vault. This reduces your recovery time if something happens to a disk (mirroring) and also protects you if you have a fire in the building that destroys all disks. You should include a section to your Critical Data Recovery Options called "Selected Strategy" and delineate the exact strategy you select. When you move into writing your business continuity and disaster recovery plan, you'll have the information you need in order to begin implementing these strategies. Avoid having to review this material at length a second time by including enough information so that the rationale behind the selected strategy is clear.

Remember, too, that when you're selecting your strategy, you should consider risk controls already in place and attempt to build on, rather than replace or circumvent, those solutions. There may be some cases where you want to completely revamp your approach and this is the place to make those decisions. In other cases, you may simply confirm that you're covered in these areas. For example, you may

already have disk mirroring and remote data backups in place. If so, you should have looked at your MTD, cost, and capability requirements and determined that these solutions are acceptable. Make a note of that finding. Later, when you're looking at your BC/DR plan, you don't want to have to go back through all these steps to determine if you used due diligence in making this decision. If something goes wrong down the line, you will also have documentation to show that you used a logical and accepted methodology for making these decisions. These data may also be used as the start of an after action review if things go wrong, so it's helpful to have it fully documented so your root cause analysis begins with documented facts.

For each critical business process, you need to identify an associated risk mitigation strategy. Some strategies will cover more than one critical business process, so you should not end up with as many strategies as you have critical business functions and processes. For example, your data management strategies will cover many of your critical business processes. By assessing these data with the big picture in mind, you can find areas where risk mitigation choices can cover more than one critical area. If you were to look at these strategies area by area only, you might miss opportunities to generate some *economies of scale*, which come from being able to apply one solution to many problems. These solutions become less expensive when they have more than one use. As mentioned earlier, any time you can use a solution across multiple business functions, you have a stronger business case for the expenditure. If you implement a remote data storage solution that meets data availability requirements for normal day-to-day business and it also meets your business continuity and disaster recovery needs, you're going to find more support for the cost and implementation of such a solution. At the very least, you'll be able to make a stronger business case for the investment.

PEOPLE, BUILDINGS, AND INFRASTRUCTURE

We're including this as a separate section because depending on the nature of your business, you may not yet have addressed these elements. In looking at the business impact, for instance, you may have dealt with critical business functions, but you may not have addressed the impact to people, to buildings, or to other infrastructure. These may or may not be part of your organization's overall risk management plan, so your job is to ensure there are no gaps. In addition, your overall risk management plan may not deal with IT specific needs effectively and you may need to supplement with IT specific plans. For example, your company may have a plan around what to do if buildings are impacted (broken water main, electrical problem, HVAC issues, etc.), but they may not specifically deal with the impact to your IT department, the data center, or your staff's ability to manage systems, infrastructure, and applications. In these cases, you need to develop auxiliary plans that address your IT department's specific needs.

If there is a business disruption, your company may have very specific needs related to people—staff, contractors, vendors, or the community. Some of these

may already be addressed in your organizational or IT risk management plan. For example, in the aftermath of a natural disaster, people need ready cash so they can buy food, medical supplies, and other immediate needs. If your company is located in a rural area where access to banks and ATMs is limited, you may want to ensure that your recovery plan includes being able to cash paychecks for employees or advance them cash against future paychecks. That may already be covered in your critical business functions under payroll, but it's a good idea to think through this again to ensure you have covered all your bases. This is not specifically an IT responsibility. However, as a leader in your IT department, you should be looking beyond your own borders to ensure that all organizational impacts you are aware of are reviewed and addressed.

In addition, there may be other areas that should be addressed in risk mitigation related to people. For example, fire drills are risk mitigation strategies that are useful not only for fires but also for other types of emergencies that require people to evacuate the building in a safe and orderly manner. Keep this in mind as you devise your risk mitigation strategies.

What other risks can be mitigated for people, buildings, and infrastructure? You might have a landscaping company come out and remove all trees, bushes, and grasses that are within 50 feet of the building if you are situated in a place prone to wildfires. That would be a risk mitigation strategy related to the building and infrastructure that might not show up because it's not a critical business function.

You might go back through your risk assessment and see if there are any elements related to people, buildings, and infrastructure that have not yet been addressed in terms of impact or mitigation. Add these to your assessment process here. Remember, too, that sometimes doing nothing (risk acceptance) is an acceptable solution as long as it is an active decision based on research and consideration and not just a passive default position.

IT RISK MITIGATION

We've discussed business impact and risk mitigation extensively. Now, let's turn our attention to the specifics of IT risk mitigation. Although the technology you use in your company will change over time and may not be the same as that discussed here, this section should give you a solid start to develop a risk mitigation strategy for your IT systems. For additional IT-specific risk mitigation strategies, be sure to read the Industry Spotlights found elsewhere in this book.

Risks to your data include not only the natural disasters we went over earlier in this book, but data disruptions and outages due to data center outages (fire, power, etc.); hardware or software failures; network security breaches; data security breaches that can include lost, stolen, modified, or copied critical data; and disruption due to critical data not being available to legitimate users (Denial of Service attacks, malware, etc.). Your risk and impact assessments should have covered these areas, and this is a good time to check to ensure all your data risks are addressed.

TIP**A Few Best Practices to Consider**

When reviewing your risk mitigation options and developing your strategy, consider using end-of-life or lower costs servers for less critical data. Also look at a reduced recovery footprint. In many cases, after having examined the entire array of organizational needs, the IT department responds by trying to meet all these needs. Instead, look at what is really required to get back up and running and attempt to develop the smallest, simplest plan possible. Also, build BC/DR into your IT lifecycle processes so that you evaluate the impact to BC/DR in a more operational manner. This will help ensure that risk assessment and mitigation become a part of the fabric of your business rather than an out-of-cycle process you need to manage.

Critical data and records

Through looking at your MTD and the cost of disruptions (lost productivity, lost revenues, etc.), you have a solid understanding of the impact a loss of various critical data would have on the organization. If you don't yet have this understanding, you should go back through the risk, vulnerability, and impact assessments with an eye toward critical data and records to determine where your critical data are stored, who generates them, what they do with them, and what they would do without them.

In addition, you should assess legal and regulatory requirements related to critical data, whether this is personal medical data, personal financial data, or other data impacted by regulations, statutes, and laws. If you've been addressing this type of data for some time in your IT department, you may have the solutions in place to meet existing regulations. However, regulations frequently change, so it would also be wise to consult with your legal counsel to determine if there are new or upcoming regulations that have (or will) impact your organization. These should be included in your assessment, if possible, so that you can develop a comprehensive data management plan within the scope of your BC/DR plan. Finally, you should review all existing controls as well as your proposed solutions in light of disaster recovery and business continuity. In some cases, your risk mitigation strategies might appear to be acceptable, but when you begin running through possible disaster or disruption scenarios, you discover that your strategies have a few holes in them. If you find you are covered, then you can be confident your BC/DR plan will meet your data needs. If you do discover some gaps, you can be relieved that at least you found them now and not in the aftermath of a disaster. At this juncture, you can look at potential solutions to address any gaps you discover between your existing data protection/data recovery solutions and those needed for BC/DR needs.

Critical systems and infrastructure

Once you understand your data management and data protection needs within the scope of the BC/DR planning process, you can begin to evaluate hardware and software solutions, vendors, and costs. There is no magic solution that will cover all your needs and if you've been working in IT for any length of time, you already know that

painfully well. However, if your analysis reveals gaps in your coverage, you'll need to look at various methods of addressing those gaps from rip-out-and-replace to patching existing systems.

If you can identify hardware, software, and vendors that can meet your needs for the next 3 to 5 years, you'll be doing well on the planning horizon. Don't try to build a solution that will last for 10 years; you'll waste time and money looking for the perfect solution. Instead, look for a solid solution that meets your data management, data security, and data recovery requirements now and into the next few years. Then evaluate the cost to acquire, implement, and manage the solution. You'll have to make a few compromises, as you know, but if you have your data constraints and budget as known variables, you can devise an acceptable (or even optimal) solution that fits within those parameters.

REAL WORLD

Leveraging Existing Assets

One approach to keep in mind throughout this planning process is your ability to leverage existing assets. That doesn't just mean looking at existing solutions to see if they meet your MTD objectives. It also means looking at assets and how they're deployed throughout their lifecycle. For example, as servers or storage platforms age, they may be suitable candidates for lower priority BC/DR solutions. Can they be relocated to a remote site and used for a backup solution? Looking at aging assets with an eye toward repurposing can, in some cases, be an effective use of depreciated capital assets. That said, be careful that you don't just "kick the can down the road" and put decrepit solutions in place for BC/DR only to have them fail when needed in a disaster.

Reviewing critical system priorities

Through your business impact analysis, you should have developed an assessment of critical IT systems that includes a prioritization of assets. For example, you might have found through your assessment of critical business functions that these IT assets have the following priorities:

- Virtualized Server Cluster—High
- Internet access—High
- E-mail access—Low
- Storage Area Network—High
- CRM application—High
- Inventory management enterprise application—Medium
- Financial systems—Medium

Based on these assessments, you should review your risk mitigation strategies to ensure that they meet or exceed your requirements for recovery based on these priorities. Dependencies between systems, especially those deemed as high priority or mission critical, should be reviewed. There might be a preferred or required order for restoration of systems after a disruption that should be addressed in the risk mitigation strategy. For example, if it's critical to restore the virtual server cluster before the

CRM application because the CRM app requires authentication data from resources residing on the virtual server cluster, this should be part of the risk mitigation strategy. Later, this will be included in your specific data recovery plans, but it is in this segment (and perhaps in the business impact analysis) where these dependencies are identified.

BACKUP AND RECOVERY CONSIDERATIONS

We're assuming that as an IT professional, you're well aware of various backup and recovery options, both those your firm has implemented and those you've learned about in the marketplace. In this section, we're going to cover some common backup and recovery options so that you can review your risk mitigation strategies in light of these options. This may help you see options you had overlooked or forgotten about; it might bring to light new options you had not considered. We won't go into a lot of detail about these alternatives, but we will provide a quick look at them to help ensure you have the best risk mitigation strategy possible given your current technology, organizational constraints, and budget.

Alternate business processes

Your risk management assessment data should already contain your key business processes and alternate methods (workarounds) for handling these processes during a business disruption, whether that disruption is to the IT systems, the building, or the surrounding area. We've covered a lot of this material, so this section is just a quick reminder in case you have overlooked any of these areas that may be relevant to your business operations.

Customer service. During a disruption or emergency, it's vital to most companies to still have the capability to provide support or customer services. Depending on the nature of the work your company does, this may be one of your most critical business functions. IT should clearly understand which technologies are required to deliver acceptable levels of customer service during a business disruption and what alternatives might be sufficient in the short term.

Administration and operations. We've focused on these activities in [Chapter 5](#) in great detail, so we won't cover them again here. You should have detailed documentation on the key business administration and operations processes for your business. These details should be at the heart of your risk mitigation strategy development. You should be challenging your counterparts across the organization to give serious thought to what options they have if key electronic systems go down.

Key business information and documents. Most businesses rely heavily upon electronic data of all kinds—e-mail, text documents, reports, and presentations, among others. Data essential to ongoing operations should be identified so that IT mitigation strategies can be developed. In addition, strategies for dealing with less critical data in the absence of key IT systems should be developed. You might decide,

for instance, that certain data must always be available so a continuous availability solution will be implemented. Other data are essential but not mission critical. For that data, you may develop a fast-track recovery solution.

Essential equipment. Other equipment essential to ongoing operations should be looked at in terms of how disruption of IT and non-IT systems may impact the availability of equipment. In some companies, IT systems run manufacturing, order fulfillment, or other operations-oriented equipment. How will the disruption of business impact these systems? How will the disruption of critical IT systems impact these operational systems? What can be done to reduce the risk to these systems?

Premises. We've discussed fire drills as a way to reduce the risk of injury or death to staff in the event of a fire or other building disaster. In addition to fire drills, there may be other ways to reduce risks to the premises. Insurance is certainly part of the equation, but fire inspections, emergency lighting, annual inspection of data center fire risk and fire suppression systems, and other emergency systems can be put in place to protect the premises and employees.

IT recovery systems

You're undoubtedly familiar with many IT recovery systems, but as part of your risk mitigation strategy development, you should scan the technological horizon to see what's available in today's market. Sometimes IT departments develop risk management strategies based on current technology and never update those strategies. Systems put in place 5 years ago that are not reviewed and updated can inject additional risk into your organization, and put your BC/DR plan at risk. Clearly what was innovative 5 years ago may be close to being a legacy system now. What was extremely expensive 3 years ago has probably dropped in price significantly. Revisit your technology solutions with an eye on what's available in the marketplace today. You might decide to upgrade, replace, or supplement existing solutions. The list included in this section is not exhaustive but should spark thoughts about solutions to consider. Be sure to do some independent research to supplement these data so that you have a comprehensive and current look at your IT recovery options before developing your mitigation strategies.

Alternate sites

The largest decision you'll need to make is whether or not to develop alternate sites. You can have a dedicated site wholly owned by your company, you can create a reciprocal agreement with another division or company, or you can go to an external vendor for a commercially leased facility. Let's look at the most common options.

Fully mirrored site

Mirrored sites are fully redundant sites that mirror everything going on in the live site. This is by far the most expensive and extensive IT risk mitigation strategy. For some companies, this solution might make sense. Mirrored sites provide the highest degree of availability (and therefore risk mitigation) because every

transaction that happens on the live site is also processed on the mirrored site simultaneously. Sometimes a solution implemented for load balancing purposes may also serve as a risk mitigation solution. For example, if you have two mirrored sites so that users can access data quickly, it might be that this same configuration works well in the event that one or the other site goes down. Certainly, user access to data will slow considerably if one of the sites goes down, but the transactions can still occur while the initial site is being repaired. Mirrored sites typically are owned and managed by the company, which can reduce the cost of implementation.

Hot site

A hot site is usually a site leased by a commercial vendor to your company for emergency purposes. The vendor will guarantee an identical technical configuration with communications that allow you to switch your IT operations to that commercial site within a specified time frame, usually within 1-4 hours. These sites typically provide enough space for hardware, supporting infrastructure (racks, cables, phones, printers), and support personnel. This is sometimes less costly than a fully mirrored site but that depends on your technology and response time needs.

The primary difference between a mirrored site and a hot site is that in a hot site, you may not have an identical configuration as your primary site. For example, you may only replicate Tier 1 services to a hot site. You may choose to have core functionality available at the hot site but not run in parallel choosing instead to use your hot site only in the event of an emergency. Typically what drives the decision about using mirrored vs. hot sites are the number of interfaces and the complexity of data exchanged between systems. Replicating interfaces to up- and downstream systems in a hot site can be challenging and a mirrored site that's always up and running is one way to address that challenge. These are just a few ways you can leverage mirrored or hot sites.

Warm site

Warm sites are partially equipped premises with some or all of the required equipment. Warm sites are often sites used during normal operations for less critical functions that are taken over for critical IT functions during a business disruption. For example, you might have a site located in your primary location and a second site in a remote office or satellite building. You might keep a server at the remote site configured with your critical business applications with Internet access to backup data. In the event of a business disruption or disaster to the primary site, the secondary site could fire up the server, restore from the most recent backup, and resume critical operations within a matter of hours. Some organizations use their warm site for Tier 1 only, other use it for Development, Test, and Training regions with production data simply being backed up to that location.

Mobile site

Mobile sites are self-contained units that can be transported to establish an alternate computing (or working) site. These often are contained within a mobile trailer that is delivered by truck to a specified location. Commercial vendors lease these types of

units. Due to the time and expense of configuring a mobile site, these arrangements should be preestablished far in advance of anticipated demand.

Cold site

A cold site is started up “cold” in the aftermath of a disruption. These kinds of sites are the least expensive in advance of an emergency but take the longest to bring online after a disruption. If your recovery needs are more than 3 or 4 days out, this might be the most cost-effective solution for you. However, your BC/DR plan should include plans for how and where you could establish a cold site should you select this option. Trying to come up with these arrangements in the aftermath of a disaster or serious disruption will be far less effective than planning in advance. That might mean identifying facilities in your area that could host a cold site, understanding how your communications needs would be met, and how you’d furnish and staff this site. Finally, you would need to document your hardware specifications, copies of applications, configuration files and detailed documentation on how to configure and test these systems. This documentation must be readily available in the event of a disruption or disaster.

Reciprocal site

You may be able to make arrangements with another company or another division of your company for use in the event of a significant business disruption. For example, you might make arrangements with another company in your area for reciprocal assistance in the event that one of your businesses is disrupted. However, if a natural disaster hits the area, it’s possible both companies will be impacted, so you need to assess the risks of such an arrangement. If you can create an arrangement with a firm outside your geographic area, you’ll reduce the localized risk. Remember, however, to create solid agreements with plenty of detail delineating how, when, where, and at what cost these reciprocal arrangements will be implemented. You don’t want another company disrupting your business for minor problems, and the use of these arrangements should be very clearly defined. That said, this type of arrangement might make sense for small businesses that can’t afford to contract with commercial vendors for alternate sites.

Storage and disk systems

Disk systems solutions continue to evolve in terms of capabilities. In today’s market, there is a blurring of lines between modular disk arrays and monolithic frame-based arrays. Though Network Attached Storage and Storage Area Networks have been around for over a decade, it’s only been in the last decade that storage vendors have added multiprotocol support to their solutions. Some offered block-level Internet SCSI (iSCSI) a while ago; others offer block-based Fibre Channel. More recently, there is a move toward Unified Storage. We’re seeing file-level storage protocols (NFS and CIFS, for example) being used in the virtualized server environment in order to reduce provisioning and recovery times. In addition, enterprise storage vendors have been adding application programming interfaces (APIs) into their systems

in order to better integrate with server operating systems and hypervisors, improving backup and recovery operations. The convergence of storage, server, and network capabilities is continually blurring the traditional lines of service. While this creates both opportunities and challenges for IT departments, it is an area that must be thoroughly assessed during your BC/DR planning. If you have (or are developing) a technology roadmap, you have a head start on this analysis. If you are not yet looking down the road, this is the time to do so. While the landscape will continue to evolve, key trends are emerging with respect to convergence and unified platforms that will impact your decisions.

A thorough discussion of disk technologies is outside the scope of this book. However, understanding some of the current trends is vital to a successful forward-looking BC/DR plan. As such, you should spend time researching what's on the market today, where the market is headed and where your competitors are going with their infrastructure.

Desktop solutions

Your organization should already have some process in place for backing up user data. In the Microsoft Windows operating system, most users save data to the My Documents folder or to a designated network location. For enterprise applications, user data may be stored more centrally. Regardless of your configuration, it's important that critical user data be backed up periodically. Ideally, this process should be automated, so it does not rely on user compliance with established backup processes. Backups of user data should also be stored securely off-site. In your business impact analysis, you may have determined that there were certain job functions that required special attention. These computers should be flagged as critical and risk mitigation strategies for key user's computers should be developed.

Creating standardized file management processes will also assist in any recovery efforts (and therefore mitigate risk). For example, requiring users to store all important documents in their named folder on a network share can help reduce the likelihood of data loss, corruption, or breach. If users travel with laptops, be sure to establish backup and security procedures for mobile users.

If your organization has implemented Hosted Virtual Desktops, or Virtual Desktop Infrastructure (VDI), using PCs, laptops, thin clients, and zero clients, you need to give consideration to how your recovery strategies will roll out. In some cases, serving up the desktop with core applications from a remote location via the Internet is a fast and effective solution. In other cases, it could hobble your recovery efforts if there are no functional desktops or laptops available to begin recovery efforts (unlikely, but worth mentioning).

In addition to implementing backup and encryption policies and procedures, risk can be reduced through standardizing hardware, software, and peripheral equipment. Reducing the number of variables not only helps in day-to-day IT activities, it can significantly reduce recovery time after a significant event. Documenting hardware, software, and configuration data along with vendor contact information can reduce the risk of serious disruption should user systems be impacted. If you've virtualized

your desktop environment, recovery could be simplified by the ability to use that desktop instance on a wider array of hardware than a standard desktop image.

REAL WORLD

Lost and Stolen Laptops—It's Not Always About The Hardware

Laptops are lost and stolen every day. Sometimes a tired traveler leaves a laptop behind; sometimes a thief wants the hardware. Other times, the thief is targeting the information on the laptop. Lost and stolen laptops have been in the headlines recently because the data on them were sensitive and unencrypted. If you have users working with sensitive data, whether that's the company's strategic direction, corporate finances, personal health information, credit card numbers, or other private customer data, be sure that all data are encrypted and that the operating system requires user authentication. Even though there are ways around user access restrictions on stolen laptops, it should be impossible to overcome strong encryption. Although laptops will always be lost or stolen, the data on them doesn't have to fall into the wrong hands. Implement strong encryption on all laptops that deal with sensitive data and be sure users understand the importance of encryption. Ideally, the encryption system will work seamlessly in the background so the user doesn't have to take any special action to protect data. Anytime security measures can be automated, you'll end up with stronger security than if left to users to remember and employ.

Software and licensing

Software and license data must be backed up and stored in a secure off-site location along with data. It doesn't do much good to store the database information if the licensing data are lost. The licensing for each operating system, application, user, and desktop system should be captured and stored in a secure manner in the event of a partial or total disruption of business.

As a corollary to that, you also need to ensure that you address licensing considerations within your BC/DR plan. If you plan on developing a mirrored, hot, warm, or cold site, you need to clearly understand the allowances and limits of your current licensing structure. Some vendors have hard stops built-in, and some use soft stops and periodic audits. Some charge if you so much as turn on a feature, others allow low or no cost licensing for test, development, or DR solutions. Be sure you review licensing for your BC/DR technology solutions to ensure you don't inadvertently develop what ends up being a very expensive or limiting solution.

Web sites

There are two primary risks related to corporate Web sites. The first is the security risk due to the nature of external (public) Web sites. As you know, Web sites are like large neon signs saying to hackers "Enter Here." Risk mitigation strategies for Web sites include implementing strong security measures along with auditing and monitoring activity on the server. Documentation on the security and configuration settings for the Web site are important in the event the Web servers go down or in the event of a security breach. In addition, many corporate Web sites are used to conduct e-commerce transactions and the disruption of these transactions can have a significant impact on revenue streams and on customer perception of the company. Some

companies use load balancing strategies to ensure Web sites have high availability, and these same strategies also act as excellent risk mitigation strategies. However, if a Web site is breached or data are corrupted, it's possible these problems will be replicated to all virtual sites, so additional risk mitigation strategies may be needed.

Your company may have a robust intranet where a lot of technical documentation and knowledge is stored. Do you have backup and recovery plans in place for that data? What would be the impact if your intranet data were permanently lost? What if it was down for a month? Be sure critical system, storage, network, desktop, and application data are documented, periodically reviewed, and updated and stored in an accessible location in the event of a serious technical failure or catastrophic event. We'll discuss this in more detail in an upcoming chapter, but this is a good place to make a note and review your risk and mitigation strategies for internal operational data and knowledge.

REAL WORLD

Malware as a BC/DR Concern

Here's a recent real world example to underscore the criticality of a solid BC/DR risk assessment. An organization purchased a subscription to a Web site for knowledge management. The company used this site to upload required courses for staff as well as to store course data required for maintaining various types of professional certifications. The Web site became infected with malware and could have infected all end user computers that connected to the site. The company immediately blocked access to the site; notified users then notified the Web company. The Web company was unaware of the problem, and it took more than 24 hours to convince them they had a problem. Once they acknowledged the problem, it took them more than 14 days to remediate just one portion of the site. During that time, the subscribing company's staff could not take required courses for renewing critical certification. Some staff were at risk of not being able to continue to work legally as their certifications were at risk of lapsing. In this case, the IT department took two parallel paths. The first was to look for competing Web sites that offered the same certifications to see if they could quickly subscribe to another service. The second path was to set up several barebones laptops with cellular phone cards. They established connectivity to the site and tested to see if they could still take the courses (while the laptop was being infected by malware). This dual path enabled the organization to address end user needs quickly. Unfortunately, this scenario had never been part of any BC/DR plan. Instead, the company's Information Security Incident Response Team found the problem and worked to find alternatives. Was this a show-stopper? No. Should it have been part of the BIA? Yes. These are the kinds of external systems that are easy to overlook in your risk mitigation strategies, so be sure to look at your company's subscriptions to external Web sites to understand your risk and mitigation strategies in advance. This story ended well, but not all do.

Documenting Your Risk Mitigation Strategy

At the end of this process, you need to wrap this information up and document it. Ideally, you will document the results of your IT risk assessment and develop a document detailing your mitigation strategies. You may also need this information to be packaged up and presented to your risk management group, to your manager, the firm's CIO, COO, or CEO, or to a Board of Directors committee focused on audit,

compliance, and risk management. While you may have undertaken this activity in order to develop your BC/DR plans, you may also need to report out on your team's current state, risk management, and compliance activities and strategies. If you have done a good job documenting your analysis, decision points, and reasons for those decisions, documenting and presenting your data should be relatively easy. If you're presenting to leadership, be sure to document the mitigation elements already in place and highlight opportunities to improve the business through implementing BC/DR strategies. This is a key method for gaining needed support for your BC/DR activities (and expenditures), so take full advantage of the opportunity, if presented.

Finally, your risk assessment, business impact analysis, and risk mitigation documents are the foundation of your overall BC/DR plan, which we'll discuss in the next chapter. If you haven't completed these three foundational steps, your BC/DR plan is almost guaranteed to have gaps. Sometimes having a bad plan is worse than having no plan at all, so be sure you have these three aspects in place before proceeding.

SUMMARY

In this chapter, you learned about a process you can use to develop risk mitigation strategies for critical business and IT functions. The inputs to this process are the risk assessment data and the business impact analysis. The key steps in this process are developing recovery requirements, understanding the recovery time of the options under consideration, comparison of these times to MTD requirements, a review of the cost and capabilities of each option, the SLAs related to each option, and finally, the selection of the option to be implemented. This process is done for all critical business processes identified. An additional review should consider dependencies between processes, functions, and IT systems. As is often the case, one solution may address several key requirements. Your review of options should attempt to find the simplest, most comprehensive, and most cost-effective solution that meets your company's critical business needs now and into the near future.

KEY CONCEPTS

Types of risk mitigation strategies

- Risk acceptance is a strategy in which the company accepts the potential consequences of a given risk. The company chooses to do nothing to avoid, limit, or transfer the risk. Acceptance usually has a very low cost associated with managing the risk (or zero cost), but can have a very high cost in the aftermath of a disruption.
- Risk avoidance is a strategy in which the risk is completely avoided. This might include shutting down critical systems and moving them in advance of a hurricane. Avoidance takes the risk to zero but often has a high cost associated

with it. Therefore, the cost of managing the risk is very high but the cost of recovery is very low.

- Risk limitation is a strategy that falls in between acceptance and avoidance. Most companies choose a risk limitation strategy, especially for IT systems where complete acceptance or avoidance is too costly on either side of a disruption. Steps such as secure, off-site backups can go a long way in reducing various organizations risks without being too expensive in implementation or recovery phases.
- Risk transference is where the exposure to the risk is transferred to a third party, usually as part of a financial transaction. Purchasing insurance is the most common risk transference method, though others exist.

Risk mitigation process

- Recovery requirements are developed during the risk assessment phase and include data from the business impact analysis. You can begin by delineating the key functional areas of your company and determining the key business processes in each.
- Recovery requirements include the time and cost of recovery as well as any specific processes or procedures required by each functional area of the company.
- Recovery options are developed for each critical business process or function. Recovery options must fit within the constraints of the recovery requirement. Otherwise, they should not be considered as part of the BC/DR process.
- Recovery options usually fall into one of three categories: as needed, prearranged and preestablished. The cost and time to implement each type of option varies.
- After recovery options are delineated, each option must be reviewed in terms of the MTD for each critical business process. Any option that falls outside the MTD should be removed from further consideration.
- The cost and capability of remaining options should be compared. In some cases, cost will be more critical than capability; in other cases, capabilities are more important than cost.
- Determining the cost, capability, effort to implement, quality, control, safety, and security of each option under consideration can help you develop a comprehensive risk mitigation strategy that meets the needs of your company.
- SLAs are important when dealing with vendors in preestablished or prearranged contracts.
- SLAs may also pertain to agreements your company has with others that must be addressed in your plan. This might include customer service functions or other externally facing functions your firm provides to others.
- Existing controls and risk mitigation solutions already in place should be reviewed after requirements and options are reviewed. In some cases, existing solutions meet BC/DR requirements; in other cases, existing solutions can be augmented or expanded to meet needs. In still other cases, no satisfactory controls exist and a solution must be developed.

- People, buildings, and infrastructure are sometimes overlooked in the BC/DR risk mitigation phase. How will risks to people, buildings, and other infrastructure be addressed through your BC/DR plan? Many of these may have been considered during the threat, vulnerability, and impact assessment phases, and they specifically should be included in the risk mitigation phase.

IT risk mitigation

- Critical data and records should be viewed in light of risk mitigation strategies under consideration. There may be additional organizational, regulatory, or legal requirements for reducing risk to critical data and records that should be addressed as part of your overall strategy.
- Critical systems and infrastructure should be assessed to determine optimal solutions for risk mitigation. There is a wide variety of solutions available in the market today. You can select the optimal (or acceptable) solution for your business only after assessing your business's critical functions and specific needs.

Backup and recovery considerations

- There are numerous areas of the company that may require alternate business processes to be developed and/or available. These areas are sometimes overlooked in planning.
- Customer service, administration, essential equipment, and premises are four areas that require specific attention in your risk mitigation planning.
- IT recovery systems are numerous and include (among many others) alternate sites, server, storage and network virtualization, and more.
- User's desktop systems must be considered as part of the overall risk mitigation process. Different strategies must be employed when using standard or hosted desktop solutions.
- Software and licensing information should be stored in a secure, off-site location with backup data. Software license constraints for DR sites must be well understood.
- Web sites are external-facing connections to the company. As such, they require special security considerations and risk mitigation strategies.

References

ISACA. The risk IT framework. <http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/The-Risk-IT-Framework.aspx>; 2009 [Retrieved February 22, 2013], from ISACA.

This page intentionally left blank

Business Continuity/Disaster Recovery Plan Development

7

IN THIS CHAPTER

- Phases of business continuity and disaster recovery
- Defining BC/DR teams and key personnel
- Defining tasks and assigning resources
- Communications plans
- Event logs, change control, and appendices
- Summary
- Key concepts

INTRODUCTION

The bulk of your work in developing your business continuity and disaster recovery plan is complete when you get to this point. Granted, you may be reading this book through from start to finish before developing your plan (recommended) and therefore you will have none of the actual work completed. However, things move quickly in the business world and there are some of you who are doing the work as you read each chapter. Either way, this is where everything comes together. The risk analysis you performed led you into your vulnerability assessment. That data helped you develop an assessment of the impact various risks would have on your business. Finally, you took all your data and identified mitigation strategies—actions you could take to avoid, reduce, transfer, or accept the various risks you found. With that, you now have to develop a plan that takes your mitigation strategies and identifies both methods for implementing those strategies, and people, resources, and tasks needed to complete these activities.

In [Chapter 8](#), we'll go over emergency activities including disaster response and business recovery, so we'll refer only briefly to those elements in this chapter where appropriate. In [Chapter 9](#), we'll discuss training and testing and in [Chapter 10](#) we'll discuss maintaining the plan. All of these are elements that should be included in your BC/DR plan as well.

It's worth noting that there are many methods for creating your BC/DR plan. After all, the BC/DR plan is a defined approach for responding to disruptive and disaster events and resuming operations afterward, and there are many ways to implement those steps. However, the two primary purposes of creating the plan are (a) thinking through the risks and implications of a disruption and (b) ensuring

you have a logical roadmap to follow in the aftermath of such an event. If you have adopted the use of a framework such as ISO or COBIT, you can certainly use that methodology to guide you in the development of your plan. All BC/DR plans have common elements, which we'll discuss in this chapter. Frameworks help you move forward in a logical and comprehensive manner, so they are great additions to this work. If you are ever in a situation where you need to use your plan, you'll be glad that you took time to think things through in advance. Being able to follow a recipe-like plan reduces the stress of an already incredibly stressful situation and enables you to be more effective in your recovery efforts.

There are two essential parts to your plan. The first part is the set of tasks you can undertake to reduce your risks in advance of a BC/DR event. This may or may not be considered a formal part of your BC/DR plan, though in the framework we're presenting, it is part of the plan. Risk mitigation is an essential element of ongoing BC/DR planning and readiness. The second part of the plan are the steps you will take if a disaster or business disruption occurs. If you look at your BC/DR plan holistically, you can see that on one end of the spectrum you have risk mitigation and on the other end, you have disaster recovery. There is a continuum of possible events that can disrupt your business, and your BC/DR plan should be comprehensive enough to address events along this continuum.

We've included many checklists in the appendices to assist you with creating your BC/DR plan. There are many different ways to present the data from your analysis and planning activities; we'll present one and you can modify it to meet the needs of your IT organization.

Your BC/DR plan fundamentally needs to state the risks, the vulnerabilities, and the potential impact to each of the mission-critical business functions. For each of these, there should be associated mitigation strategies. In some cases, there will be multiple mitigation strategies; in other cases, you may have elected to simply accept the risk. However, all of this should be clearly laid out in your documentation thus far. Next, you need to determine how and when those strategies are implemented and by whom.

Your work breakdown structure (WBS) will look something like this:

1. Identify risks (*complete*).
2. Assess vulnerability to risks (*complete*).
3. Determine potential impact on business (*complete*).
4. Identify mission-critical business functions (*complete*).
5. Develop mitigation strategies for mission-critical functions (*complete*).
6. Develop teams.
7. Implement mitigation strategies.
8. Develop plan activation guidelines.
9. Develop plan transition guidelines.
10. Develop plan training, testing, and auditing procedures.
11. Develop plan maintenance procedures.

As you can see from this simplified list, you should already have items one through five completed. We'll discuss developing teams in this chapter as it relates to carrying

out the BC/DR plan, not the planning team that you should already have in place (and who hopefully have helped you accomplish tasks one through five). We'll cover developing plan activation and transition guidelines in this chapter before heading into [Chapter 8](#). At the end of this chapter, you'll have items one through nine complete (or will understand how to complete them when you begin project work).

As with previous chapters, we'll begin with a review of where we are in this process. As shown in [Figure 7.1](#), we have completed the risk assessment, the business impact analysis, and the risk mitigation steps.



FIGURE 7.1

Business continuity and disaster recovery plan development.

This next step is where you pull all the data together and develop your plan. Creating the BC/DR plan entails organizing all the decisions and data you've developed so far and adding a bit more detail. We'll walk through the creation of the BC/DR plan document in this chapter, but keep in mind you'll have to circle back later to add detail that we develop in upcoming chapters.

IMPLEMENT RISK MITIGATION STRATEGIES

This set of tasks is, essentially, a precursor to developing your BC/DR plan. As you've looked at your risk profile, your threat environment, and your business impact analysis results, you've identified steps you can take immediately to reduce or remove certain threats. A great example is creating a process for quickly testing and deploying antivirus and anti-malware software updates. This is a risk mitigation process that every company should be doing on a regular basis. If yours is not among them, this would be one of the first and easiest steps to take in reducing your risk profile. Similarly, reviewing firewalls for unnecessary open ports, reviewing log files, and setting up server patch processes are all steps that form the foundation of both solid information security practices and BC/DR. These are all risk mitigation techniques and should be undertaken as soon as you have completed your analysis and identified these gaps or areas for improvement. While you will still need to take time to develop your BC/DR plan, there is no reason to wait for the plan to be complete to take these fast and relatively easy mitigation steps.

Other common risk mitigation strategies, which may be appropriate for your environment based on current resources available, include, but are not limited to, the following:

- Ensuring separation of duties for personnel with elevated access permissions, and implementing separate, encrypted administrative password databases for different roles;

- Implementing physical security controls for all IT equipment, such as six-wall boundaries, locked doors, and video surveillance systems;
- Implementing password expiration policies and changing administrative passwords periodically or when staff changes occur;
- Implementing strong centralized password and authentication policies, such as with Microsoft Active Directory;
- Implementing a standalone computer not connected to the network for scanning all removable media, such as USB drives, CD-ROMs, or DVDs, for viruses or malware before they are used on the network;
- Consolidating and automating security log analysis with a Security Information and Event Management (SIEM) system or appliance;
- Backing up systems and data periodically to removable media and storing backups off-site, or backing up to a secure cloud, or Internet, provider;
- Maintaining spare IT hardware at an off-site location or contracting with a secure cloud, provider beforehand to be able to quickly spin up needed virtual servers or workstations in order to recover systems and data housed internally;
- Implementing automated IT hardware and environmental monitoring and alerting tools, such as Simple Network Management Protocol monitoring, for events such as failed disks, bad memory, temperature events, leak detection, fire detection, etc.;
- Formal documented training for all employees on basic IT security and disaster recovery procedures, typically as part of the employee on-boarding process or during annual training exercises.

REAL WORLD

Insider Attack

In 2011, a leading provider of IT cloud services in Virginia which provides IT co-location and IaaS/PaaS (Infrastructure as a Service/Platform as a Service) services for several hospitals and other large organizations was attacked repeatedly by a former employee over a period of weeks, resulting in multiple unplanned outages of critical IT services for several clients and subsequent loss of business, revenue, and reputation. The attacks were carefully planned by the former employee, who had been with the company since its inception 10 years earlier. The cloud IT services company had recently been acquired by a larger company that actively acquired smaller companies, but whose primary business wasn't IT. The new owner put in their own management, and the former employee in question, who had been part of a small team who had built out most of the company's infrastructure since its inception, wasn't fond of the new nontechnical management. Equally, he wasn't happy with the fact that his suggestions were often dismissed and his responsibilities were reduced. Disgruntled, he left the company shortly after the acquisition and took all the administrative passwords with him. The cloud IT services company had very few employees, and the employees had all been with the company for a long time, so they did not have any strong procedures for creating separate administrator roles or changing all passwords when an employee with elevated privileges left. When the company was acquired, the new owners and management, who were not skilled in basic IT security practices, failed to recognize they had this significant threat on their hands. Moreover, the former employee had critical knowledge of IT operations, and when he left, there were no employees remaining that were sufficiently cross-trained.

Continued

REAL WORLD—cont'd

Over a period of weeks and months, the former employee would remotely access critical systems he had built at the IT cloud services company and selectively take down a system, covering his tracks each time. He would then open up a chat session with former employees, many of whom were folks he hired and had stayed in contact with, and would ask how things were going. When they would tell him that systems went down unexpectedly and clients experienced loss of service, he would offer “advice” to help expedite service recovery. Employees working at the small company were blindsided by what was occurring, and they worked for weeks, as repeated attacks occurred, to try to figure out what was happening. Each time, the former employee was able to successfully cover up his tracks and avoid detection.

Unbeknownst to the former employee, the company had contacted a security services firm after multiple unplanned outages, suspecting that they had a security breach. The outside firm secretly monitored all traffic coming in and out of the facility, and they finally caught the former employee in the act. The former employee had been logging on with shared administrative credentials, still in use by current employees, and with each subsequent chat session opened up with the current employees, he would send the transcript of the chat session to his new e-mail address via his old company's e-mail servers, apparently taking pride in his successful hack attempts. The security services firm was able to identify these abnormal e-mails, their timing, and their contents, squarely implicating the former employee. The new owners then passed this evidence onto the FBI, who performed a search warrant on the former employee's house soon after, in the wee hours of the morning while he, his wife, and his newborn were sleeping. The FBI confiscated all of his computer equipment and removable media (including his home DVR system, even), and his day in court was set.

At the time the search warrant was executed, the former employee had taken a job at another company working in an IT department where he had high-level administrative privileges. He had passed a background check at his new company and was working with critical IT systems which controlled critical infrastructure. His new employer had strict role-based access and separation of duties procedures, as well as separate encrypted password databases for each IT support team. His new employer got word of the search warrant, only because one of the items confiscated by the FBI that morning was his work mobile phone issued by his new company. The new owners contacted his current employers and gave them all the information they had. The employee was soon put on administrative leave that same day, and his new employer immediately disabled his access and changed all administrative passwords he had access to. They then brought in their own security services to examine his work computer and scan all servers he had access to. After a week on the job scanning hundreds of systems, questioning staff, and charging tens of thousands of dollars, they produced a report showing a low risk of any security backdoors or new internal threats caused by the former employee. Additionally, they pointed out that the security controls his new employer had in place were very successful at containing the threat, once it was known, and significantly reduced the company's risk profile for insider threats.

The moral of this story is that insider threats are one of the highest risk vulnerabilities often overlooked by companies of all sizes. Insider threats should be evaluated as continually having a high likelihood and high impact, and additional risk mitigation strategies, such as background checks, separation of duties, encrypted password databases, processes for quickly changing passwords and disabling access, and SIEM, should be employed to reduce this risk to an acceptable level.

Throughout this book, we've mentioned the usefulness of operationalizing many of these BC/DR activities. When they are built into everyday processes and practices, you continually focus on the most common areas of vulnerability. The BC/DR plan can be primarily focused on recovering from a disruption, as minor as a broken

sprinkler head in a relatively unpopulated area of the data center, to a disaster like a hurricane, earthquake, insider attack, or fire.

Figure 7.2 depicts the risk profile of your company over time when you implement both operational risk mitigation strategies and disaster recovery plans.

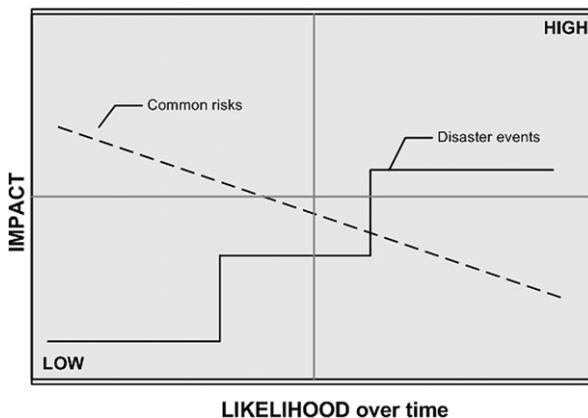


FIGURE 7.2

Risk mitigation tasks and disaster recovery tasks.

As you can see, your highest risks, initially, are related to threats where exploits are commonly known or where likelihood of occurrence is continually high. For example, if you move to a new home, threats such as theft or fire may be continually high from day one. Therefore, you may change the locks, install fire detectors, install a security system, and/or change the garage door remote code, in order to keep intruders out and notify you quickly of a security breach or fire. These preventative measures are relatively easy to implement and inexpensive, and they provide one or more layers of protection for the more common threats. Similar operational risk mitigation items that should be addressed quickly in any IT shop include automating antivirus updates, implementing ongoing security patch management, installing and monitoring firewall and perimeter defenses, and the like. As you add these to operations, often referred to in Lean circles as standard work, you incorporate them into the DNA of your organization and your risk of more common threats occurring over time is reduced to consistent reasonable levels. This chart is NOT a likelihood/impact chart we depicted in our business impact analysis phase. This diagram shows how the likelihood of different threats changes over time and how to prioritize risk mitigation tasks for such threats. Disaster events, in contrast, are often outside of your direct control and are therefore not influenced by many of the common risk mitigation strategies you might take. A clear example is that the impact of an earthquake or flood is not changed by whether or not you have patch management in place. Since the likelihood of a disaster occurring increases with time, it is important to plan for one and, in doing so, enhance your long-term risk mitigation strategy. When a disaster occurs, ongoing planning efforts can limit the impact to your operations,

and lessons learned after recovery can be incorporated into your daily operational tasks in order to further limit the impact of future disasters. The goal is to reduce the impact of each threat to reasonable levels based on likelihood and timing. It's important to understand what steps you can take immediately and how they impact your overall risk profile versus plans you need to make for future potential events. They're not at all the same but they do require planning throughout the continuum.

Risk mitigation of common operational elements should be underway as part of your day-to-day work. If it's not, it's worth pausing briefly in your BC/DR planning activities to take a look at some quick and easy wins on this front. By implementing a change management process, separation of IT administrative duties, a patch management cycle, or an antivirus updating schedule, you'll be addressing the more common risks quickly and effectively. Going forward in this chapter, we'll focus on the larger disaster recovery elements and we'll assume you've taken care of the operational items along the way.

PHASES OF BUSINESS CONTINUITY AND DISASTER

Given today's threat environment, it's becoming more likely for businesses of all types that you will have to activate at least a portion of your BC/DR plan at some point. Hopefully you'll never have to activate a full-blown BC/DR plan, but if you follow these fundamental steps, you'll be better prepared in any event. Let's begin with a quick look at the phases of the business continuity and disaster recovery plan, as shown in [Figure 7.3](#): activation, disaster recovery, business resumption or business continuity, and transition to normal operations.

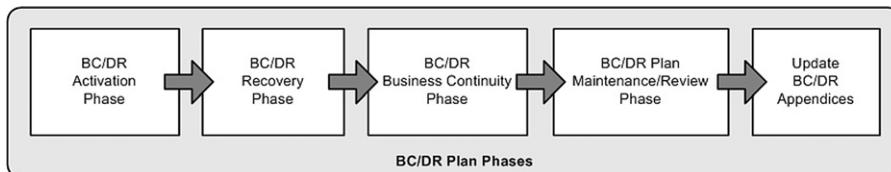


FIGURE 7.3

Phases of business continuity and disaster recovery.

Activation phase

The activation phase of your BC/DR plan addresses the time during and immediately after a business disruption. In this section of your plan, you need to define when your BC/DR plan will be activated and in what manner. You don't want to activate your plan for every little glitch your business runs into, so you'll need to develop a clear set of parameters that you can use to determine if or when to activate your BC/DR plan. In addition, you will need to define how your plan is activated, including who

has the authority to activate it, and what steps that person (or persons) will take to initiate BC/DR activities.

Activation includes initial response and notification, problem assessment and escalation, disaster declaration, and plan implementation. After you have begun implementing the plan, you proceed into the recovery phase, as shown in [Figure 7.3](#).

The plan activation phase should define various disaster or disruption levels so that you know when, if, and how to implement your plan. For example, if you experience a network security breach, you'll have to activate different phases of your plan than if the server room is flooded. Therefore, defining various disaster types and levels is important in understanding what should trigger the implementation of BC/DR plans. You may choose to use a three-level rating system, as described below. However, make sure that whatever system you devise, it's tailored to your specific business configuration and that it gives you the guidance you'd need to make these crucial decisions based on predetermined and agreed-upon criteria. It is important to note that specifying and documenting "events of varying severity and duration" in order to decide which parts of your plan to activate is a basic legal requirement for most companies who operate under one or more government regulations, as described in [Chapter 2](#).

REAL WORLD

Working Your Plan

It's common sense but it bears repeating—a disruptive or disaster event generates fear and uncertainty. It's often chaotic. Whatever plan you create should have clear and relatively simple guidelines that almost anyone could follow in a disaster. Use short sentence and clear statements. Test those statements for possible misinterpretation. You don't want to compound the problem during a disaster by having someone later say "Oh, I thought that step meant...." Make it foolproof. After you've developed your plans, we'll walk you through performing table-top exercises intended to test your plans. This will be your opportunity to further hone your documentation to make it simple, clear, and effective. The goal is not for your plan to read like a high-end business plan but like an in-the-trenches "how to" manual.

Let's take a look at activating your plan for minor, intermediate, and major disasters, in that order. The steps you take for a minor disruption will likely be very different than the steps you take for a major disruption, so it's important to put detail around each of these types or levels of disruption.

Minor disaster or disruption

Minor disruptions occur every day in the business world and rarely, if ever, are full BC/DR plans activated. The likelihood of a minor event occurring is high, but the associated disruption is relatively low. Here are four guidelines for defining this category.

1. Typically, the effects are isolated to one component, one system, one business function, or just one segment of a critical business function.

2. Normal operations can often continue, almost uninterrupted, in the face of a minor disruption.
3. Critical business functions still occur for some period of time after this type of disruption.
4. The failure of a single system or service can typically be addressed during the normal course of business.

For example, the failure of a single server, system disk, or phone system is problematic but usually does not require the activation of a BC/DR plan. There may be examples, however, where minor disruptions should be addressed by the activation of part of a BC/DR plan. If that is the case, be sure to clearly identify those disruptions along with which sections of the BC/DR plan should be implemented when and by whom.

REAL WORLD

Malware, Antivirus, and Incident Response

While it's outside the scope of this book to delve too deeply into information security, there is a point at which BC/DR and information security incident response intersect. Take as an example recent hacks on governmental Web sites. Intruders got into Web sites and networks and disrupted business. The information security teams implemented incident response plans to first observe, then track, and then stop the attacks. Their plan was predetermined and followed an organized set of steps. Was the building impacted? No. Did anyone have to evacuate? No. Was this event a significant disruption? Not to all users, but the potential impact was enormous. This is a great example of working through your threat scenarios to understand what might occur and how you will respond. Having a plan for incident response is part of a BC/DR plan and is another aspect that can be worked in parallel.

Intermediate disaster or disruption

An intermediate disaster is likely to occur more frequently than a major disaster, but obviously less frequently than a minor disaster (hence the "intermediate" designation). Its impact will also fall in the middle of the spectrum. These are the guidelines for defining this type of disruption:

1. This type of disruption or disaster interrupts or impacts one or more mission-critical functions or business units, but not all of them.
2. Operations will experience significant disruption; entire systems or multiple systems may fail or be unavailable, but not all of them.
3. An intermediate event could include a fire or flood in the building that impacts IT systems and equipment, structural damage to part of the building where critical operations occur or where vital equipment is located.
4. An intermediate event could also include an event with a limited impact but a long duration, such as a minor disaster where recovery exceeds the established RTO.

As with the other levels of disruption, it's important to define not only what each tier consists of, but which parts of the BC/DR plan should be activated and which

team members should begin implementing BC/DR activities. As with a major disruption, clearly delineate which systems, functions, and operations would be impacted to earn an intermediate designation so you can define triggers that will address these types of situations.

Major disaster or disruption

The possibility or likelihood of this type of disaster occurring is low, but the business impact is extremely high. Guidelines for defining this type of event include:

1. This event disrupts all or most of the normal business operations of the company and all or most of its critical business processes.
2. The disruptions occur because all or a majority of systems and equipment have failed or are inaccessible.
3. This includes destruction to the entire facility; a major portion of the facility; or entire networks, subnets, or sections of the business.

Once you've defined what this level of disaster or disruption entails, you should define the process for determining which parts of your BC/DR plan should be activated and which team members should be called upon. We'll discuss triggers more in a moment; for now you should attempt to define the business systems, mission-critical functions, and major operations that, when affected, would cause a major disruption. This will help you develop appropriate triggers to determine when and how to activate your BC/DR plan.

Activating BC/DR teams

Clearly, the BC/DR plan cannot activate itself; someone or a team of people need to make appropriate assessments of the situation and make a determination as to whether or not to activate the plan or portions thereof. Therefore, it's also important to create and maintain BC/DR teams who handle the response to the business disruption by implementing appropriate sections of the BC/DR plan. We'll discuss the makeup of these teams later in this chapter, but for now we'll list some of the BC/DR teams you may want to define and populate as you continue in this planning process.

- Crisis management team (CMT)
- Damage assessment team
- Notification team
- Emergency response team
- Business continuity coordinator or lead
- Crisis communication team
- Resource and logistics team
- Risk assessment manager

Depending on the size and nature of your company, you may or may not need some of these functions. It's also possible that one person may fill one or more roles

if you're working in a small company. We'll discuss these roles in more detail in a section coming up later in this chapter.

Developing triggers

If you're familiar with project management, you're probably familiar with triggers. Typically, risks and triggers are identified so that if a project risk occurs, a trigger defines when an alternate plan or method should be implemented. The same is true here. If you are going to implement your plan, you'll need to define how and when that should occur—those are your triggers. For example, if you use the three categories of major, intermediate, and minor, you'll need to define what actions are taken in each case. Each level of disruption should have clearly defined triggers. Let's look at a hypothetical example. You're the IT manager of a small firm and the head of the BC/DR team. You're at home one evening just sitting down to dinner when one of the data processing operators who works until 9 PM calls you. She reports that there was a fire in the building, it's been evacuated, and the fire department is on the scene. You ask her a series of questions and ascertain that the fire seems to have been contained relatively quickly but that some of the networking gear may have been damaged either by the fire or by the fire containment efforts. She believes the server room is intact but she's not sure. If you have clearly defined triggers in place, you may determine that this appears to be either a minor or an intermediate disruption and that you should most likely activate a portion of your BC/DR plan. The trigger might be defined as a series of steps such as:

1. Business disruption event has occurred.
2. Disruption to business operations has occurred.
3. Initial assessment by employees on the scene indicates intermediate-level damage, including the following:
 - A portion of the network is or may be out of service.
 - One or more critical servers are or may be out of service.
 - A portion of the physical facility has been impacted by the disruption.
 - It is likely employees will not be able to resume normal operations within 2 hours.

This is an example of a trigger you could define for intermediate types of events. As you've done previously, using scenarios helps you define these elements more clearly. By defining three statements and four attributes, you have a good understanding of whether or not to activate the BC/DR plan for intermediate outages. You also have a defined time line—if normal business operations cannot resume within 2 hours. This should be tied to your overall maximum tolerable downtime (MTD) and other recovery metrics developed earlier. If your MTD is 24 hours, an intermediate disruption might be something that will disrupt normal operations for 2-6 hours. You and your team will need to define these various windows, but be sure to tie your triggers to your recovery metrics.

Your intermediate activation steps are related to the trigger. Once you know you should activate your plan, you should define the immediate steps to be taken. This

helps remove any uncertainty about next steps and helps begin a focused response effort. An example of the first steps for an intermediate disruption is shown here.

1. If a disruption appears to be intermediate on initial assessment, within 2 hours:
 - Attempt to gather information from the emergency responders, if appropriate.
 - Activate the damage assessment team.
 - Notify the CMT to be on standby notice.
2. After 2 hours from event notification, gather initial evaluation from damage assessment team. Analyze data and determine:
 - Take remedial action and resolve issue.
 - Partial or full activation of BC/DR plan.
3. After 3 hours, notify CMT of next steps (stand down, fully activate).
4. Within 3 hours of event notification, BC/DR plan should be implemented if assessment indicates intermediate or major disruption.

Notice that the description of the actual disruption levels includes trigger information. How many systems are impacted? How extensive is the damage? The more clearly you can define these details, the more precise your triggers will be. This will help you determine if and when to activate your plan. Spend time clearly defining the circumstances that will warrant plan activation at the various levels you've defined. Also define initial steps to be taken in each phase so that you have checklists of next steps. We'll provide additional checklists you can use as starting points for your own lists when we go over disaster recovery steps in the next chapter as well as in the appendix materials at the end of this book.

Transition trigger—Activation to recovery

Another trigger to define is when to move from one phase to another, the *transition trigger*. In this case, that means when to move from the *activation* phase to the *recovery* phase. This transition is one that typically occurs fairly naturally, so you don't need to overengineer this. However, you may want to define the transition trigger like this:

1. The damage assessment team's initial evaluation indicates an intermediate disruption.
2. The CMT has been called in and is on scene.
3. The immediate cause of the event has stopped or been contained.
4. The intermediate BC/DR plan has been activated.

You may wish to define other triggers for your transition, from activation to recovery, suitable to your organization. When defining your triggers throughout, keep your MTD and other defined metrics in mind so that you can work within those constraints. For example, if your MTD is very short, your time between activation and recovery also should be very short. In this case, you may have to err on the side of timeliness and take action with incomplete or preliminary data. You'll have to balance your need to collect information with your need to get the business back

up and running as quickly as possible (and within your MTD constraints). Rarely, if ever, is there perfect data in an emergency (or any other time). Clearly defining these triggers and constraints in your plan can help you make better decisions in the stressful aftermath of a business disruption or disaster. Help the team make the best decisions possible by spending time now to define these triggers as clearly and unambiguously as possible.

Recovery phase

The recovery phase is the first phase of work in the immediate aftermath of the disruption or disaster. This phase usually assumes that the cause of the disruption has subsided, stopped, or been contained, but not always. For example, in the case of flooding, you may decide that if it's external flooding, you will wait until waters subside to begin recovery efforts. This may be required by local officials who restrict access to flooded areas. However, in other cases, you may be able to or choose to initiate recovery efforts while flooding is still occurring. This might include placing sandbags around the entryways to the building or removing equipment that is not yet under water. As you can tell, many of your actions will be dictated by the specifics of the situation, so there's no simple rule to follow here. However, we can say that recovery efforts have to do with recovering from the immediate aftermath of the event, whether or not the event is still occurring. This phase may also include evacuating the facility, removing equipment that can be salvaged quickly, assessing the situation or damage, and determining which recovery steps are needed to get operations up and going again. The recovery phase is discussed in detail in [Chapter 8](#).

Transition trigger—Recovery to continuity

You'll learn more about recovery activities in [Chapter 8](#), so you'll need to circle back and define these triggers after you understand the information covered in that chapter. At this juncture, you can make a note that you need to develop triggers that help you know when to transition from *recovery* efforts to *business continuity* efforts. Typically, these triggers will have to do with determining that the effects of the disruption have been addressed and are not getting any worse. For example, if you experience a fire in the building, the fire is out, the assessment has been done, any equipment or supplies that can be salvaged have been, and alternate computing facilities have been activated. Those are activities that take place in the recovery phase and when these are all complete, it's time to move into the business continuity phase, which typically includes starting up systems so that normal business operations can resume. Defining these points should include specific events that have occurred, milestones that have been met, or time that has elapsed. Also keep your MTD in mind as you define triggers for this transition.

TIP**Backup During Recovery**

There's a bit of a circular problem to resolve in this process and it's important to note. Once you have stabilized your environment and you're beginning to look to business continuity, you need to have a plan in place for backing up the data that are being generated in this new environment. It's easy to plan for data backups during your normal operations. It's sometimes overlooked that if you activate your DR plan, you'll need to ensure you've thought about backing up and safeguarding *that* data. So, let's assume you've lost a part of your data center and you're running from your alternate location. Are you backing up that data? Have you made plans for off-site storage of that data? You can't assume that you'll have disaster after disaster, but you should assume there may be some glitches in your alternate computing environment (especially if you're not running it as a mirrored site) and that data may need to be recovered. It could be as simple as deciding you'll use cloud-based backup solutions if you activate your disaster plan. It's important to think through how long you'll be running from your alternate location and how you'll protect that data if you'll be running from that alternate location for any length of time.

Business continuity phase

The business continuity phase kicks in after the recovery phase and defines the steps needed to get back to "business as usual." For example, if you have a fire in the building, the recovery phase might include salvaging undamaged equipment, ordering two new servers from a hardware vendor, and loading up the applications and backup data on the servers at a temporary location so that you can begin to recover your data and your business operations. The business continuity phase would address how you actually begin to resume operations from that temporary location, which work-arounds need to be implemented, what manual methods will be used in this interim period, and so forth. The final steps in the business continuity phase will address how you move from that temporary location to your repaired facility, how you reintegrate or synchronize your data, and how you transition back to your normal operations. This detail is discussed in [Chapter 8](#). You'll also need to define triggers here that define when you end business continuity activities and when you resume normal operations. Again, as with the other triggers, you should strive to be as clear and concise as possible. You'll have enough to deal with later if you do end up activating and implementing your plan, so spend time here to save yourself a headache later on.

Although it might seem intuitive that you'll resume normal operations when everything is back to normal, things sometimes do not return to normal after a business disruption of any magnitude. Certainly, business operations will resume, but some things may change permanently as a consequence of this disruption. For example, your company may decide as a result of a major fire or flood that it wants to move to a new location and it's going to do that while operating from the alternate site. That would complicate things because it would mean moving from the alternate site to a new site, with all the concomitant challenges inherent in both resuming normal operations and moving to a new facility. Though this example may seem outside the bounds of normal business decision-making, be assured that disruptions can change the way companies see their businesses and the way they approach operations.

Another example is developing a work-around that's used in the recovery phase that works so well that someone decides to use it full time. When do you transition back to normal operations if you select your BC/DR work-arounds as your new normal? When do you officially transition back to normal operations if you decide that the new server role or network configuration actually works better than the original? It might be a simple matter of formally evaluating the change, agreeing to make it permanent, and declaring you're now running under normal operating conditions. However, you now need to back a new BC/DR plan to address a potential failure at your new location—including how and where you store backups generated at this new location. You and your team can define these triggers in advance and you may need to modify them later, but at least you won't be starting with a blank slate.

Maintenance/review phase

The maintenance phase has to occur whether or not you ever activate your BC/DR plan. On a periodic basis, you need to review your BC/DR plan to ensure that it is still current and relevant. As operations and technology components change, as you add or change facilities or locations, you'll need to make sure that your plan is still up-to-date. One common problem in BC/DR planning is that companies may expend time to develop a plan, but they often do not want to (or will not) expend the time and resources necessary to keep the plan current. Old plans are dangerous because they provide a false sense of security and may lead to significant gaps in coverage. If a plan is not maintained, then all the time and money invested in creating the plan is wasted as well. We've repeated it numerous times due to the effectiveness of the approach—seek to operationalize plan maintenance as well. Ensure that every time you stand up a new server, switch or storage solution that you review how it impacts (and is impacted by) your BC/DR plan. This review can be an established part of your IT change control process, and your change control documentation can call out any necessary changes to your BC/DR plan as a result of each change. We will discuss change control as it relates to BC/DR plan maintenance later in this chapter.

In addition, if you end up activating your BC/DR plan at some point, you'll want to assess the effectiveness of the plan afterward, when things settle down. You should do this relatively close to the end of the recovery and business continuity cycles so that lessons learned can be captured and applied to your BC/DR plan before memories fade and people go back to their daily routines. Reviewing the plan in the immediate aftermath of a disruption will give you valuable insights into what did and did not work. Incorporating this knowledge into your plan will help you continue to hone the plan to meet your evolving business needs. This is discussed further in [Chapter 10](#).

DEFINING BC/DR TEAMS AND KEY PERSONNEL

There are numerous people in positions that are critical to the activation, implementation, and maintenance of your BC/DR plan. Although these may not all be relevant to your organization, this will serve as a good checkpoint to determine who should be included in your various phases. You'll also need to form teams to fulfill various

needs before, during, and after a business disruption or disaster. Where possible, you should specify a particular position or role that meets the need rather than specifying individuals. If your Facilities Manager should participate in the Damage Assessment Team, for example, you should specify the Facilities Manager and not Joe, who happens to be the Facilities Manager now. That will allow your plan to remain relevant whether Joe wins the lottery and leaves the company, gets hit by a bus and is out for an extended period of time, or is promoted to vice president.

We'll look at the types of teams your company should have in place, but often these are in place and are outside the scope of the IT department's direct responsibilities. Whether you'll ultimately be responsible for defining and creating these teams or not, having awareness of their functions can be helpful as you craft your BC/DR plan. Since these teams do not have specific IT implications for the most part, we'll review them quickly.

Though we only briefly define types of teams and their roles in the BC/DR effort, you should take time to clearly define the roles and responsibilities of each team if you are responsible for this broader BC/DR type of activity. Having clear boundaries will help ensure that teams are not working at cross-purposes and that all aspects of the plan are covered. Gaps and omissions occur when these kinds of definitions are ill-formed. If helpful, you can create team descriptions that read like job descriptions and you can task members of your HR department on the BC/DR team to assist with or lead this activity. A good team description will identify the following attributes:

- Positions or job functions included on the team (Facilities Manager, HR Director, etc.)
- Team leader and contact information
- Team mission statement or set of objectives
- Scope of responsibilities (define what is and is *not* part of this team's mission)
- Delineation of responsibilities in each phase of BC/DR (i.e., when will the team be activated and deactivated?)
- Escalation path and criteria
- Other data, as needed

Let's look at a few commonly used teams and how you can incorporate them into your BC/DR plan.

Crisis management team

In most companies, the composition of CMT will mirror the organizational chart. It should have representatives from across the organization and should bring together members of the company who have the expertise and authority to deal with the after-effects of a major business disruption. The CMT will decide upon the immediate course of action in most cases and, when necessary, they can contact senior management. They will direct the distribution and use of resources (including personnel) and will monitor the effectiveness of recovery activities. They can adjust the course

of action, as needed. They should be in charge of activating, implementing, managing, and monitoring the business continuity and disaster recovery plan and should delegate tasks as appropriate.

Management

Each company has a management team or structure that oversees the business and its operations. You'll need to determine which positions from your management team should be included in your plan. Remember to review all the phases. For example, you might decide that only a member of the management team can cause the BC/DR plan to be activated. Management might be required to decide when to transition from disaster recovery to business continuity activities or they might be the one(s) to decide how and when the BC/DR plan should be tested. In addition, different levels of management may activate parts of the plan or the entire plan, depending on disaster level. Identify the positions that should participate as well as define how they should participate in each phase. It's important to note that documenting "roles and responsibilities" of disaster responders is a basic legal requirement of most companies which fall under one or more government regulations related to IT security, as described in [Chapter 2](#). Furthermore, having these roles and responsibilities documented can limit a company's legal liability in the aftermath of a disaster.

Damage assessment team

A damage assessment team should be comprised of people from several key areas of the company, including Facilities, IT, HR, and Operations. Your company's damage assessment team may contain other members, depending on how the company is structured and what type of business you're in. If you work in a small software development firm, you may just need the CEO, the IT manager, and the office manager to operate as the damage assessment team. In larger companies with multiple locations, you'll need to have several damage assessment teams or you may choose to create a mobile team that can fly to any site and assess damage within 24 hours of an incident. You may choose to have both a local and a mobile corporate team so that the right team can be called in. If the building floods, you may not need the mobile team to come in. However, if you have a large fire, earthquake, or other major event, you may need the support services of a mobile damage assessment team.

Operations assessment team

You may choose to have a separate operations assessment team comprised of individuals who can assess the immediate impact on operations. A damage assessment team may be tasked with this job, but in some types of companies, you may need a separate operations team that can assess what's going on with operations and how to proceed. The operations assessment team can also be tasked with beginning recovery

phase activities, monitoring and triggering the transition from activation to recovery, recovery to business continuity, and BC to normal operations.

IT team

Clearly, you need an IT team that can not only assess the damage to systems but also begin the disaster recovery and business continuity tasks once the plan is activated. This IT team will work closely with the damage assessment team and/or the operations assessment team to determine the nature and extent of damage, especially to IT systems and the IT infrastructure. You may not need some of the technical specialties listed here, but this should be a good starter list for you to work from to determine exactly what expertise you'll need on your team.

- Operating system administration
- Systems software
- Server recovery (client server, Web server, application server, etc.)
- Storage recovery
- Database recovery
- Network operations recovery
- LAN/WAN recovery
- Application and data recovery
- Telecommunications
- Hardware salvage
- Alternate site recovery coordination
- Original site restoration/salvage coordination
- Test team
- Information security team

Administrative support team

During a business disruption, there are a wide variety of administrative tasks that must be handled. Creating an administrative support team that can respond to the unique needs of the situation as well as provide administrative support for the company during the disruptions is important. This might include ordering emergency supplies, working with vendors arranging deliveries, tracking shipments, fielding phone calls from the media or investors, organizing paper documents used for stopgap measures, and more.

Transportation and relocation team

Depending on the specifics of your BC/DR plan and the type of company you work in, you may need to make transportation arrangements for critical business documents, records, or equipment. You may need to move equipment in advance of an event (like a hurricane or flood) or you may need to move equipment after the event to prevent further damage or vandalism. Relocating the company and its assets

before or after a disruption requires a concerted effort by people who understand the company, its relocation needs, and transportation constraints.

Media relations team

You may need to create a crisis communication plan because you usually will need to provide information about the business disruption/disaster to employees, vendors, the community, the media, and investors. One key area that should be well prepped is media relations. Unlike other stakeholders mentioned, the media make their living selling interesting stories. Since a disruption at your business may qualify as news, you might as well craft the message rather than leaving it to outsiders. Creating a team that knows how to handle the media in a positive manner and that understands the policies and procedures related to talking with the media is vital to help ensure your company's image and reputation are maintained to the greatest extent possible. Certainly, if your company is at fault, you will have to deal with a different set of questions than if your company experiences a natural disaster. Still, you'll need to manage the story either way. Most mid-sized to large companies have a communications team who handles exactly these kinds of issues, so the team may already be in place. If that's the case, your plan should address how to bring that team into the loop in the event of a disaster.

Human resources team

The aftermath of a crisis is an incredibly stressful time for all employees. Having an HR team in place to begin handling employee issues is crucial to the well-being of the employees and the long-term health of the company. Retaining key employees, adequately addressing employee concerns, facilitating insurance and medical coverage, and addressing pay and payroll issues are part of this team's mission. This team may also be responsible for activating parts of the BC/DR team as it relates to hiring contract labor, temporary workers, or staff at alternate locations.

Legal affairs team

Whether your legal experts are internal or external to your company, you should identify who needs to address legal concerns in the aftermath of a business disruption or emergency. If you hire outside counsel to assist you with legal matters, you should still assign an internal resource as the liaison so that legal matters will be properly routed through the company. If you operate in a heavily regulated industry such as utility, banking, government, finance, or health care, you should be well aware of the constraints you face, but having a legal affairs team can assist in making decisions that keep your company's operations within the bounds of laws and regulations. Even if you're not in a heavily regulated industry, you may need advice and assistance in understanding laws and regulations in your recovery efforts. These items may be outside the scope of your IT duties, but in small companies where people wear many

hats, you may be the only one thinking about these kinds of issues. If you work in a larger company that has legal counsel, you may want to think through any potential legal issues you may face with respect to IT. For example, if you're a service provider, you may have legally binding service-level obligations that are impacted in a disaster. Having a legal representative step in during a disaster to handle those issues could be helpful. At a minimum, it is prudent to have outside legal counsel review your BC/DR plan for any gaps related to your company's legal obligations to provide "reasonable security" and "security breach notification," as described in [Chapter 2](#).

Physical/personnel security team

In the aftermath of a serious business disruption, you will need a team of people who address the physical safety of people and the building. These might be designated Human Resource representatives, security staff, or people from your Facilities group, for example. If you work in a large company or in a large facility, you may have a separate security department or function that manages the physical and personnel security for the building. If this is the case, designated members of their team should be assigned to be part of the BC/DR team. If you don't have a formal security staff, be sure that the members of this ad hoc team receive training. Someone from HR or facilities might be willing to take on the role of security in the aftermath of a disaster, but they need to be trained as to the safest, most effective method of managing the situation. Training for part-time or ad hoc security teams is crucial because if a natural disaster strikes, emergency personnel such as your fire or police department will focus on helping schools, day care centers, nursing homes, and hospitals first. Your company may fall very low on the list of priorities, so having trained staff that can fill the gap in an emergency may literally mean the difference between life and death. We'll discuss training later in the book, but keep this in mind as you develop your teams.

Procurement team (equipment and supplies)

Every company has some process in place for procuring equipment and supplies. In small companies, this might fall to the office manager or operations manager. In larger companies, there's usually a purchasing department that handles this function. Regardless of how your company is organized, you need to determine, in advance, how equipment and supplies will be purchased, tracked, and managed after a localized disaster such as a fire or in the aftermath of a widespread disaster such as a hurricane or earthquake. This includes who has the authority to make purchases and from whom, what dollar limit the authority carries, and how that person (or persons) can get authority to make larger purchases. For example, a company might specify that three people have the authority to purchase equipment and supplies up to \$20,000 per order and up to \$100,000 total. Beyond that, they have to have the president or vice president sign off on purchases. This predetermined purchasing

information can also be communicated to key vendors so they know the three people who are authorized and what the authorization limits are. In this way, if disaster strikes, the company can turn to trusted vendors who, in turn, know the rules. This can expedite the recovery process.

Keep in mind that this team needs to be large enough that there is no “single point of failure.” If you authorize only one person and something happens to that one person, you’ll be scrambling to obtain emergency authorization for other individuals. Instead, authorize enough people to provide flexibility but not so many as to create chaos. Also, be sure your limits are appropriate to the type of business you run. If you may need to replace servers at \$9500 a piece, make sure the limits reflect that. If a purchaser has a \$5000 limit per item, that will preclude him or her from making a simple purchase needed to get the company running again.

General team guidelines

Though we recommend populating teams first with needed skills based on *roles* and *positions* within the company, we also recognize that ultimately *people* are assigned to the team. People should be chosen to be on teams based on their skills, knowledge, and expertise, not because someone wants to be on a team or because someone’s boss placed them on a team. In a perfect world, you could choose team members solely on competence, but we all know that in the real world, that’s not always the case. Occasionally, you get the people who have the most time on their hands, who sometimes are the junior members of the team or the least competent people in the department. You have to work within your organization’s constraints and culture, but also strive to populate your teams with the right people with the right skills. Ideally, these are the same people who perform these functions under normal conditions. It doesn’t make sense to have the database administrator take on media relations duties during an emergency, just as you don’t want the marketing VP managing the restoration of the CRM database. Certainly, in small companies many people are called upon to perform a variety of tasks and if that’s the case, the same will be true if the BC/DR plan has to be activated. The teams also should be large enough that if one or more members of the team are unable to perform their duties, the team can still function. If you have other personnel or other parts of the organization that can wholly take up the BC/DR activities, so much the better. If not, you may also choose to designate key contractors or vendors to assist as alternates in the event of a catastrophic event. These personnel should be coordinated and trained as alternates along with internal staff.

LOOKING AHEAD

Specialty Vendors Help BC/DR Plans

There are numerous specialty vendors that can provide tremendous assistance to your firm in the event of a business disruption such as a fire or chemical spill. Although the numbers and types of firms in your area will vary, you should consider your specific needs in advance of any

Continued

LOOKING AHEAD—cont'd

disruption and search for a firm that will meet your needs, even if that firm is located across the country. These firms provide a wide and unusual assortment of services, some of which are listed here:

- Chemical oxidation
- CO₂ blasting
- Condensation drying
- Contact cleaning
- Corrosion removal
- Damp blasting
- Degreasing
- Deodorizing
- Fogging for odor removal or disinfection
- Manual hand wiping
- High pressure and ultra-high pressure jetting
- High temperature steam jetting
- Hot air drying
- Low pressure jetting
- Microwave drying
- Ozone technology
- Sanitation
- Steam blasting
 - Vacuum drying
 - Water displacement

As you can see, this is quite a list and it's not exhaustive. Be sure to think through the various scenarios that apply to your firm and determine which specialty services might best be outsourced to a qualified third party. You'll save yourself time and money in the long run and you'll likely get up and running much more quickly with targeted, competent help than if you try to do everything on your own.

BC/DR contact information

After you've developed the requirements for your teams in terms of the specific skills, knowledge, and expertise needed, you'll identify the specific people to fill those roles. Part of plan maintenance, discussed later in this book, involves ensuring that the key positions are still in the BC/DR loop and that key personnel are still aware of their BC/DR responsibilities.

Another mundane but crucial task in your planning work is to compile key contact information. Since computer systems often are impacted by various types of business disruptions—from network security breaches to floods and fires—you'll need to have contact information stored and available in electronic and hard copy. It should be readily available at alternate locations and copies should be stored in off-site locations that can be accessed if the building is not accessible. However, since this list contains contact information, it should also be treated as confidential or sensitive information and should be handled and secured as such. This information should include contact information for key personnel from the executives of the

company (who will need to be notified of a business disruption) to BC/DR team members to key suppliers, contractors, and customers, among others.

Develop a list of the types of contact information you need, including:

- Management
- Key operations staff
- BC/DR team members
- Key suppliers, vendors, and contractors (especially those with whom you have BC/DR contracts)
- Key customers
- Emergency numbers (fire, police, etc.)
- Media representatives or PR firm (if appropriate)
- Other

After you've identified the contact information you want to include, you'll need to determine where and how this information currently is maintained. In most companies, this information is stored in a multitude of locations and is not easily compiled with a few clicks of the mouse. You may need to develop a process for maintaining an up-to-date list, both electronically and on paper, of these key contacts. For example, many of your key contacts may be in a contact management application made available to everyone in the company. However, information such as executives' cell phone numbers and home phone numbers may not be included in this company-wide contact database, for obvious reasons (especially if you work in a medium to large company). Therefore, you'll need to have a copy of the contact information plus information not included there. Developing a process for gathering and maintaining that data is an important part of BC/DR readiness. If a serious business disruption occurs in the middle of the night—for example, the building catches on fire—who will you contact? How will you know who to contact? Where will you find the key phone numbers you need if you can't get back into the building and you can't access computer systems? Since notification is one of the first steps in activating your BC/DR plan, you'll need to have key phone numbers available (*you* meaning the person(s) responsible for activating the plan). Develop a process for this during your BC/DR planning project and make sure that your maintenance plan includes regularly updating this information.

In addition to developing and maintaining a contact list, you should also define a contact tree. This defines who is responsible for contacting other teams, members of the company, or the management team. That way, each team member is tasked with specific calls to specific people and the notification process is streamlined. If you have a Help Desk or Operations desk, this task can be delegated to this team, assuming they have a process and will be able to activate this task. You can also tap into your organization's larger disaster recovery communication plan, which typically will cover all these elements and may also provide a mass communication capability.

REAL WORLD**Maintaining Up-to-Date Contacts**

Maintaining up-to-date contact information can be a challenge, especially since that information seems to change so frequently. It is becoming more common for people to keep their cell phone numbers regardless of where they work, so you could potentially end up calling someone at 4 AM who hasn't worked for the company in a few years—embarrassing and a waste of precious time in an emergency.

In addition to using your company's contact list, you may also choose to select a Web-based service. If your company has a mass notification system in place, you can leverage that. If not, you can certainly set something up for your IT department. You want to be able to reach people by cell, text, and e-mail. You may choose to have people set up DR-specific e-mail accounts outside the organization. You may choose to use other Web-based or external teleconferencing services. You could certainly use social media—though you want to be careful about what information you share publicly. Remember, there may be legal liability related to a downtime, so you don't want to tweet "this is a total disaster, we blew it." However, be creative in looking at the solutions you have available. One option to keep phone numbers current is to identify the system of record(s) for contact information in the company, e.g., the HR system, asset management system for mobile devices, or Active Directory, and create batch processes to export these data in a readable format and copy them to your off-site DR location or secure cloud storage nightly. Most important is to ensure it is up-to-date, annually at minimum, semi-annually or quarterly would be even better.

DEFINING TASKS AND ASSIGNING RESOURCES

The tasks and resources that need to be assigned have to do both with implementing the mitigation strategies you've defined as well as fleshing out the rest of the plan. First, you have to ensure your risk mitigation strategies will be properly implemented. This may mean creating project plans to address any new initiatives you need to undertake in order to meet your risk mitigation requirements. We'll assume you've got that covered as part of your risk mitigation strategy. If not, now's the time to develop your WBS, tasks, resources, and time lines for completing any risk mitigation strategies that need to be completed in advance of a disruption. This might include purchasing and installing new uninterruptible power supplies for key servers, updating your fire suppression systems, or implementing a data vaulting solution. Other mitigation strategies such as arranging for an alternate site need to be completed in advance, but activating it requires a different set of tasks that occur later.

Other tasks have to do with defining your BC/DR teams, roles, and responsibilities; defining plan phase transition triggers; and gathering additional data. Let's start with tasks related to some major activities including alternate sites and contracting for outside BC/DR services. Clearly, there are other tasks and resources you'll need, but this should get you started in developing your own list of tasks, budgets, time lines, dependencies, and constraints for the remaining BC/DR activities in your plan.

As you develop these tasks, keep in mind standard project management processes:

- Identify high-level tasks and use verb/noun format when possible (i.e., “test security settings” rather than “security settings”).
- Break large tasks into smaller tasks until the work unit is manageable.
- Define duration or deadlines.
- Identify milestones.
- Assign task owners.
- Define task resources and other task requirements.
- Identify functional and technical requirements for task, if any.
- Define completion criteria for each task.
- Identify internal and external dependencies.

We’re not going to go through all that detail for these next two high-level tasks, but you should include this level of detail in your plan.

Alternate site

Although this should be part of your BC/DR plan, it’s worth calling it out separately due to its importance and the need for advance work. If part of your risk mitigation strategy is to develop an alternative site or off-site storage solution, you should develop a number of details before moving forward. These should be tasks (or sub-tasks) within the WBS just discussed, so let’s look at some of the details you might include. Also keep in mind that you need to develop a trigger that helps you determine if or when you fire up the alternate site. You probably don’t want to activate the alternate site if you have a minor or even an intermediate disruption, so how do you define when you should? When all systems are down or when some percentage of systems down? You have to take your MTD into consideration along with other factors such as the cost of firing up the alternate site and the cost of downtime. If your downtime is estimated to be 12 days and that cost is \$500,000 but the cost of firing up the alternate site is 3 days and \$250,000, is it worth it to activate the alternate or should you just hobble along until you can restore systems at the current location? There’s no right or wrong answer, it’s going to depend on your company’s MTD, potential revenue losses, cost of starting up the alternate site, and so on. Have the financial folks on your BC/DR team prepare some analyses to determine metrics you can use to help determine your trigger point. As you’re going through the activities listed in this section, keep these factors in mind.

Selection criteria

Selection criteria are the factors you develop to help you determine how to select the best alternate site solution for your company. This includes cost, technical and functional requirements, timelines, quality, availability, location, and more. Be sure to consider connectivity and communications requirements in this section along with your recovery requirements such as MTD. Remember that you need to find the best balance between risk and mitigation—so your selection criteria should not be so rigorous as to exclude all but the most expensive, iron-clad options. You may choose to

use prioritization in your selection criteria language. For example, availability and technical requirements might be your first priority; location might be second or even third. By prioritizing, you can ensure you don't box yourself into a solution that is overengineered (or under-engineered) for your needs.

Contractual terms

Determine what contractual arrangements are appropriate for your company. Many vendors have predetermined service offerings and contracts are fairly standard. Other companies can accommodate a wider range of options and will work with you to develop appropriate contractual language. In either case, be sure to run these contracts past your financial staff and your legal counsel to make sure you are fully aware of the financial and legal consequences of these contracts in advance of signing them. If you're not clear what they mean operationally, be sure to talk with the vendor and add clarifying language to the contract. Do not simply take the vendor's word that a particular paragraph or section means something. Verbal agreements are always superseded by written contracts, so make sure the contract spells it out clearly. If the language is vague, confusing, or contradictory, work with the vendor and your contracting or legal department to clarify. You should never rely on verbal commitments when it comes to implementing your BC/DR solutions, so be sure to put everything in writing in advance.

Comparison process

Be sure to specify what process you'll use to select the vendor. This might include a list of technical requirements the vendor must meet, but it might also include an assessment of the vendor's geographical location, financial history, and stability and industry expertise, among other things. Selecting the right vendor for an alternate site or off-site storage is a very important aspect to your BC/DR success and should be undertaken with the same rigor as your other planning activities. Again, using prioritization of criteria will help you select the right solution.

Finally, check references before making a final selection. If you can find customers the vendor does not directly supply to you, you're more likely to get an accurate picture. If the vendor supplies you with customer references, be sure to ask that customer some leading questions such as "When you had problems with connectivity, how did the vendor respond?" By asking this type of question, you can lead even a reference customer into discussing issues that came up. Your intent is not to trick anyone, but to get a clear and accurate picture of the vendor's capabilities and responsiveness.

Acquisition and testing

Once you've selected your alternate site or off-site storage vendor and completed the contract, you will need to make whatever additional arrangements are needed for developing this solution so that it is fully ready in the timeframe you've designated. This might include purchasing additional hardware and software, setting up communications channels, and testing all solutions implemented. Create a thorough

acquisition and testing plan for this phase so you can transition to it as seamlessly as possible in the event of a business disruption. During your testing phase of the BC/DR plan (see [Chapter 8](#)), you should test the process for firing up this solution on a periodic basis.

Cloud services

Cloud services are one of the newest developments in BC/DR risk mitigation strategies. Cloud services encompass many different service offerings, including:

- IaaS (Infrastructure as a Service)
- PaaS (Platform as a Service)
- STaaS (Storage as a Service)
- DRaaS (Disaster Recovery as a Service)
- SaaS (Software as a Service)

In contrast to using a co-location or your own facility as an alternate DR site where you house your own separate networking, hardware, and software for DR operations, cloud computing allows for the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). Cloud services are typically priced on a pay-per-use basis. End users access cloud-based applications through a Web browser or lightweight desktop or mobile application while the business software and user's data are stored on servers at a remote location.

In the case of SaaS, users are provided access to application software and databases, and cloud providers manage the infrastructure, platforms that run the applications, as well as all IT disaster recovery operations. This allows businesses to reallocate IT operations costs away from hardware/software spending and labor expenses associated with IT support, toward meeting other goals. Through economies of scale and use of converged, shared infrastructure, cloud providers are typically able to offer similar IT services at a cheaper operational cost. In addition, cloud computing allows users to obtain, configure, and deploy cloud services themselves using cloud service catalogs, without requiring IT assistance. One major downside often noted with such an arrangement is the increased risk of unauthorized access to sensitive business data should the cloud provider not have consistent security controls in place that meet or exceed business requirements.

In the most basic cloud service model, providers of IaaS or STaaS offer compute (servers or workstations) and storage as two distinct offerings. Cloud providers supply these resources on-demand from their large resource pools in remote data centers. For secure connectivity, customers can use either SSL/TLS encryption over the Internet or dedicated virtual private networks (VPNs) with IP-based encryption. In the PaaS model, cloud providers offer a full computing platform, which typically includes an operating system, programming language execution environment, database, and/or Web server.

Use of cloud services to enhance DR mitigation strategies may offer real, tangible benefits, depending upon requirements. For example, Broadband Capital Group, a

New York financial services firm, uses both SaaS-based e-mail in the cloud as well as IaaS for backing up their other critical data and systems which run on-premise. For their SaaS-based e-mail, their provider handles off-site backups to the cloud, so they don't need to use a local e-mail server or perform any backups on premises. They use another IaaS cloud provider to back up all on-premise systems and data. In the event of a disaster, they can recover compute and storage and access their systems through a VPN from an alternate physical site with an Internet connection, including an employee's home. In addition, some companies are using the cloud as a full disaster recovery strategy. For example, in 2010, MacNair Travel Management, a Virginia-based corporate travel agent, was hit by two major storms that dumped about 55 in. of snow in the Washington, DC, area and could have crippled their business. During both storms, not a single employee made it into the office. MacNair uses cloud services for business operations, for all employees, by housing all company applications at an IaaS/PaaS cloud provider ([Brandon, 2011](#)). Their provider handles the data backups and duplicates data between two facilities. Despite the storms, MacNair was able to access their applications, operating systems, and data during the storms with only an Internet connection and a browser. Not being dependent on a single location or data/voice carrier and having full backups handled by their cloud provider enabled MacNair to continue limited operations temporarily from employee's homes. Despite success with cloud services for business continuity planning, MacNair admitted that an overall disaster recovery plan is still needed to determine things such as where employees will work, restoration of company facilities, and which IT services can be suspended while critical systems are restored.

Despite these success stories, cloud services are not yet the panacea for mitigating all disaster recovery scenarios. The surge in demand for cloud services has largely been driven by small/medium-sized businesses and start-up application development shops, and other enterprises with limited IT resources. In addition, although larger enterprises are beginning to move to limited cloud services for things like cloud-based backup and archive, several challenges still remain before cloud services can be adopted more widely. Availability, performance, privacy, compliance, legal, open standards, and vendor lock-in concerns remain sticking points. For example, the U.S. Government was criticized during the Megaupload seizure process in 2012 for suggesting that people lose property rights by storing data on a cloud computing service ([Kravets, 2012](#)). The question of who is in "possession" of the data and systems residing at cloud providers remains unclear. "Possession" is referenced in law involving trademark infringement, licensing compliance, security concerns, and the like. If a cloud provider is the possessor of the data, the possessor has certain rights. If the cloud provider is the "custodian" of the data, then a different set of rights would apply. Many Terms of Service agreements are silent on the question of ownership, and legal precedent has yet to fully establish clear boundaries when it comes to protection of either party with regard to cloud services. The important message here is to perform due diligence and engage legal counsel, at a minimum, if you are considering incorporating cloud services as part of your BC/DR risk mitigation strategy.

Contracts for BC/DR services

Although we highly recommend you involve your purchasing, finance, and/or legal professionals in executing your BC/DR contracts, you should also have a general understanding of some of the elements to consider. As with alternate site or cloud considerations, keep your MTD, your costs, and potential losses in mind. Have your financial folks help you with performing financial analyses to determine what makes financial and business sense for your company. If a firm wants to charge you \$50,000 for some sort of contract but your downtime estimate with associated revenue and collateral loss is only \$40,000, the contract might not be worth entering. Additionally, determine your triggers for calling upon these contractual arrangements so you don't prematurely fire up these contracts or avoid using them during times when they should be activated. Examples of triggers are provided in the sample BC/DR plan checklists at the end of this book.

Develop clear functional and technical requirements

You know from project management fundamentals that developing functional and technical requirements is often what defines the difference between success and failure. The same is true here. If you have not clearly and fully defined your functional and technical requirements, you'll get all kinds of vendor responses. The more specific you are, the more fully a vendor can address your needs. In addition, if you leave too many elements open to discussion, you'll endlessly discuss possibilities without being able to identify appropriate solutions. Have these discussions in advance and then come to a firm agreement about the requirements. If some requirements appear to be optional or "nice to have," then list them as options and not as requirements. Pare down your requirements to the elements you absolutely must have. Remember, the more options you include, the higher the cost. Therefore, if cost is an issue (and it almost always is), be sure to list what you require and what you desire as separate items. When this information has been finalized, write up formal requirements documents that you can provide to potential vendors. Also, be sure that your requirements documents are reviewed by subject matter experts, including IT experts and those in your company who understand regulatory, legal, and compliance issues. Your requirements should meet all these needs before going out to the vendors.

Determine required service levels

Service levels are typically part of technical requirements, but we've listed them separately because they are vitally important when developing Requests for Proposal (RFP) or Requests for Quote (RFQ) from vendors. You may have contractual obligations to provide certain levels of service to your customers, so you may need to specify requirements for your vendors that meet or exceed these metrics. Even if you have no externally facing service-level agreements (SLAs), you should still specify SLAs in your contracts with vendors. If you're contracting for Internet connectivity, you should specify bandwidth, minimum upload and download speeds, and maximum downtime per specified period, for example. These may sound like

technical requirements, but let's look at how this can play out in a contract. You write up your requirements, which include bandwidth, minimum upload/download speeds, and maximum downtime. Three vendors respond to your RFQ to provide backup Internet connectivity to your company in the event of an outage from your main vendor or in the event that your company's facilities are damaged. All three companies give you quotes that indicate they can meet or exceed those three requirements (bandwidth, speed, availability). However, those are not contractual terms, those are the company saying they *can* meet or exceed those metrics. If it's not in the contract, it's just a statement of capabilities, not a commitment. A SLA will specify minimum bandwidth availability during a 24-hour period, 7 days a week. It would state that you will have access to [insert bandwidth metric] 24 hours a day, 7 days a week until [insert termination metric or trigger]. This way, the vendor can't provide you the bandwidth you requested only from 11 PM to 6 AM on Saturdays and Sundays and short you the rest of the time. Granted, most vendors are on the level and want to provide the services to you they've agreed upon, but that's why contracts exist—to clearly define who does what, when, and at what cost. This keeps the guess work (and the finger pointing) to a minimum. In addition, tying financial consequences (penalties) to failure to perform under contractual terms is recommended. If there are no negative consequences for the vendor, the contract has no real effect. You may invoke breach clauses and get out of the contract, but in the midst of a disaster, you're not going to go that route. However, when specific financial penalties are tied to lack of performance, you have slightly more refined tools for managing the vendor relationship.

Compare vendor proposal/response to requirements

Once you receive vendor responses to your proposals, you should evaluate how closely each vendor comes to meeting the requirements of your plan. Any vendor that does not meet the requirements should not be considered further. There may be two exceptions to this. First, if your requirements are unique enough that no single vendor can meet your needs, you may have to circle back and find two or more vendors who can work together to meet your unique requirements. Second, you may discover from vendor responses that your requirements were too broad, inclusive, or vague, and that none of the vendors' responses meet your requirements exactly. In that case, you may have to refine your requirements and go back out for bid. Assuming your requirements are well written, your next step is to eliminate vendors that cannot meet your needs and focus only on those vendors who addressed your requirements fully in their responses.

Identify requirements not met by vendor proposal

If there are one or more requirements not met by any vendor, you may need to find two or more vendors to work together to provide the full range of services you need. If none of the vendors met a particular requirement, you may also choose to review that requirement and reassess it in light of vendor responses. Remember, you contract with vendors in order to leverage their specific expertise. If none of them meet a

particular requirement, you may wish to talk with several of your short-list selections to find out why they did not address that aspect. It might be redundant or otherwise unneeded. In that case, you should revise your requirements to reflect this new information.

Identify vendor options not specified in requirements

Vendors also may offer additional options not specified in your requirements. Again, based on the vendor's expertise, they may offer additional choices that can round out your requirements or plan. Utilizing their expertise can be a good way of ensuring you have the best solution in place. For example, the vendor might say (in essence), "Everyone who's asked for A, B, and C also has found that D was an extremely important option they'd overlooked. Perhaps you'd like to add D to your plan as well." They may be sharing industry expertise and best practices with you or they may simply be trying to up-sell you. You'll have to look carefully at these options and perhaps do some independent research to determine whether these options are "must have," "nice to have," or "useless add-ons." If you have an established relationship with these vendors, they'll more than likely offer you additional options but won't put pressure on you to upgrade unless they feel it's vital to your success. However, we all know there are sales people that will try to sell you every option they can think of just to make a bigger sale, so you have to be an active participant in the transaction. Know your options, know what makes sense, do some additional research, and determine if any of the additional options would enhance your plan or fill in gaps you didn't realize existed. Don't be forced into upgrades and options you don't really need just because you have a very persuasive sales person in front of you.

REAL WORLD

Managing the Sales Process

Sometimes your purchasing department manages the purchase of goods and services, but when you're talking about the purchase of backup, storage, or alternate site services for your BC/DR plan, there's a good chance you will be directly involved. If you haven't been involved with the sales process in the past, you might find yourself being swayed by excellent sales people—the ones who can convince you that you need something you really don't. Most sales people are honest and are trying to balance their need to sell with your need for the product or service they're selling. They also realize that loyal customers are borne out of an honest sales experience, not out of strong-arming someone into purchasing more than they need. In order to be successful in the process, take time to be clear about your objectives before a sales meeting. If you intend on making a purchasing decision at that time, write down the terms or parameters you will accept. Keep these to yourself but know that this is your bottom line. If the sales person cannot or will not meet your bottom line objectives, there is no deal to be struck.

The same holds true in any negotiation—know what your bottom line is and work toward meeting (or exceeding) that bottom line. If you have developed clear requirements and you know your bottom line, you should be able to successfully navigate the sometimes tricky sales process. Negotiation skills can help you in all aspects of life and they'll certainly help you in the business world. If you're interested in learning more about the art of negotiation, there are thousands of helpful books, courses, and seminars you can turn to for more information.

COMMUNICATIONS PLANS

Earlier in this book, we discussed the need for various communications plans. In this section, we'll define various communications plans you should develop and identify some of the common elements in such a plan. If you already have communications plans in place, you can use this section as a checkpoint to ensure you've got all your bases covered. For each plan, you should define specific steps just as you would for any other process in your BC/DR plan. You should define the following:

- Name of communication team, members of team, team lead, or chain of command
- Responsibilities and deliverables for this team
- The boundaries of responsibilities (what they *should* and *should not* do)
- Timing and coordination of communication messages (dependencies, triggers)
- Escalation path
- Other information, as appropriate

Communications plans can be assigned to other existing teams. A good example of this is that the employee communication plan may be the responsibility of the HR team. There's no need to create additional teams to execute communications plans if these activities fall within the scope of defined teams. However, in some companies, it might make sense to have most of the communications come from one dedicated communications team in order to maintain control over communications and to ensure that a single consistent message is delivered to all stakeholders. The decision is yours and usually is based on how large the company is and how it currently operates.

Internal

The internal communication plan is really part of the BC/DR activation and implementation plan. If a business disruption occurs, you need to have a process in place for notifying BC/DR team members. This is done as part of BC/DR plan activation and is a critical aspect that should be clearly delineated. How will team members be notified and updated? What processes, tools, and technology are needed? Are these included in your plan yet? If not, add them to your project plan's WBS or in a section called Additional Resources so they are captured and addressed in advance of a business disruption.

Employee

Employee communication is also internal communication but differs because it is any communication that goes out to employees who are not part of the BC/DR activation and response team. If a business disruption occurs, you'll need to know how to notify all employees. You'll also need to let them know answers to the most basic questions including what happened, what is being done to address the problem, and who they should go to for more information. For example, if the building burns

down overnight, employees may show up for work in the morning as scheduled. The BC/DR team may already be in action but the general employee population needs information. If the building can be occupied but the data center has been shut down because the fire containment systems were triggered, employees need to know what their next step should be. How this information is communicated and by whom should be identified. It often makes sense to develop an information tree so that key communicators know to whom they should go for updates and official information. For example, in a small company, you may designate the HR manager as the person who will communicate with employees on all BC/DR matters. The HR manager should know who to go to for information on the status of the BC/DR activities. This might be the Facilities manager or the BC/DR team leaders (who should be identified in the activation plans, discussed earlier in this chapter).

Customers and vendors

Customers and vendors typically require different types of communications but the information is often similar. They may need to be notified of the business disruption, the basic steps being taken to rectify the problem, the estimated time to recovery, and any work-arounds needed in the meantime. Knowing how to communicate in a disaster is a skill that can be taught and someone in your company should be responsible for that. Whether it's your company's CEO, General Manager, or owner, someone should be trained in public communication. It can mean the difference between recovery from the disaster and the failure of the company. This is not a task that is specific to IT BC/DR but it's something that should be known and addressed in the overall company's BC/DR plan. That way, if there is an IT-related event (fire in the data center, for example), you know who at your company is responsible for crafting and delivering public statements.

Shareholders

If you have shareholders of any kind (debt or equity investors, shareholders, etc.), you must communicate the nature and extent of the disruption. In most cases, they are concerned with the ongoing viability of the company and possibly the short-term financial impact of the disruption on the company as well as any legal liability. Therefore, communication with this group requires that specific issues be addressed. As you can tell, these issues are very different than, say, employee issues, so someone well versed in investor relations should be charged with this communication. In most companies, this task falls to the CEO or a high-ranking corporate officer who can specifically address the concerns of those who have a financial stake in the company.

The community and the public

In addition to communicating with all the other stakeholders we've mentioned, you also will need to communicate with the general public. Local newspapers, TV, and radio stations will certainly take an interest in a localized business disaster such as a

fire or flood. National and international media may also take interest if the event is unique in some way or is part of a widespread disaster. Members of the local community may also have more than just vicarious interest—they may need to understand the impact your business disruption may have on them. Businesses in communities don't exist in isolation, and what happens to one business may have a ripple effect on other businesses even if those other businesses are not customers or suppliers.

Communicating with the media is a tricky proposition and many executives at large firms go through extensive media training sessions in order to learn how to deal with the media. Although an extensive discussion of this topic is outside the scope of this book, you will learn the basics by reading the case study that follows this chapter. Additional media relations training resources are readily available online and there are hundreds of excellent books on the topic as well. As the leader of the BC/DR project plan, you may or may not be called upon to communicate with the media, but being prepared is always a good idea.

This plan should be well thought-out and you may wish to seek legal counsel with regard to what must be disclosed, to whom, and in what time frame. As you learned in [Chapter 2](#), there are numerous legal requirements regarding notification and remediation that must be met in certain circumstances. To ensure you comply with regulations and laws in your industry, be sure to seek appropriate input from subject matter experts as you craft your shareholder communication plan.

TIP**Learn How to Communicate in a Crisis**

Many public relations firms specialize in crisis communications. You can work with this type of firm in advance to develop appropriate communications plans. You can also contract with these kinds of firms to assist with communications in the aftermath of a major event. In most cases, they can advise you on the best course of action, potential communications pitfalls, and provide guidance regarding certain legal issues. You may also need to get a legal opinion in certain matters, especially if death or injury occurred on your company's premises or as a result of company action. The PR firm you work with can help you understand how to communicate effectively and when to seek additional input before, during, and after your business disruption.

EVENT LOGS, CHANGE CONTROL, AND APPENDICES

In traditional IT, event logs track a variety of system and network activities. In a broader sense, you may choose to create a BC/DR event log for tracking various events and milestones. For example, your decision to activate your BC/DR plan may be based on two or three event types occurring, either simultaneously, in quick succession, or within a specified time period. These events may trigger the activation of the BC/DR plan itself, or they may signal the point in time when it's appropriate to move to the next stage in your plan. Having a chronological log of events can help clarify circumstances so appropriate decisions can be made in a timely manner.

Another very helpful process in managing your BC/DR plan is change control. As we've discussed throughout this book, your best approach usually is to operationalize many BC/DR activities. Adding assessments to hardware or software provisioning, for example, helps ensure you consider BC/DR when standing up new systems. What process do you have in place for updating your BC/DR plan when that occurs? What new or additional risk does it inject into your organization? Finally, you will likely want to add a section at the end for discrete sections of data as appendices. We'll discuss these in this section.

Event logs

As an IT professional, you're probably well versed in reviewing event logs as they pertain to systems and security events. However, in BC/DR, event logs are not necessarily logged by a computer system. In many cases, event logs are hard copies developed sequentially over time by making notes on what happens when. Event logs help you track events, in order, over time, and can help in identifying appropriate triggers for key activities.

Keep in mind that these logs establish who knew what and when, so they may become legal documents at some point in the future. You have to balance the need for timely information with the potential for litigation. As unfortunate as it may be, sometimes too much documentation leaves the company open to lawsuits, even when the company has acted as best it could given the circumstances. We don't suggest you do anything illegal or unethical—quite the opposite—but you may want to talk with your legal counsel to understand what can and cannot become evidence in the event there is a lawsuit that stems from some sort of business disruption. If something can become a legal document or be used as evidence in some manner, you should be aware of that going in. Your legal counsel may have recommendations about how to record data to minimize the possibility of litigation while maintaining accurate useful logs.

In the absence of specific legal advice on how to develop logs, the best general advice is to record only the relevant information and stick to the actual facts, not conjecture. Instead of "Barnett seemed confused by the request to review the equipment," you might simply say, "Barnett was contacted to begin reviewing the equipment at 11 P.M., 2/22/13" or "Barnett had numerous questions regarding the request to review equipment. Issue escalated to Barnett's boss, Martina." All these statements are true but the first statement contains conjecture—was Barnett confused or did you just assume he was because of the look on his face? If you state in your log that Barnett was confused, this might be the basis of a lawsuit claiming that appropriate action was not taken in a timely manner. Stating only the facts keeps everything moving forward and does not unnecessarily open the door to legal problems down the road.

On the other side of the legal coin, there may be legal or regulatory requirements to log certain events or make notifications within a certain time line. Event logs can help you operate within these legal requirements as well. For example, in health-care

IT, it often is critical to record when the system went offline, what steps were taken to notify clinical staff, and what work-arounds were put in place. If you operate under these constraints, be sure to include these requirements in your BC/DR plan, perhaps with hard copy templates of the event logs, so that your team knows clearly what the logging or notification requirements are in the stressful aftermath of a business disruption.

Change control

Change control is a necessary element in any project and BC/DR planning is no exception. There are two types of change control you'll need to develop. First, you need to devise a method of updating your BC/DR plan when change occurs in the organization that impacts your plan. Second, you need a method of monitoring changes to the BC/DR plan to ensure they don't inject additional uncertainty or risk into your plan. Let's look at both of these scenarios briefly.

As companies grow and expand, numerous changes occur to the organization's infrastructure. This can include departmental reorganization, the creation of new departments, the expansion to additional facilities, and more. It also comes with changes to the IT infrastructure including the location and duties of servers, the implementation of new applications and technologies, and the reorganization of existing infrastructure components. All these kinds of changes impact the existing BC/DR plan. These elements should be addressed in the plan maintenance activities, which we'll discuss in [Chapter 10](#). You can't control the change that occurs in the organization, but you can put in place a system for assessing change and how it impacts your BC/DR plan. In most cases, this occurs during the periodic review of the plan and we'll also review this with you in [Chapter 10](#).

A subset of change control is version control. Be sure to include a process for managing revision history for your BC/DR plan. Many people choose to simply put a small table at the beginning of the document outlining the changes in chronological order. [Table 7.1](#) shows an example of a revision history table that might be used in your BC/DR plan.

Table 7.1 Document Revision History Example

Revision Number	Revision Date	Detail
1.0	08.22.13	Finalize first version of BC/DR plan
1.1	09.20.13	Modify network diagrams in Section 4.2
2.0	09.30.13	Revise plan to include acquisition of ABC Co.
2.1	01.05.14	Include new specifications; contract for alternate site

You can define what constitutes a major and minor revision. Typically, going from 1.0 or 1.1 to 2.0 is considered a major revision (when the number to the left of the decimal point increases); going from 1.0 to 1.1 or 2.11 to 2.2 is considered a minor revision (when the number(s) to the right of the decimal point increase). Clearly, the numbering scheme is not quite as important as keeping track of revisions, unless you work in a company that has a very formal system for revision control in place. A quick note in the Detail section can help clue you in to the changes in the revision. Some people also like to document more extensive information about the changes and this can be done in the beginning of the document. For example, you could create paragraphs labeled, “Changes in Revision 1.1,” and note the key changes made to the document. This helps you see at a glance how the plan has changed without reading the entire document. There are numerous systems for managing revisions and you should select one that is consistent with the way your company operates. Don’t make it into a huge production or it may be circumvented, but do use some system for tracking changes so you don’t have to compare two documents side by side to figure out what changed between revisions.

Distribution

Although the plan is not yet complete, you should devise a strategy here for distributing and storing the final BC/DR plan. The revision history will help you and the team with version control, but you will still need a method of distributing the latest revision or notifying the team that a new version exists. In some cases, the plan may be stored in a software program that performs version control and revision notification. In that case, you’re pretty well set other than adding team members to the notification list. If you’re not using such a program, you can still maintain the plan on a shared, secured network location and provide team members or team leads with access to the folder. Keep in mind that this document is a very sensitive document and all precautions should be taken to ensure it does not fall into the wrong hands, is not leaked to competitors or to the media, or otherwise compromised. Use standard security and encryption where this document is concerned. Distribute the document in soft copy via e-mail only as needed. If possible, simply e-mail a notification that a new version is available while maintaining the document in the secure location. Remind people that the document is sensitive and should not be copied, distributed, or otherwise handed out. The document should only be distributed to those who have a defined need to know.

Finally, be sure you create a process or method for *printing* the updated plan so you have a hard copy version available if systems go down. The BC/DR team lead or leads should all have a paper copy in a secure location, both on-site and off-site. When new versions are available, old versions should be shredded or destroyed in a secure manner. Many companies distribute soft copy via CD-ROM, DVD, or thumb drive. That is helpful but in the event of a disaster, having a notebook you carry with you with the data you need at your fingertips might be helpful. It’s your choice, just make sure the plan is distributed and taken off-site and updated each time

there is a revision. That's a process your operations folks can take on, but it's one that has to be triggered through your change control process.

Appendices

Any information relevant to your plan that does not belong in the body of the plan should be attached or referenced as an appendix. There are no strict rules about what should or should not be included in the appendices, but it's usually detail required for successful implementation of the plan that may pertain to only one group or subset of BC/DR teams. For example, you might include the technical specifications of mission-critical servers in an appendix. As servers are moved, updated, or decommissioned, you can easily update the related appendix without modifying the plan itself.

Contracts with external vendors should be kept as appendix items so that they are located in one central place for reference. Your finance and/or legal departments may want to retain originals of these contracts, which are fine, but be sure to include copies in your BC/DR plan. If you have to activate your plan, you don't want to have to run around looking for someone from finance or legal to determine how and when you can activate your external contracts.

Templates for event logs, communications, and other predefined processes can be included. In event log templates, be sure to include time, date, event, notification requirements, legal, or compliance issues and other requirements so they're easily accessible in the event of a business disruption or disaster.

Key contact information should be included in the plan, but you may choose to include it as an appendix, especially if it changes frequently. If you choose to do this, you should include key contacts within the body of the plan and use the appendix for additional contact information, as appropriate. The reason for including the key contact information within the body of the plan is twofold. First, key contacts are integral to the successful activation and implementation of the plan. As such, that information should be incorporated into the body of the plan. Second, if that information changes, it should trigger a BC/DR plan revision. Key personnel need to be trained, they need to understand their roles individually and as part of the BC/DR team, and they need to be given the tools, resources, contacts, and information needed to do so successfully. If a key member of the BC/DR team leaves, for any reason, the person replacing them needs to be brought up to speed. This should trigger a quick review of the plan. If the successor has been assigned by virtue of position (the Facilities manager resigns and a replacement is hired), the replacement needs to be trained in all aspects of their duties with regard to the BC/DR plan. If the successor is not assigned and needs to be found, looking through the roles and responsibilities of this position can help you select the right person to fill the gap.

Any other information that is related to the plan that needs to be updated, maintained, and correlated to the BC/DR plan itself should be included as an appendix. Don't throw everything you can think of into an appendix and think you're covered. More is not necessarily better in this case, but do be sure to include key information

you'd want to have quick access to in the event of a natural disaster or other significant business disruption. To give you a few ideas about what else might be attached to your plan in an appendix, we've provided the following list. Not all of these elements are needed by every company, but you can pick and choose based on your unique situation.

- Critical work space equipment and resource information and related vendor data
- Critical IT hardware, software, equipment, and configuration information, and related vendor data
- Critical manufacturing, production, and warehousing information, and related vendor data
- Critical data and vital records information, including storage and retrieval information
- Alternate IT or work-site information
- Crisis management center resources and information
- Insurance information including all relevant policies, policy numbers, and insurance contact information
- Letters of authorization, passcodes, key codes, and other access information that can be safely stored in such a document
- SLAs (that you must provide to customers or that vendors must provide to you)
- Standards, guidelines, policies, and procedures
- Contracts related to BC/DR
- Forms
- BC/DR plan distribution list
- Glossary

Every company and every BC/DR plan is different, so there is no hard-and-fast rule about where information belongs, as long as critical data are included in a logical manner. If writing a plan or organizing data is not your strong suit, be sure to recruit assistance to draft a plan that makes sense. It should follow a logical progression and match the way your company does business to the greatest extent possible.

Additional resources

What other resources do you need to successfully implement and maintain your plan? In the next chapter, we'll discuss emergency and business recovery plans, so some of this may come up in that context. However, if there are communication tools, equipment, or resources you think of as you develop your plan, they should be noted in a section called Additional Resources (or other similar heading), and they should be added to your WBS to ensure someone takes ownership of gathering these needed resources.

WHAT'S NEXT

When you complete the work in this chapter, you should have a fairly robust BC/DR plan in the works. It will have gaps related to specific emergency and disaster recovery efforts (see [Chapter 8](#)), and in training, testing, auditing, and maintaining the plan

(see [Chapters 9](#) and [10](#)), but other than that it should be well on its way to completion. If not, step back and review your data, your plan, and your company to determine what is missing and how you can address those gaps.

SUMMARY

Putting your business continuity and disaster recovery plan together requires pulling together the data previously developed and adding a bit more detail. Understanding the phases of the BC/DR plan helps you develop strategies for managing activities if you have to implement your plan. The typical phases are activation, disaster recovery, business continuity, and resumption of normal activities. The plan must also be tested and maintained, regardless of whether it's ever implemented.

Potential disruptions need to be categorized and we discussed three levels: major, intermediate, and minor. By clearly defining these for your organization, you can ensure you understand what recovery steps should be implemented. This will define how and when you activate your BC/DR plan. After the plan is activated, a trigger should define when disaster recovery tasks begin. These recovery tasks should be well defined in your BC/DR plan and we'll cover these in detail in the next chapter. The transition from disaster recovery to business continuity should also be well defined so that you can begin to resume business activities, though things will not be back to business as usual at this juncture. This is also discussed in detail in the next chapter.

Developing your BC/DR teams is a vital part of your planning. There are numerous roles and responsibilities in each phase of your BC/DR work, and defining these and populating your teams in advance are crucial to your success if the plan is ever activated. In addition, these teams will need to be trained in implementing the BC/DR activities. Training is discussed in detail in [Chapter 9](#).

After you've created your teams, you can further develop your planning tasks and assign resources, timelines, and budgets. You can identify task dependencies, develop milestones, and create completion criteria for key tasks. Since each company's set of tasks will vary widely, we presented only a sampling of high-level tasks related to acquiring an alternate computing site and contracting with vendors.

Communications plans are part of the BC/DR process because if a business disruption occurs, many different groups of people will need status updates and information. This includes employees, management, shareholders, vendors, customers, and the community, among others. You'll need to decide who needs to know what and when they'll need to know it. Then, you'll need to develop distribution methods appropriate to those groups (and to the circumstances of the disruption).

Event logs can help you manage the business disruption from start to finish, but remember that these may become legal documents later on. You may wish to consult with your legal counsel regarding what should and should not be included in the event logs. For example, it's generally considered fine to include facts but not

conjecture or opinion. Sticking to the facts helps keep the log clear and concise and can avoid misinterpretation of data. In addition, there may be legal or regulatory requirements for event logging or notification, so be sure to include this in your process and make a note of it in any log files you develop (whether soft or hard copy).

Keeping track of document revisions is a bit of a “housekeeping” task but an important one when it comes to your BC/DR plan. Use a simple, concise method of ensuring that the plan is updated and that everyone has the latest plan. Develop a method for distribution and storage of the plan so that it’s accessible to key personnel in the event of a disruption. Finally, include additional data such as technical requirements, SLAs, and vendor contracts as appendices to the main BC/DR plan. Keeping all relevant data with the plan can make plan implementation and maintenance much easier.

KEY CONCEPTS

Phases of business continuity and disaster recovery

- The various phases of the BC/DR cycle include activation, disaster recovery, business continuity, and maintenance/review. Plan maintenance and review occurs periodically, regardless of whether or not the plan has ever been activated.
- The activation phase occurs when a disaster or business disruption occurs, and it is determined that the plan should be implemented. Clear directives on how and when to activate the plan should be included.
- The disaster recovery phase includes the tasks that must be undertaken to stop the impact of the event and to begin recovery efforts. This includes damage assessment, risk assessment, salvage operations, as well as the evaluation of appropriate alternatives and solutions.
- The business continuity phase entails the activities required to restore the company’s business operations. This assumes disaster recovery has been completed and that the business is up and running in a limited mode. This is not yet business as usual and may involve the use of temporary solutions and work-arounds.
- Maintenance and review are similar phases. Maintenance requires a review of the plan from time to time to ensure everything is still current and that changes to the company or its infrastructure are reflected in the plan.
- Review occurs after the plan has been activated and implemented. Gathering lessons learned and updating the plan with new information gleaned from the experience help the organization avoid making the same mistake twice and help the organization learn from the experience.

Defining BC/DR teams and key personnel

- You should have already identified key personnel, positions, skills, and expertise needed for your BC/DR activities. In this phase, you should form your BC/DR teams based on those stated needs.

- There are many different types of teams you may need. In smaller companies, people may take on multiple roles. Be sure teams are large enough to accommodate the potential that one or more team members may be unavailable during or after a disaster (for a variety of reasons).
- Key personnel should also be identified at this time. This may include certain members of the executive or management team, people or vendors with specific skills needed, and the like.

Defining tasks and assigning resources

- Tasks, owners, timelines, budgets, dependencies, and completion criteria are among the details that should be developed for BC/DR plan activities. Additional detail and checklists are provided in [Chapter 8](#).
- All the tasks needed to activate, implement, manage, and monitor the BC/DR plan in action should be defined. You can create project plans for each subsection of work or develop detailed checklists.
- Be sure to note key internal and external dependencies for tasks. Milestones should be added to your project plan or as items on a checklist.
- Maximum downtime and other time-based objectives should be noted and addressed within the project plan or checklist.
- Contracts for alternate sites, equipment, and other products/services should be defined in the BC/DR plan as well. The finalized contracts can be added as appendices to the final BC/DR document. Include SLAs, where applicable.
- Address MTD and other constraints along with legal or regulatory requirements that must be met in the aftermath of a disruption to ensure continued compliance.

Communications plans

- There are many different kinds of communications needs during and after a major event, disruption, or disaster. You should develop plans for communicating with various stakeholders in these cases.
- Management and employees require communication regarding the current status of the business, where/when/how to report to work, who to contact for information, and so on. This often is handled by the HR team, who can be tasked with managing the employee communication plan.
- External communications are needed to contact key customers, vendors, suppliers, and contractors to notify them of the event and the company's next steps.
- Communications with local, national, and international media may be required. In these cases, it's best to have someone from the company who is trained in media relations handle these communications. PR firms often offer plan development, training, and guidance in the aftermath of an event.

- In some cases, the information communicated can become the basis of legal action in the future. Therefore, you should consult with your company's legal counsel or an expert in media relations to determine how, what, when, and where information should be communicated. This should be done before any emergency communication is needed.

Event logs and change control

- Event logs, like emergency communication, can become the basis of legal action, so be sure to understand the requirements and constraints various kinds of emergency reporting may have on your company.
- Event logs help you keep track of what's going on, what's been done, and what needs to be done next. Keeping detailed logs in real time helps keep track of details that might later be lost.
- Your company may be required to meet certain legal or regulatory reporting requirements. Event logs can be helpful in ensuring you meet those requirements. Consult with legal counsel if necessary and include these requirements in soft or hard copies of your logs.
- Changes to the BC/DR plan should be tracked and noted so that team members can easily determine if they have the latest revision of the document as well as the general nature of those revisions. Be sure to develop a distribution system that notifies team members of new revisions, provides a method for accessing new documents, and reminds teams to print and store the documents in locations accessible both on- and off-site.
- BC/DR plans should be treated as confidential documents. They should be handled and stored in a secure manner and old copies should be destroyed appropriately.

Appendices

- Information that should not be included in the body of the plan but that is nonetheless vital to the plan should be included at the end as an appendix.
- Appendix data can include event log or other document templates, vendor contracts, technical specifications, SLAs, customer contacts, or any other relevant data that would be useful to have along with the BC/DR plan if/when it's activated.

References

Brandon J. How to use the cloud as a disaster recovery strategy; 2011. <http://www.inc.com/guides/201106/how-to-use-the-cloud-as-a-disaster-recovery-strategy.html> [Retrieved May 26, 2013], from Inc.

Kravets D. Feds say no dice in retrieving your data seized in megaupload case; 2012. <http://www.wired.com/threatlevel/2012/10/no-dice-megaupload-data/> [Retrieved May 26, 2013], from Wired.

This page intentionally left blank

Business Continuity and Disaster Recovery in Financial Services

IN THIS CHAPTER

- Finance industry requirements for business continuity
 - Industry impact—September 11 attacks
 - Industry impact—super storm Sandy
 - Industry impact—cyber threats
 - Looking forward
 - Summary
-

OVERVIEW

Over the past several decades, the financial industry has become fully electronic. Every transaction, from a check deposit made via a smart phone to a trade on one of the world's stock exchanges, is done electronically. With the rise in the use of technology for real-time trading, transactions, and reporting has come the need to develop highly reliable, redundant, and fault-tolerant systems. In tandem has come the need to develop sophisticated disaster recovery solutions to meet the needs of millions of companies and billions of customers worldwide. In this chapter, we'll look at some of the aspects of the financial industry as it relates to business continuity and disaster recovery (BC/DR) and we'll take a look at what happened during some recent events—from super storms to cyber threats. Finally, we'll look at what is being done today to provide resiliency tomorrow.

FINANCE INDUSTRY REGULATION OVERVIEW

In the United States, there are numerous regulatory bodies that oversee financial services. If you work in this sector, you are likely well aware of the regulatory bodies that oversee your particular business. However, we'll review just a few of these and we'll touch on those in other countries to give you an idea of how tightly this industry is regulated around the world. Clearly, these regulations impact the way in which you'll develop your BC/DR plans, so having a basic understanding of these is crucial. Your legal or compliance officer can also provide valuable input into what is required to develop a compliant BC/DR plan.

Clearly, there are a wide variety of financial organizations ranging from banks to securities to credit bureaus, financial planning, and more. Though there are

significant differences among these types of firms, they are all subject to a similar set of financial regulations with respect to BC/DR and we'll focus on this area.

United States financial regulation

In the United States, the Federal government provides regulatory oversight for most financial transactions. Unlike many European countries, the United States maintains separate regulatory agencies for different financial industry sectors—including banking, securities, commodities, and insurance regulatory agencies at the federal and state level such as Federal Deposit Insurance Corporation (FDIC), Financial Industry Regulatory Authority (FINRA), and Office of the Comptroller of the Currency (OCC) among others. We discussed many of the overarching regulatory aspects in [Chapter 2](#), so you may want to refer back to [Chapter 2](#) for more in-depth discussion.

The U.S. Department of the Treasury is responsible for a wide range of activities such as advising the President on economic and financial issues, encouraging sustainable economic growth, and fostering improved governance in financial institutions. The Department of the Treasury operates and maintains systems that are critical to the nation's financial infrastructure, such as the production of coin and currency, the disbursement of payments to the American public, revenue collection, and the borrowing of funds necessary to run the federal government.

The OCC's primary mission is to charter, regulate, and supervise all national banks and federal savings associations. They also supervise the federal branches and agencies of foreign banks. The OCC was established in 1863 as an independent bureau of the U.S. Department of the Treasury.

Another notable organization is the FINRA, the largest independent regulator for all securities firms doing business in the United States. FINRA's mission is to protect America's investors by making sure the securities industry operates fairly and honestly. All told, FINRA oversees about 4275 brokerage firms, about 161,550 branch offices, and approximately 629,980 registered securities representatives.

During the 9/11 attacks in 2001, securities firms were directly impacted by the attacks and their BC/DR plans were not only implemented but severely tested. FINRA has long maintained standards for BC/DR readiness. Rule 4370, FINRA's emergency preparedness rule, requires firms to create and maintain business continuity plans (BCPs) appropriate to the scale and scope of their businesses, and to provide FINRA with emergency contact information ([Financial Industry Regulatory Authority, Inc., 2013](#)). We'll discuss these plans and tests a bit later in this chapter.

In addition to these, there are many others—including (but certainly not limited to) the FDIC, Consumer Financial Protection Bureau, Federal Reserve Board, Federal Trade Commission, National Credit Union Administration, and the Securities Exchange Commission.

If you're interested in learning more about financial oversight in the United States, there's an interesting document available from the Congressional Research Service (CRS) titled, "Who Regulates Whom? An Overview of U.S. Financial

Supervision,” available on the Open CRS Web site at: http://assets.opencrs.com/rpts/R40249_20101208.pdf (Jickling and Murphy, 2010).

We’ve really only scratched the surface of regulatory bodies, and we haven’t looked at State regulatory bodies at all. This section is not intended to be an exhaustive look at U.S. financial regulatory bodies but merely an opening for you to do further research if your interests lie in this area.

European financial regulation

The European Union (EU) is a unique economic and political partnership between 27 European countries that together cover much of the continent.

The EU was created in the aftermath of the Second World War. The first steps were to foster economic cooperation: the idea being that countries that trade with one another become economically interdependent and are more likely to avoid conflict. The result was the European Economic Community (EEC), created in 1958, and initially increasing economic cooperation between six countries: Belgium, Germany, France, Italy, Luxembourg, and the Netherlands. Since then, a huge single market has been created and continues to develop toward its full potential.

What began as a purely economic union has evolved into an organization spanning policy areas, from development aid to environment. A name change from the EEC to the EU in 1993 reflected this ([European Union, 2013](#)).

With the creation of the EU, financial regulation has been primarily the purview of three regulatory bodies (there are numerous, these are three of the prominent bodies). The European Systemic Risk Board, the European Banking Authority, and the European Securities and Markets Authority are responsible for overseeing financial activities within the EU. These organizations, along with others, are directed by the EU and as such provide a single set of regulations for EU members.

While each financial institution in each country must address its own disaster preparedness, the EU itself organizes EU-wide discussion on disaster preparedness, risk management, and insurance issues. The distributed nature of the EU mitigates some financial system risks and introduces others.

Other regions’ financial regulation

There are hundreds of countries outside the United States, Canada, Mexico, and EU, and there are more regulatory bodies than countries. Clearly, some of the larger governing bodies influence regional and worldwide financial activities, including disaster recovery. Think back to the tsunami in Thailand or the tsunami that hit Japan—both events had significant impact on the country’s economies and on the institutions within those countries. For an interesting list of financial regulatory bodies around the world, you can start with an article on Wikipedia at: http://en.wikipedia.org/wiki/List_of_financial_regulatoryAuthorities_by_country (Wikipedia, 2013).

The sophistication of various financial regulatory bodies dictates the depth to which they may have reviewed and/or regulated BC/DR requirements for

participating organizations. Clearly, financial institutions (whether local, regional, or international) must have plans in place to deal with disasters from natural disasters to cyber threats.

FINANCE INDUSTRY REQUIREMENTS FOR BUSINESS CONTINUITY

In [Chapter 2](#), we covered the high-level requirements for financial industries. What is important to take away from that chapter is the notion that financial institutions must have plans in place to protect the confidentiality, availability, and integrity of financial data. These three aspects, often referred to as CIA, are integral to any information security plan.

Financial data must remain confidential, available, and unaltered, even in the face of serious events and disasters. As was witnessed during the 9/11 attacks, financial institutions closed briefly to regroup and recover, but once back online, there were no serious issues with financial records being missing or incorrect for large institutions.

All financial institutions must ensure all data are safe and recoverable. As you'll see from the examples we'll discuss next, that's becoming both more challenging (e.g., cyber threats) and more achievable (e.g., virtualization, private cloud).

INDUSTRY IMPACT—SEPTEMBER 11 ATTACKS

Financial services firms in and near the World Trade Center were severely affected by the 9/11 attacks. The industry experienced an unprecedented loss of lives and property, requiring massive, long-term relocations to contingency sites and dedicated efforts to protect and reassure staff. The destruction of telecommunications infrastructure supporting lower Manhattan disrupted the telephone connections for several days between the whole nation and financial markets and intermediaries located in the lower Manhattan financial district. This disruption created bottlenecks in the processing of financial transactions and caused a temporary—but severe—dislocation of liquidity for financial institutions. The primary markets closed temporarily, to facilitate disaster recovery efforts and to ensure fair and orderly markets, until telecommunications could be restored.

Despite the shock, long-term devastation, and disruption of public infrastructure and commercial activities in the world's financial center, the U.S. financial system largely remained open throughout the day and thereafter. Banks and other financial intermediaries stayed open. Key wholesale and retail payments system remained operational, like other financial activities, except to the extent that telecommunications disruptions had a temporary or local effect. Even firms in the

World Trade Center were able to resume business from other offices or from contingency sites within hours of the attack. The response of the financial industry and the speed with which it resumed business was extraordinary and can be attributed only to its long-standing commitment to, and extensive preparations for, ensuring continuity of operations in the wake of physical and cyber disruptions (Ferguson, 2002).

As the world watched the horrific events of September 11, 2001 unfold, numerous financial firms began wondering what the impact would be to their employees and to their businesses. The World Trade Center towers were in the heart of the New York financial district. Many trading and financial firms were located in the towers that fell. Their backup systems were just a few miles away—just across the river in New Jersey or on Long Island. More than half of the small-to-medium financial enterprises that were impacted by 9/11 never resumed operations. Several large firms were impacted because their data centers were relatively close to one another, their staff for both data centers were impacted by the same disaster, and their data centers were on the same power grid.

In light of those events, many large financial firms made significant changes to their business continuity solutions. Merrill Lynch lost two data centers on 9/11 and subsequently decentralized their core IT functions. Today, they have a main data center on Staten Island and a backup data center in Manhattan. Both are on separate power grids and far enough away from each other that they would be less likely to both be impacted by another attack or a failure of the power grid. Morgan Stanley also had data centers that were close to one another before 9/11 and subsequently separated them after 9/11.

In a February 2002 meeting between members of the Federal Reserve Board and several large financial institutions in the aftermath of 9/11, numerous recommendations were made including:

- “Business-resumption plans need to be expanded to provide for wide-scale and regional events. They also should take into account the loss or inaccessibility of staff.
- Obvious vulnerabilities are associated with the current geographic concentration of market participants and some of their backup facilities. As a result, geographic diversity for critical operations and backup facilities should be a key consideration of business-resumption plans.
- Institutions should identify their critical business lines and the systems or business processes that support those lines, including closely related activities that should have the same level of resiliency. They should also consider the extent to which their critical business lines depend on external parties—market utilities, major counterparties, and customers—and how to mitigate the risks that dependence poses for the continuity of operations.
- Make certain that business continuity arrangements will be effective and compatible within and across institutions. The industry can accomplish this effectiveness and compatibility only through developing multiple levels of

backup, depending on the criticality of the function or business line. Moreover, the discussion group believed that industry participants must engage in robust testing of their contingency plans and backup facilities, internally and with financial utilities.

- Business-resumption plans should reflect recovery-time objectives for critical functions. Previous assumptions about how long backup facilities may need to be used and their capacity levels should be revised to incorporate the possibility of longer-term disruptions and to accommodate normal or increased volume of transactions—as occurred when the markets reopened on September 17” ([Ferguson, 2002](#)).

In addition to addressing the technology issues, large financial firms have come to understand the importance of people and process. In the aftermath of 9/11, there was no staff available to address disaster recovery. When staff in one area are overwhelmed dealing with a disaster, having data in a nearby location is not helpful. For smaller firms that are not geographically distributed, this can be a problem regardless of where the backup data center may be located.

Another lesson learned in the financial sector was to test disaster plans. While it's not clear exactly how many financial services firms had BC/DR plans before 9/11, it became clear after 9/11 that plans were needed and they needed to be tested. Many companies now conduct full or partial fail over tests, and trading companies practice trading from their alternate location to ensure they can still run systems and manage their businesses.

Though the lessons should have been deeply ingrained from 9/11, even a decade later, many companies still struggle to have a meaningful BC/DR plan in place.

Ten years ago, Wall Street firms' back up data centers were often located just a few, unsafe, blocks away. Traders and other workers did not tend to work remotely. Few people had smart phones. (Research In Motion had just developed the BlackBerry in 1999.) Disaster recovery planning cost millions of dollars, and few firms were willing to spend the money on an area that didn't have an immediate business value.

Fastforward to 2011: working remotely has become pervasive on Wall Street and elsewhere and no one can imagine life without their BlackBerry or iPhone; Wall Street firms generally have back up data centers tucked safely away in New Jersey or Pennsylvania; and strict regulations on disaster recovery, whereby firms must have contingencies for providing customers with access to their funds and securities during a disaster, as well as data backup and recovery, an alternate physical location for employees, and communication among the firm and its employees, have forced firms to rethink their business continuity plans ([Rodier, 2011](#)).

Over the past 5 years as various financial industry firms have weathered the financial storms in the United States, they have made cuts to staffing and technology. Cost cutting and layoffs have left many firms vulnerable because they have neither the staff nor the expertise left to regularly test and verify their BCP's.

As concerning is the proliferation of storage requirements. As more electronic records are created, they must be stored and made available per regulatory requirements (as well as to meet business and consumer needs).

More than a decade later, there are smaller firms who cannot confidently state that they could restore their data within the service level agreements they have committed to (or required to by regulation). These untested organizations are playing a bit of business roulette, betting that there's a good chance they will not need to utilize their BC/DR plans to the same degree ever again. However, as we'll see in the Hurricane Sandy section (next), many of these same firms were tested when power went out and storm waters inundated lower Manhattan.

Many financial firms were hard hit during the recession that began in 2008. Many found themselves struggling to simply survive—spending on backup and recovery solutions was not only low on the list of priorities, it was often a source of savings many companies used to maintain solvency. Unfortunately, that approach now leaves these same firms vulnerable to any number of disasters that could, in one swipe, simply put them out of business. Moreover, in today's landscape of increasing cyber threats, these same firms are extremely vulnerable to having their data hacked, altered, or stolen. As we've referenced throughout this book, cyber security is very much part of the business continuity and disaster recovery realm as BC/DR is intended to ensure the confidentiality, integrity, and availability of data regardless of the event that occurs. Many financial firms may be more at risk today than they were just over a decade ago.

Sang Lee, founder and CEO of the advisory firm, Aite Group, agrees that Wall Street has been struggling to handle spiraling amounts of data. Most have not yet settled on an efficient way of dealing with it, he says. ‘Firms have focused on being able to access data from different locations, but there’s a risk involved in that as well, a risk that you could lose your data altogether,’ he asserts. Firms need multiple instances of backup. ‘It’s not a cheap proposition. The larger firms can deal with it by throwing resources at it. But smaller firms have a lot more challenges.’

Cloud computing is a more cost effective way of managing data, Lee adds. ‘And it will play a role in the future for small to mid-size firms.’

Tabb agrees that private clouds, including new offerings such as NYSE’s cloud or Thomson Reuters’ Elektron could help firms achieve robust continuity and direct access at all times. ‘The cloud could be a very powerful tool to help with that in the future.’ (Rodier, 2011)

According to Thomson Reuter's Web site, "Elektron brings together the global financial community, facilitating mission critical information flows between clients, counterparties and service providers. Elektron connects the global financial community. 96 of the top 100 banks; 19 of the top 20 asset managers; 8 of the top 10 hedge funds and 10 of the top 10 global exchanges are already part of the Elektron community" (Reuters, 2013). This single solution is just one of the advances in financial service BC/DR management that has been developed. These solutions are enabled by

advances in virtualization, cloud-based services, and globalization of a wide range of services.

While this is a high-end solution for larger organizations, it shows the general trend toward managing BC/DR solutions with third-party developed solutions rather than each company creating its own. This certainly is likely to ensure broader adoption through a common platform, assuming it is affordable and useful to participating organizations.

INDUSTRY IMPACT—HURRICANE SANDY

Both Hurricane Sandy and Hurricane Katrina were dubbed *super storms*. These storms were massive storm systems that impacted enormous areas simultaneously. To have a regional BC/DR solution for these disasters would have been completely inadequate. As any organization (financial or otherwise) in a hurricane-prone region knows, BC/DR backup sites need to be far outside the region to avoid being impacted by a single super storm.

The storm hit in late October 2012. The New York Stock Exchange shut down for 2 days while power was out and water was lapping at the doors of the Exchange. However, markets were up and running on Wednesday, October 29, 2012. After shutting down in advance of one of the largest Atlantic storms in history, worldwide clients expected the industry's computer systems, financial data, and trading platforms would all come back online and start working instantly after the storm passed.

Of course, the New York area had been hit with a number of crises over the past decade—from the attacks of September 11, 2001, to a major blackout in 2003 and Hurricane Irene in 2011—all of which have left firms more prepared to face worst-case scenarios. They were not only prepared, but they had advanced notice, which lead to the best possible outcome given the circumstances.

Financial companies, in particular, developed trilateral solutions, which provide high availability locally as well as redundancy further away. Creating a regional data center that staff could commute to (within 50 miles of each other, for example) provides one layer of protection. Developing a remote data center that may be in another region or even another country helps provide the next layer of protection.

The global nature of firms' assets distribution, including skilled resources, also allows for work redistribution, whereby New York activities are picked up temporarily by London, Singapore, Tokyo, and elsewhere. As IT technologies have advanced (especially since 2001) and financial firms have become more aware of regional risks, they have distributed their resources and reduced their risks accordingly (Mamudi, 2012).

In the aftermath of the massive impact from Hurricane Sandy, one financial services organization surveyed its members on six key metrics. One of the key differences with this storm versus others was that people along the U.S. east coast had ample notice of the impending disaster. That's not always the case with large disasters, but there were many lessons learned from Hurricane Katrina, whose path was

also tracked for days, that were leveraged in advance of Hurricane Sandy. The six key metrics surveyed were:

1. Business continuity preparedness
2. Disaster recovery
3. Supply chain disruptions
4. Response
5. Recovery
6. Risk mitigation

The results were quite interesting. Overall, few had to fail over to their DR sites, but that was largely because of the ability to take precautionary steps in advance of the storm. Firms regularly communicated with key stakeholders, the community, and customers via e-mail, phone calls, and Web site postings. Many staff were able to work remotely; however, many staff lacked power or Internet connectivity and were unable to telecommute. As expected, many staff were more concerned with the welfare of their families than they were their company's business, and numerous staff were unavailable as a result. Finally, it was clear that regular and relatively recent business continuity preparedness and awareness training activities had paid off.

Due to the tidal surge and the power grid going down in lower Manhattan, one of the key lessons learned, as we've discussed numerous times, is that potential regional impact should be considered when creating BC/DR plans. Hurricanes and earthquakes tend to have the largest regional impacts, so for those of you in areas that experience these two types of disasters, you should absolutely be thinking outside your region.

Hurricane Sandy also showed that even large firms were still subject to the vagaries of nature as Wall Street and trading firms in lower Manhattan were impacted by surging flood waters, a downed power grid, and employees who could not make it to work nor could connect remotely as most of their staff live in the area. Large financial firms did have the distinct advantage of having thousands of staffers outside the impact area that would work remotely, move data to safer sites, and shut down systems. This may have minimized the impact of Hurricane Sandy for larger firms. Smaller firms were not so fortunate. However, all financial firms were impacted by the NYSE being offline for 2 days. Operational events such as failures to deliver, access to cash, money markets, and settlements were impacted by the market closings.

What lessons were learned and what can you apply to your BC/DR efforts, whether you work in the financial industry or elsewhere?

1. Regional planning is insufficient in areas where large regional events are likely to occur, most notably (in the United States) hurricane and earthquake. Elsewhere, tsunamis have to be taken into consideration.
2. Don't count on key staff being available. They may not have access to transportation or they may not have basic utilities at their homes. They will be more concerned with their own welfare and will make efforts to preserve family and friends before jobs.

3. Many firms do not take into account several things going wrong at once. In this case, flooding, the shutdown of public transportation, the shutdown of power, and the lack of availability of key staff all impacted firms simultaneously.
4. Over 90% of the financial firms surveyed had dedicated DR sites; just under 10% did not. Having a dedicated recovery site helped reduce downtime and recovery time.
5. Almost 97% of the financial firms have an employee notification system that was very useful in communicating with staff before, during, and after the event.
6. About three quarters of the firms had key vendor contact information included in their BC/DR plan. This was critical because another major impact of the storm was on supply chain.

In summary, Hurricane Sandy came several years after Hurricane Katrina and the 9/11 attacks. It appears many financial services firms learned to be prepared, to be proactive, and to activate their plans in advance. These steps were lessons learned from previous disasters and have served the financial industry well in the past decade.

INDUSTRY IMPACT—CYBER THREATS

According to a 2012 Deloitte study, the top threats are mobile technology and social media vulnerabilities, financial fraud, and “hacktivist” groups. And while 80% of all banks think their security is good, more than a quarter of the world’s banks experienced security breaches in 2012. Additionally, about 40% of all major insurance companies also experienced breaches during the same time period. Survey results show that most companies are hampered by inadequate funding for security efforts and increasingly sophisticated threats, including state-sponsored cyber terrorism ([Deloitte, 2012](#)).

According to the Deloitte report, 20% of financial organizations spend less than 1% of their IT budget on information security. Since 2008, customer impersonation is up to 300% and, of course, financial services are the most affected by this trend ([Deloitte, 2012](#)).

If you work in the financial services industry, you are well aware of the constant threats to your data and the critical importance of ensuring your data is secure. Interestingly, the street value of credit card and consumer identity data has dropped compared to the value of medical identity data, although there is still an enormous market for stolen financial data. Listen at any company break room or in the hallways and you’re sure to hear what has now become a familiar story—the bank sending a new credit card because of the possibility the credit card was compromised. Unfortunately, though these automated phone calls and automatic card replacements were rare even 5 years ago, they are now the norm for most consumers. While it’s heartening that financial companies including banks and credit card issuers are taking these problems seriously, it doesn’t change the fundamental issue: financial data are compromised with increasing regularity.

This is not to say that financial institutions are not doing their best to keep financial data secure, but given the alarming statistic reported a PWC report ([Potter and Waterfall, 2012](#)) that 20% of financial institutions spend less than 1% of their revenue on information security, it's surprising there haven't been more dramatic attacks "The types of attack, the execution and exploitation require significant resources and coordination, which implies professional hackers and organized crime have taken over a domain once ruled by 'script kiddies' and one-off hackers," says Mike Maddison, director of security and privacy services at [Deloitte \(2012\)](#).

Phishing and pharming accounted for more than half the external attacks, while insider fraud (28%) and leaking customer data are the most common internal threats. Typically, those companies that experienced a security breach say the direct and indirect costs of the damage are £0.5 m (\$0.77M USD). This doesn't speak to the loss of consumer confidence and the potential negative effect to brand and reputation ([Computer Weekly, 2006](#)).

An April 26, 2013 article from MIT Technology Review reported that a computer hobbyist pinged every computer on the Internet (about 3.9 billion devices), and he found that many were vulnerable due to basic security flaws such as default passwords, open ports, lack of vulnerability patching, and more ([Simonite, 2013](#)). This points to one of the most fundamental aspects both of information security and BC/DR: spend your time focusing on the basic vulnerabilities first then look for more sophisticated approaches. Many companies spend time and effort worrying about more sophisticated issues when the basics are not addressed. The largest payoff will be in focusing on ensuring you have all the fundamentals covered. It's not only the smartest way to approach BC/DR but also the most practical. Once you address the "small things," you've reduced your footprint by 80%. Casual hackers and weekend hobbyists are not going to accidentally breach your systems because you left the door wide open. Next, you'll have to worry about the remaining 20%, which are attacks carried out that are specifically targeting your business, your industry, your region, or your country in particular. These are more complex threats, often carried out by professionals, political hacktivists, or even other countries' governments, but you can focus on these complex threats once you've addressed the basics. Needless to say, it's also far less difficult to explain how that your systems fell victim to a sophisticated professional hack than to explain why you left default passwords on your routers.

Increasing threats, increasing business requirements, and an always evolving regulatory environment make information security a top priority for the financial services industry. Financial service companies are becoming more proactive in their security approach, but all are facing the same challenges—increasing threats, sophisticated technologies, and limited budgets.

Information security is an increasingly important part of BC/DR and while we're not focusing on information security in this book, it's a constant theme. Cyber threats are becoming big business—for the criminals and, unfortunately for us, for the companies that sell tools and remediation services. It's a natural shifting of market

resources and it's a trend that has just begun to coalesce. In the coming decade, we'll see more sophisticated tools and techniques and all vital information and systems will be interconnected.

LOOKING FORWARD

How are financial institutions dealing with BC/DR in light of increasing reliance on technology, including mobile technologies? How are they addressing natural disasters and cyber threats?

According to the 2012 Deloitte Financial Services Industry survey, nearly half of banking respondents have already implemented or purchased cloud computing services. Of those who have not implemented cloud computing services, close to 90% of the respondents believe the benefits outweigh the security risks. Cloud services are not without controversy—some large outages over the past several years have demonstrated that even highly redundant, highly available, and highly secure cloud resources can still be vulnerable to attacks and downtime ([Deloitte, 2012](#)).

Still, many firms are assessing cloud storage and/or cloud computing as this provides one of the most cost-effective DR solutions for many organizations. Whether cloud storage or computing is appropriate for your financial institution is a decision you'll have to make based on the cost/benefit analysis as well as the overall risk profile such a move would create.

Though the move to cloud computing is not necessarily without its challenges, there has been a dramatic move toward virtualization, a precursor for cloud computing. Many mid-sized and large companies are virtualizing their servers in order to remove the one-to-one relationship of hardware and software. By doing so, they can reduce risk and cost while increasing efficiency and consistency. The benefits of virtualizing are well known at this juncture, and there are few firms that don't understand how it might positively impact their environment. Moreover, it enables companies to save configurations and spin up new servers in a matter of minutes thousands of miles away. The ability to run parallel environment or even hot sites makes virtualization a benefit to daily operations and to BC/DR planning.

While most companies virtualize servers first, one banking firm found that it made more sense to virtualize its desktop environment first. The bank, which supports about 300 PCs, decided there was greater financial benefit to virtualizing its desktops because in the event of a disaster, they could instantly pull up an image and use a virtual desktop from anywhere.

Desktop virtualization shifts the cost and administration from the desktop to the server environment, and sometimes the cost trade-off doesn't actually balance out. However, if you add the benefit of "a desktop anywhere" and include this as part of your BC/DR ROI analysis, you might find it does make sense for your firm.

Regardless, cloud computing and virtualization (server and desktop) are the two current trends driving financial institutions IT departments with respect to BC/DR.

The use of mobile devices will also continue to shape the industry. That makes accessing data anytime, anywhere much easier - for the good guys and the bad guys. Of course, the same can be said of many other industries. However, finance (along with healthcare and utilities) is held to very high standards for data security, integrity, and availability. As such, each firm must evaluate its current infrastructure, its future plans, and its risk profile and determine what technologies make sense going forward.

SUMMARY

The globalization of financial services has led to the need to develop solutions that span time zones and countries. Given this imperative, financial services firms have developed technical solutions that provide high availability and high reliability. These solutions have worked well in times of natural disasters and terrorist events, though lessons have been learned after each incident.

The September 11 attacks in the United States showed the vulnerability of the financial industry with resources and assets tightly grouped around Wall Street and Manhattan. Since that time, the financial industry (in particular) has developed leading edge solutions for ensuring business continuity. Most notably, they have developed trilateral recovery solutions—primary, local secondary, and remote tertiary—compute and storage locations. This alone reduced much of the risk when subsequent events hit the area.

The increasing use of cloud compute and storage capabilities is another clear trend, though many financial institutions are leery of the security of such solutions. Combined public/private solutions (hybrid cloud solutions) is gaining acceptance, but each firm must determine whether these solutions meet the unique needs of the organization. Virtualization has enabled the use of trilateral solutions and ensures configurations are consistent and reliable across the locations.

The financial services industry has developed global solutions to shift computing load to other areas and to rely on those resources located outside the reach of a disaster.

The growing threat is cyber security, and financial institutions are in the bull's-eye of attackers. They will continue to have to invest in proactive monitoring, BC/DR solutions for when breaches do occur and continue to stay two steps ahead of the bad guys. That's an expensive and never-ending proposition, but that's the reality of financial services in today's world.

References

- Computer Weekly. Finance firms face surge in security breaches; 2006. <http://www.computerweekly.com/news/2240063046/Finance-firms-face-surge-in-security-breaches> [Retrieved May 24, 2013].

- Deloitte. 2012 DTTL global financial services industry security study: breaking barriers; 2012. http://www.deloitte.com/assets/Dcom-Global/Local%20Assets/Documents/Financial%20Services/dtt_fsi_SecurityStudy2012.pdf [Retrieved May 24, 2013].
- European Union. How the EU works; 2013. http://europa.eu/about-eu/index_en.htm [Retrieved May 24, 2013].
- Ferguson JR. Implications of 9/11 for the financial services sector; 2002. <http://www.federalreserve.gov/boarddocs/speeches/2002/20020509/default.htm> [Retrieved May 24, 2013].
- Financial Industry Regulatory Authority, Inc.. Business continuity planning; 2013. <http://www.finra.org/Industry/Issues/BusinessContinuity/> [Retrieved May 24, 2013].
- Jickling M, Murphy EV. Who regulates whom? An overview of U.S. financial supervision; 2010. http://assets.opengrs.com/rpts/R40249_20101208.pdf [Retrieved May 24, 2013].
- Mamudi S. Wall Street plans for quick Sandy bounceback; 2012. <http://www.marketwatch.com/story/wall-street-plans-quick-sandy-bounceback-2012-10-29?pagenumber=1> [Retrieved May 24, 2013].
- Potter C, Waterfall G; 2012. http://www.pwc.co.uk/en_UK/uk/assets/pdf/olpapp/uk-information-security-breaches-survey-technical-report.pdf [Retrieved May 26, 2013], from Information Security Breaches Survey—Technical Report.
- Reuters T. Thomson Reuters Elektron: The Community; 2013. http://thomsonreuters.com/products_services/financial/financial_products/trading_data_infrastructure/elektron/the_community/ [Retrieved May 24, 2013].
- Rodier M. A decade after 9/11, business continuity is still a work-in-progress on wall street; 2011. <http://www.wallstreetandtech.com/technology-risk-management/a-decade-after-911-business-continuity-i/231601073> [Retrieved May 24, 2013].
- Simonite T. What happened when one man pinged the whole Internet; 2013. <http://www.technologyreview.com/news/514066/what-happened-when-one-man-pinged-the-whole-internet/> [Retrieved May 24, 2013].
- Wikipedia. List of financial regulatory authorities by country; 2013. http://en.wikipedia.org/wiki/List_of_financial_regulatoryAuthorities_by_country [Retrieved May 25, 2013].

Emergency Response and Recovery

8

IN THIS CHAPTER

- Emergency management overview
- Emergency response plans
- Crisis management
- Disaster recovery
- IT recovery
- Business continuity
- Summary
- Key concepts

INTRODUCTION

The most basic rule about planning for emergencies is this: keep it simple. The more complicated your emergency response plans are the less likely they will be effective in a real emergency. It's sometimes easy to overengineer a plan in the relative calm of everyday business activities. When an emergency strikes, people are not likely to remember a lot of rules, procedures, and details. So, when you create your emergency response and disaster recovery (DR) activities, you should strive to keep things really simple. Once the emergency has subsided, you can use more complex plans to begin restoring business operations.

We're not going into tremendous detail on emergency response, but we will provide a few pointers. If you want to create a detailed emergency response plan, you can work with local emergency responders who will be best able to provide details relevant to your community, its resources, and its geography. We also discuss computer incident response, disaster response, IT recovery, and business continuity.

In addition, we've provided several detailed checklists for emergency and disaster response and recovery in [Appendices B–E](#) at the end of this book, which you can use to develop your own detailed checklists. We chose to place them in the Appendix area so you have easy access to these lists in one location rather than having to leaf back through the book looking for these checklists. We refer to the lists in this chapter and refer you to these appendices to view related checklists.

EMERGENCY MANAGEMENT OVERVIEW

Regardless of how your company is organized, managed, and run, your emergency management process should follow a very simple rule: assign clear roles. If no one knows who's in charge or who has the authority to make decisions, nothing gets done. On the other hand, if everyone believes they have the authority to make decisions, chaos will reign. The aftermath of Hurricane Katrina is a testament to this problem—everyone assumed some other organization was in charge, no one knew to whom to turn for solutions. The Federal Emergency Management Agency was assumed to be in charge but was clearly late in gaining control of the situation. As a result, thousands of people were without food, water, ice, and shelter for an extended period of time. The lesson from this catastrophe that companies can learn is this: someone has to be clearly in charge and take immediate and effective action.

Throughout earlier chapters in this book, we've referred to the fact that emergency responders may not be able to get to your company for an extended period of time because they will prioritize your business lower than hospitals, schools, or nursing homes, to name a few. Therefore, your BC/DR plan should include some sort of internal emergency response capability in the event emergency responders are not available.

TIP

Using Your Community's Emergency Responders

Whenever possible, use your community's emergency responders to assist you in an emergency. Dial 911 or contact emergency services in your area as quickly as possible after a disaster or emergency occurs. At the same time, have your Emergency Response Team (ERT) respond to the incident. In many cases, first responders can help save lives by providing early care until trained professionals arrive. Administering CPR, for example, can help keep someone alive until paramedics arrive. Whenever possible, be sure to contact your emergency responders for assistance, as most company's employees lack the thorough training and experience to provide the same level of emergency support.

EMERGENCY RESPONSE PLANS

Emergency response may be outside of your immediate responsibilities as an IT professional, but it's important for you to understand how companies respond to emergencies so you can coordinate your BC/DR activities. It's important you understand team roles and responsibilities, as well as timing and sequence of emergency response activities so you can activate your IT BC/DR tasks in an appropriate and helpful manner.

Emergency response plans stem from the risks you've identified for your company. Remember, though, the emergency response is the *immediate* response to the incident. If fire breaks out, the emergency response is evacuating the building and calling the fire department while perhaps having trained employees use fire extinguishers to try to control the blaze. These are the basics of a fire emergency

response. However, there are other kinds of risks your company faces and these also require emergency response plans. Rather than creating a separate plan for every type of event that could occur, it's often advisable to create a basic emergency response checklist that can be used regardless of the emergency. The basics don't change—contact appropriate emergency personnel, get people out of harm's way, determine if there have been fatalities or injuries, determine if anyone is missing or unaccounted for, determine the source of the emergency, take measures to contain or halt the source of the problem if possible, and so on.

Develop an emergency response plan that meets the needs of your company. A simple response plan that covers a variety of similar emergencies will help ensure things run more smoothly if an emergency does occur. For example, there might be several different reasons you would choose to evacuate your building—a fire, internal flooding (burst pipes, etc.), or a bomb scare. The threat sources are different, but the action is the same. Therefore, look through your risks and identify which emergency actions would be needed. Then, group them together so you can develop just three or four emergency responses, if possible.

The basic set of emergency response tasks are these:

- Protect personnel
- Contain incident
- Implement command and control (ERT, Crisis Management Team (CMT) step in)
- Emergency response and triage (medical, evacuation, search, and rescue)
- Assess impact and effect
- Notification
- Next steps

The response procedures, in order of importance, are: (1) protection of people, (2) containment of the emergency, and (3) assessment of the situation. Regardless of the type of plan you create, these should be your priorities. Although it seems intuitive that you'd address the health and safety of people first, it's not always the first thing that comes to mind when an emergency strikes, so having a well-rehearsed set of procedures for emergency response that focuses on getting people to safety first, then addressing the emergency, will help form an appropriate response if something does occur.

Each plan should include:

- Roles and responsibilities
- Tools and equipment
- Resources
- Actions and procedures

Roles and responsibilities identify who's on the team and what they should do in an emergency. Tools and equipment for those emergency roles should be identified. This might include fire extinguishers, first-aid kits, hard hats, hazmat suits, walkie-talkies, shovels, and more. Any tools identified by the ERT should be purchased and stored in a suitable location. A list of these supplies should be maintained and

someone on the ERT should be responsible for periodic inventory as well as testing and replenishing of supplies. For example, first-aid kits have various medicines such as antibiotic creams and aspirin that expire and should be replaced periodically. Other resources the ERT might need should be acquired or identified. If specialized equipment such as a fire truck with an extension ladder would be needed to reach top stories of the building, that should be noted. The local fire department should be contacted to determine whether they have appropriate resources (such as a truck with an extension ladder). If equipment is not available, alternate plans should be created that address the specific needs. The company should also develop numerous evacuation scenarios and procedures that address the possibility of a fire in the upper floors of the building. Finally, actions and procedures should be developed, which the ERT will initiate in the event of an emergency. Of course, these tasks normally are not the responsibility of the IT department, but you may work in a small company where it would be helpful to head or assist with this type of planning.

We've provided a detailed emergency response checklist in [Appendix C](#), so you can easily refer to it later. If you take a moment now to mark this page, flip to the back of the book, review the list and then come back, you'll see that there is extensive detail in the list. It provides a generic step-by-step process that you can tailor to your company's specific situation so that you have a solid emergency response plan in place. The plan must be executed by people, so let's take a moment to discuss the role of the ERT.

REAL WORLD

Powering Up After Hurricane Katrina

Hurricane Katrina has become an icon for many people. The enormity of the storm and its impact took most disaster planners off guard and few organizations responded effectively in the aftermath of the storm. For many, the most immediate need was for electrical power. Imagine trying to restore power in an area where power poles were torn down, transmission lines were shredded, employees' homes were destroyed, roads were blocked, and communications were nonexistent. That's the situation faced by Mississippi Power's CIO Aline Ward. For a fascinating recount of what Aline Ward did to restore power to the area, visit this link: <http://mediatechtarget.com/digitalguide/images/Misc/AwardMississippi.pdf> (Ward, 2006). It's a real world view of the aftermath of a natural disaster of massive proportions and how one person managed to bring order from the chaos to get power back to the area in record time.

EMERGENCY RESPONSE TEAMS

Your company should have an ERT with defined roles and responsibilities for team members. Each person should clearly know the bounds of their authority and to whom they should turn for help or for escalation of issues. Previously, we've referred to a CMT, which may or may not be the same as an ERT. If you're in a small company, it may be the same set of people, but in many cases these are not the same people because the skills required are different. [Figure 8.1](#) shows the hierarchy and high-level responsibilities of the ERT, CMT, and DR team(s).

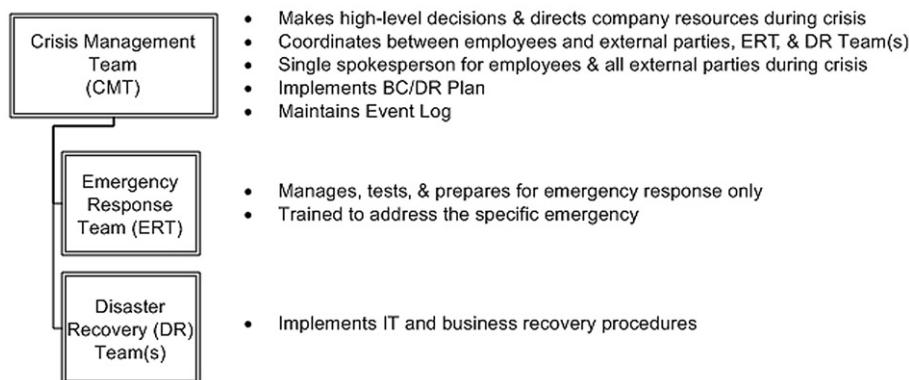


FIGURE 8.1

Emergency response team hierarchy.

The ERT leader is responsible for activating and coordinating the emergency response and for notifying civil authorities such as the police or fire department, contacting hospitals or paramedics, and so on. The ERT leader should also be a member of the CMT and should coordinate closely with the CMT to ensure that the appropriate level of BC/DR activation occurs in a timely manner. Emergency response and DR activities can occur in parallel. Typically, only trained members of the ERT can address the actual emergency, which may include medical staff, evacuation or shelter-in-place leaders, search and rescue staff, and the CMT manager and/or a corporate executive contact. Members of the CMT can begin assessing damage, evaluating options, and implementing the BC/DR plan as soon as possible.

The ERT is also responsible for ensuring that the proper communication equipment is available prior to an event, for activating and distributing that communication equipment in an event, and for communicating appropriately throughout the event.

ERT members should receive training on the aspects of the job they'll be expected to perform in an emergency. If team members are expected to fight small fires by using fire extinguishers, they should be trained not only on the use of the fire extinguishers but also on how to fight fires. This includes safety procedures for firefighting as well as methods for fighting different types of fires. Training is critical to ensure team members' safety and effectiveness in an emergency.

Emergency response training may include:

- Relocation and evacuation safety and techniques
- Firefighting equipment, safety, and techniques
- Search and rescue safety and techniques
- Hazardous material handling
- Chemical spills or leaks (liquid, airborne, etc.)
- CPR, first aid, and emergency medical skills

- Water safety, water rescue
- Cold weather survival
- Emergency shutoff/shutdown procedures
- Damage assessment and control

Obviously, the type of training required depends largely on your company, the nature of its business and its geographical location. Identify the types of emergency response training that would be helpful for your company's staff to have and develop training plans to ensure training occurs periodically. Skills should be tested, rehearsed, and refreshed from time to time. Also, develop some method for responding to the loss of ERT members through retirement, attrition, or transfer. Finally, be sure several people on the ERT have similar skills and training so your team does not have a single point of failure. If only one person knows how to shut off the main electrical breaker and he or she is injured in an explosion, you have a problem (well, several major problems, actually).

It's also helpful to assign ERT members roles and responsibilities outside of emergency situations related to continued preparedness. For example, the ERT might be responsible for staging emergency training sessions or simulations on an annual basis that the entire company participates in. It might also be tasked with periodically checking fire extinguishers (e.g., are they where they should be, are they well-marked, are they functional, have they been tested, have they expired?), or checking emergency lighting from time to time. This keeps the team intact and functional during nonemergencies, which can help them work together as an effective team during an emergency. It also helps maintain safety measures for the company, which is another risk mitigation strategy. If no one is responsible for checking fire extinguishers, there's a good chance you'll run into a problem if a fire actually does flare up. Define roles and responsibilities for ERT members that help reduce your company's risks and liabilities.

CRISIS MANAGEMENT TEAM

There are hundreds, if not thousands, of books on crisis management available and if this is an area of interest, you should do additional research to delve into the details of this topic. As you know from watching the news or reading blogs, there are all kinds of crises that companies have to manage, not all of them related to BC/DR. In this section, we cover the basics of crisis management with an eye specifically toward BC/DR activities.

When you declare an emergency, disaster, or crisis event that must be managed, you begin implementing your BC/DR plan. The CMT is the team responsible for making the high-level decisions; for coordinating efforts of internal and external staff, vendors, and contractors; and for determining the most appropriate responses to situations as they occur. They should be well versed with the BC/DR plan and the various team leaders for BC/DR activities either should be part of the CMT or should report to them.

Emergency response and disaster recovery

The CMT oversees the ERT and the DR team(s). Once an emergency occurs, the ERT leader should take charge of managing the emergency itself, and the leader of the CMT should begin coordinating efforts between ERT, civil emergency responders (if appropriate), and other initial activities related to the BC/DR plan. The ERT leader should be a member of the CMT and should report to the team periodically throughout the emergency response. The ERT should be quickly released back to emergency duties while someone from the CMT documents the information provided by the ERT. This is part of the event log that should be initiated and maintained throughout the event. In addition to coordinating the emergency response, the CMT also coordinates activities related to initiating the DR efforts. Once the ERT leader has notified the CMT that the actual emergency has ceased and that DR can begin, the CMT takes over coordinating all activities. Typically, once the DR efforts conclude and business continuity efforts begin, the CMT winds down and operations may resume through normal management channels. This is a decision each company must make based on its unique structure, but in general, the CMT leader should manage the situation until it makes sense to hand over control to the operations team.

It is important to note you should clearly define the point at which the CMT stands down and normal operations take over. If you fail to clearly identify this line of demarcation, you risk having turf wars, power struggles, and people working at cross-purposes. Create a clear set of criteria for when the CMT hands over operations so that there is no question in anyone's mind about how the transition should occur. Often a simple checklist that both the CMT and operations teams reviews together can be helpful in deciding when to resume normal operations. This is usually not a major issue in companies where the members of the CMT are members of the senior management team. In some companies, however, there may be confusion over roles, responsibilities, and authority, so be sure to clearly delineate these in advance.

Alternate facilities review and management

The CMT is responsible for overseeing the activities related to DR and business continuity at alternate sites. They should review the activities leading up to activating the alternate site and should be the ones with final authority over decisions that need to be made related to the alternate site, such as bringing in additional services, equipment, or vendors if original arrangements do not meet current needs. They are responsible for resolving problems and issues that arise and should be the final decision makers for escalated issues.

Crisis communications

Crisis communications cover a lot of territory and may involve numerous teams working in a coordinated fashion, but the messages being communicated from the ERT and DR team(s) should originate from or be approved by the CMT. In an

emergency situation, you should avoid having multiple sources of communications going out since it can cause confusion, error, frustration, and worse. Though you don't want to create a bottleneck in your communication stream, in the early stages after a business disruption or emergency, it is in the company's best interest for the ERT and DR team(s) to communicate directly with the CMT and allow the CMT to act as the single spokesperson for all communication about the crisis to executives, other company departments, and outside entities. This will ensure that the message is correct, consistent and adheres to other established Crisis Communication Plan guidelines. In addition, this establishes a two-way communication channel between the CMT and the teams working on DR activities and helps in the coordination of activities and teams. This is critical for disasters or disruptions that also disrupt communication lines.

One of the most severe long-term impacts of any disaster is the loss of confidence by employees and their families, investors, customers, suppliers, regulators, and the community at large. In many cases, poor handling of crisis communication leads to exacerbation of the damage caused the disaster, further decline in sales, increased regulatory fines, increased likelihood of lawsuits, and decreased customer and shareholder confidence. With the 24-hour news cycle and the use of the Internet as a news source, companies cannot afford to simply allow information to "manage itself." Saying nothing also allows others to fill in the blanks. Rumors, innuendos and outright lies about the company, the situation, the cause, the impact, and all other details need to be managed and controlled by the company, not the public at large. Therefore, it is critical to not only develop a Crisis Communication Plan with clear guidelines for the CMT spokesperson, but also to practice it regularly, just like a fire drill.

The Crisis Communication Plan should adhere to three simple rules for effective crisis communication, which, if followed, should mitigate, to the greatest extent possible, any further damage caused by the disaster.

1. Always tell the truth.
2. Appoint a spokesperson to be the face and voice of the company with the media.
3. Provide information that addresses who, when, what, where, why, and how.

First, there are numerous case studies demonstrating the power of the truth. When companies own up to mistakes they've made and take action to prevent these mistakes from being repeated, they invariably come out on top. It can be a painful journey, but the organization is stronger as a result. The alternative leads to additional risk for the company. Almost always, the truth will eventually come out, and lying about mistakes made or actions taken or not taken will only increase the likelihood of litigation and financial harm. It is important to note that telling the truth doesn't mean spilling your guts or divulging every last detail. However, it does mean stating only the known facts (no speculation) and keeping communication short, simple, and to the point as per rule #3 discussed earlier.

Second, a person well trained in public and media relations should be appointed as the single spokesperson for communicating outside the company. Whereas you may have multiple communication teams working internally to address various

needs such as employee communications or DR tasks, the official corporate spokesperson will deliver a consistent, professional, and appropriate message to all external communication channels. ERT and DR teams should always refer requests for information coming from outside the CMT, ERT, and DR teams to the official CMT spokesperson, even if these requests are coming from other company departments.

Third, the CMT spokesperson, trained in public and media relations, should know how to craft messages which address the needs of reporters and adhere to journalistic best practices. Namely, the spokesperson should address who was involved, when did it happen, what happened, where did it happen, why did it happen, and how did it happen? By addressing these areas, the spokesperson can spot potential pitfalls and find ways to carefully craft answers that help quell fear and chaos without being caught off guard, speculating, rambling on, or overly injecting emotion. Your Crisis Communication Plan should include language that can be used to help neutralize the crisis by providing factual data without editorials, emotions, and other extraneous data. Also, before releasing specific data, the spokesperson should ensure that it is legal, ethical, and appropriate, based on where the company is with respect to its response and recovery checklists. The spokesperson should not release information about the potential cause (e.g., how, why) of the event until it's been cleared with executives, investor relations, finance, and legal counsel. Providing templates with guidelines for crisis communication, along with training and practice, can help ensure crisis communications meet everyone's needs without escalating the problem or incurring further damage for the company.

Human resources

Representatives from human resources should be included on the CMT so that they can specifically address the needs of employees and maintain a communication channel with employees through preplanned methods. They should track employees who may be injured from the event or not available for work due to leave of absence, vacations, and so on. They should provide support for injured employees and their families, including facilitating access to emergency or ongoing medical or psychological services. They can also assist employees with financial, legal, and insurance issues related to the injury or death of an employee or family member. They should prepare and update an employee head count to determine who is available for recovery operations and who may be available later for business continuity activities. If temporary staff or contractors are needed, they can help select, manage, oversee, and monitor temporary staff as well as manage timecards and other payments for such staff. Last, they can determine the status of payroll and ensure employees get paid in a timely manner. This is one of the biggest concerns employees will have in the aftermath of disaster, and having someone actively manage and monitor this process can alleviate some of the stress of the situation. Pro-actively addressing these concerns will also reduce the number of calls, e-mails, and contacts related to questions about payroll, freeing up time to address other HR-related concerns.

Legal

Depending on the nature of the disaster or disruption, you may need to have the CMT contact legal counsel. The firm's lawyers or legal representatives may need to review or approve emergency contracts; review language in agreements with vendors, suppliers, or contractors; review documents related to injury, death, or property damage; or address regulatory and compliance issues. As soon as the CMT is activated, it should be someone's specific responsibility to contact legal counsel and notify them of the event so they can provide appropriate information, feedback, and guidance throughout the remainder of the event and during its aftermath.

Insurance

As we've discussed, insurance is a risk transference method and one used by many, if not all, businesses today. In some cases, your firm may be required to hold certain types of insurance; in other cases, it may be voluntary. Your BC/DR plan should have contact information for your insurance company representatives, and they should be notified upon activation of the CMT. The CMT may also perform an initial damage assessment and document it for the insurance company. This might include taking photographs or video images as well as making detailed notes. Members of the CMT team should also begin gathering documents related to insurance claims and submit loss estimates to the insurance company. Finally, someone on the CMT should review the insurance documents to determine exclusions, limitations (financial, time, location, cause, etc.), or maximums on various policies. Any issues with insurance should be escalated to management and/or legal counsel for review and resolution.

Finance

The CMT should also have representatives from the financial department available to assess the status of the company. This might include assessing the cash availability of the company, the viability (or advisability) of processing employee payroll early, or to provide advances to employees. Financial representatives also need to assess the status of the accounts payable and receivable to ensure bills and invoices are issued in a relatively timely manner and that revenue and payments are received in a timely manner as well. A process for managing, tracking, and monitoring expenditures during the disaster or disruption should be implemented and managed by the financial representative(s) on the CMT. Estimates for repairs and other expenditures should be submitted to this team for review and approval. Upon resumption of business operations, the financial team should assess the status of the company's finances and report to executives or senior management.

DISASTER RECOVERY

We discussed the different phases of business continuity and DR in [Chapter 7](#), including activation, DR, business continuity recovery, and maintenance/review. In this section, we're going to discuss the DR activities in a bit more detail. This

detail belongs in your BC/DR plan, but breaking it out into sections in this manner will help you process and manage the massive amount of detail required to address these activities properly. Once you've developed your emergency response, DR, and business continuity responses, you can (and should) include that information in your BC/DR plan. We've included various checklists, in [Appendices A–G](#) at the end of this book that you can use as the basis for creating your own checklists or project plans. These can be included in the body of your BC/DR plan or as appendices at the end of your document for ease of use.

Activation and emergency response checklists

You may find it helpful to develop a variety of checklists, which can be extremely useful in making quick decisions for moving forward. Since you and your team may not have time to rehearse these plans frequently, checklists can help remind you of critical steps to take, regardless of the situation. Activation checklists delineate all the activities and triggers that should take place prior to and during plan activation. This begins with some sort of disruptive event occurring, someone notifying the BC/DR team, and someone determining that the BC/DR plan should be activated as a result of the disruptive event. Remember, there may be some minor events that do not trigger the activation of the BC/DR plan, so deciding what criteria will be used to activate the plan in whole or in part should be part of the process. Emergency response checklists can be referenced in the immediate aftermath of a disaster affecting (or likely to affect) human safety. These checklists include prescribed actions which help contain the effects of different environmental disasters, limit the effect of the disaster on human safety, and notify appropriate emergency response personnel. The checklists included in Appendices A through G of this book provide a framework for you to develop your own activation and emergency response processes.

Recovery checklists

The recovery phase also has specific tasks that should be undertaken. The specific steps to be taken should be defined in your BC/DR plan. If you've looked at the various risks and potential impacts of these risks, you should have numerous scenarios that require planning. By developing plans for various scenarios, you will have the steps you need in almost any type of disaster because even though the details of the disaster may vary, the steps you need to take will be the same in a major disaster or a minor disaster. As with the activation phase, there is a long list of items you can use for this stage of work. Remember, the lists in the Appendix materials are intended solely to get you thinking about how you will manage your company's BC/DR efforts, you will need to modify them accordingly.

It is important to note that these initial recovery checklists typically precede any actual IT recovery tasks. Therefore, you should pay special attention to any information you may need to complete these tasks successfully since access to this information may not be available until after IT recovery has commenced. Remember, IT recovery can't commence until physical, safety personnel, travel, financial, and other concerns

are addressed first. If such information isn't explicitly contained within your written BC/DR plan, then you should incorporate it (e.g., add it as an appendix) or figure out an alternate way to easily retrieve it along with your BC/DR plan itself. For example, if information critical to early recovery efforts is stored electronically on internal network drives and is referenced externally within your written BC/DR plan, you may not be able to access this information early on in the recovery process in order to make necessary decisions prior to IT recovery tasks beginning. Such pre-IT recovery BC/DR plan information may include employee and vendor contact lists, system and network designs, equipment lists, location of data backups, alternate site access information, facility restoration procedures, physical security response procedures, credit card/payment information, passwords, access codes, physical location of keys, maps, or other records. Since such BC/DR plan information may change frequently or not be readily available due to damaged IT infrastructure or systems, it is best to review your pre-IT recovery checklists to determine how updated copies of critical information will be periodically copied securely off site and easily accessed in the event activation of the BC/DR plan is required. For example, you may choose to keep all such information printed out periodically and kept in secure physical storage at several different employees' homes. Or, you may choose to copy all such information in an encrypted fashion on removable media in several different locations each night. Or, you may choose to copy such information in a securely transmitted, locally encrypted fashion to the cloud nightly for easy access via any Internet connection. Better yet, employ a couple of different methods to further minimize risk in the event either physical or electronic access is unavailable. Whichever method or methods you choose, ensure CMT, ERT, and DR teams know where they can access such information at all times and do not rely on particular individuals being alive or otherwise accessible to answer such questions in the early stages of a disaster.

IT recovery tasks

The tasks needed to recover IT systems are probably quite familiar to you, but they should be delineated within your BC/DR plan. Each subteam should have a clear set of guidelines and procedures for how and when they will perform their work. Be sure to note dependencies within the checklist so that teams don't work at cross-purposes. You can add items to the checklist as checkpoints for these purposes, much like milestones are used in project plans. Sample IT recovery checklists are included in the Appendix of this book, including checklists for infrastructure, applications, office area and end-user equipment, business process, and manufacturing, production, and operations recovery steps.

Since restoration of network and systems infrastructure must be complete before any of the other IT recovery checklists can be completed, it is important to carefully review information needed to complete each step of the infrastructure checklist(s) to ensure you have access to this information, similar to our discussion of pre-IT recovery checklists above. For example, if you first need to stand up network routing and switching in order to connect backup systems and perform restoration of individual

servers, or to get voice communication back online, but you don't have access to IP address lists, or switch build or security configurations, because they are not readily accessible, you may need to spend extra time physically traveling to a remote location or have to instruct remote IT support blindly over the phone, or worse, start from scratch. If such information is stored electronically on systems which are damaged, or are otherwise inaccessible, or cannot be connected to directly (such as remotely isolated backup systems), you will waste precious time trying to recover this information instead of performing essential recovery tasks for the business. This lack of planning will further delay infrastructure recovery time and potentially cause additional downstream delays for application or business process recovery teams that have to reconfigure restored systems and/or applications before they can be brought online. In such situations, it is common for recovery staff to get easily frustrated and tire quickly, further impacting the team's ability to execute effectively. These "bottlenecks" which are all too common during IT recovery operations can be alleviated simply by planning ahead. You should make provisions before a disaster, as part of your regular backup operations, to identify, export, and securely copy and store such information periodically off site, where it is easily accessible in the event of a disaster, along with your BC/DR plan. It should be noted that regular testing of your BC/DR plan and associated recovery procedures as described in [Chapter 9](#), either as a result of a disaster and/or through preplanned tests, will readily identify potential problems with accessing required information early on in IT recovery operations. So, if you are having trouble identifying all information required up front, the best solution is to test your plan.

After recovery of network infrastructure, end-user connectivity and other dependent network services are complete, it is often confusing to know in what order to restore applications. Given the likelihood that your company will have limited IT resources for recovery operations, it may be impossible to bring all critical systems back online simultaneously within the allowable recovery time objective (RTO). Without a centrally managed IT recovery operation, individual departments will all expect their applications to have priority and be restored first. In the application recovery sample checklist in the Appendix, it states that mission-critical data should be reviewed to determine which applications should be restored first. But, who determines what the mission-critical data are and what the restore order should be? Hopefully, your BC/DR plan already contains this guidance in the form of a company-wide service level matrix or other similar priority list. A service level matrix typically classifies sets of applications/services by tiers (e.g., Tier 1, Tier 2, Tier 3, and so on) based on requirements such as RTO/MTD, normal operational hours (24/7 vs. 8 × 5), regulatory, safety, financial, or operational constraints, and/or any workarounds or manual business continuity processes which may be available to business staff before IT restoration. You typically want to focus on recovery of Tier 1 applications first. However, it is important to remember that the CMT has ultimate responsibility for identifying and prioritizing application restore order based on changing circumstances on the ground. Therefore, it is important that the CMT and DR teams communicate regularly during recovery operations in order to provide

up-to-date information on restoration activities and in order to change direction at a moment's notice based on CMT guidance. For example, the CMT may be notified that a building control system is nonfunctional and impairing emergency response efforts; the CMT can then instruct the appropriate DR team to make this their first priority. In addition, all client requests which come in during recovery operations should be funneled through the CMT so that they can be properly assessed and managed per BC/DR plan guidance. This also allows for the central CMT event log to properly record all requests, activities and decisions as they are occurring, so that the BC/DR plan can be improved after normal operations resume.

Once you know what application to recover next, individual written application recovery procedures should be referenced in order to restore full application functionality as quickly and accurately as possible. Such procedures should already specify all application details and IT-related dependencies prior to restoring the application and its data, such as: (1) application vendor contact information, including support phone numbers, phone numbers for account execs and inside sales engineers, customer IDs, support contract numbers, and vendor support Web site logon information; (2) application version and version of any supporting database(s); (3) network location(s); (4) number of client workstations by location; (5) server(s); (6) database(s) by location; (7) virtual PC(s), thin clients and/or terminal servers; (8) network services, such as Internet access, e-mail, mobile synchronization, network drives/directories/files, FTP, Fax, remote network access, network printing (by location), etc.; (9) external real-time interfaces to other systems; (10) dependent data inputs from other systems; and (11) dependent mobile devices by location, including any static host names or IP addresses.

The last part of the application recovery document should be step-by-step procedures to fully restore and test the application and any associated databases, data sets or real-time interfaces. In addition, these step-by-step procedures should be written so that any IT support staff could understand them and successfully restore the application, even if they've never supported it. Moreover, screen shots should be used to simplify and expedite restoration activities. Finally, it is helpful to describe any temporary business continuity procedures that would be used by the business while the application is unavailable during recovery operations, such as tracking transactions on paper, sending personnel out into the field, handling phone calls, etc. This way, the personnel responsible for IT recovery better understand the temporary impact to the business during DR operations.

On a final note, you will notice two tasks are repeated throughout the recovery checklists in the Appendix: (1) the documentation of observations and results in an event log and (2) communication with appropriate parties. For each IT DR team, it is critical that a single person be appointed as the scribe or recorder during recovery operations. This person should also have the role of communicating with the CMT or other leadership, reporting progress and receiving updated direction on next steps for the team. This way, the recovery team can focus on getting things back up and running as quickly as possible, in order of company-wide importance, without any distractions.

Computer incident response

In addition to recovery from disasters that cause damage to physical structures or loss of IT equipment, IT recovery also involves responding to, stopping, and repairing problems caused by system failures, security breaches, or intentional data corruption or destruction. Depending on the nature or severity of the attack or incident, you may need to activate a computer incident response team (CIRT). Let's take a moment to discuss computer incident response and the team that performs these tasks.

REAL WORLD

Training Is Not Optional

When disaster strikes, most people resort to what they know best; they fall back on their training. The same is true of IT professionals. In the face of a major system outage or security breach, IT staff will do what they've been trained to do. Training is not an option for emergency preparedness, it is a *requirement*. Emergencies by their very nature are incredibly stressful and chaotic. People, by their very nature, feel most comfortable in any situation when they know what to expect and what to do. In an emergency, they won't necessarily know what to expect, but they will know what to do if they've been trained. Training is also important for CIRT teams because security incidents can be devastating to a company. CIRT members should know what to look for and exactly what actions to take in order to address a potential security breach or other serious incident. It doesn't help to shut down a server if a hacker gained root access to the firewall; it doesn't help to shut down the e-mail server if a worm has infected PCs through removable media and can copy itself to open Windows shares. In addition to general IT skills, CIRT members should represent the various areas of expertise required in your IT department including servers, infrastructure, security, database administration, and applications, to name a few. CIRT members also should have checklists or step-by-step instructions to follow for standard incident types such as distributed denial of service, firewall breach, virus outbreak, and so on. This helps reduce stress and ensures everyone follows standard procedures to halt the immediate impact of any computer-related incident.

Most IT departments have some process in place for addressing and managing a computer incident. An incident is defined as any activity outside normal operations, whether intentional or not; whether man-made or not. For example, the theft in the middle of the night of a corporate server is an incident. A Web site hack or a network security breach is also an incident. A database corruption issue or a failed hard drive is also an incident, but for the purposes of this discussion, we're going to stick with the emergency kinds of incidents and leave the more routine incident handling to your existing IT operations procedures. For example, we'll assume you can handle a bad hard drive or a failed router through standard operating procedures and we won't cover that here. What we will cover are the incidents that require a swift and decisive action to stop a security incident from spreading or causing further damage. This includes events such as a network security breach or a denial of service attack and events such as a fire in the server room or a flood in the building.

The first step in this process is to form a CIRT. You may already have a team in place that addresses computer incidents such as security breaches. If that's the case you have the foundation of a CIRT that can be used in the event of a more widespread

disruption such as a fire, earthquake, or flood. The members of the team, like the ERT, should have defined roles and responsibilities. As with the ERT, CIRT members should also be trained in their roles. For example, if you have staff responsible for monitoring network security and they notice a potential breach through a particular port, they should also know how to shut down that port and have the network permissions that enable them to do so. If all they know how to do is monitor the log file or traffic, for example, and have no idea how to shut down a port or stop the problem, it could be hours before the problem is addressed. Therefore, members of your CIRT should have training and appropriate network permissions to address these problems.

CIRT responsibilities

In order for the CIRT to be effective, its duties must be well defined. There are five major areas of responsibility for the CIRT team. These are:

- Monitor
- Alert and mobilize
- Assess and stabilize
- Resolve
- Review

Monitor. Every network must be monitored for a variety of events. Some of these are failure events that indicate a problem has occurred such as a hardware failure or the failure of a particular software service to start or stop appropriately. Other events are tracked in log files for later review or auditing. These might include failed login attempts or notification of a change to security settings, for example. Other incidents may include unusual increases in certain types of network traffic or excessive attempts to login to secure areas of the network. Whether the event stems from intentional or unintentional acts, the network needs to be monitored. The CIRT should be involved with helping to determine what should be monitored as well as assisting in monitoring the network. Not all events have significance and sometimes it's only through seeing recurring events that a pattern can be discerned. Therefore, having experienced team members monitor the network will help reduce the lag time between an unwanted event and a response.

While a serious security breach might not cause you to activate all or part of your BC/DR plan, suppose you had some very strange activity on four of your corporate servers and the CIRT member couldn't determine the source of the anomalies, or there was an unexpected loss of data or widespread outage of IT services. Is this a disaster or not? If it's caused by fire in the server room, yes. If it's caused by an errant software update that was just applied, maybe not. The point is that your CIRT team should monitor the network activity and take appropriate action, regardless of the source of the problem. In some cases, this will involve activation of the BC/DR plan, and in other cases it won't.

Alert and mobilize. Once an unusual, unwanted, or suspicious event has occurred, the CIRT member should alert appropriate team members and mobilize for action. This may involve shutting down servers, firewalls, e-mail, or other services,

removing offending hosts from the network, or turning off network ports once the offending host is identified. Alerting and mobilizing should have the effect of stopping or containing the immediate impact of the event while still being able to preserve, secure, and document any evidence or artifacts (such as the existence of malware files or event and audit logs) that will later help identify the vulnerability that was exploited.

Assess and stabilize. After the immediate threat has been halted, the CIRT team assesses the situation and attempts to stabilize it. For example, if data have been stolen or databases have been corrupted, the nature and extent of the event must be assessed and steps must be taken to stabilize the situation. In many cases, this phase takes the longest because determining exactly what happened can be challenging. If you have members of your team that have been trained in computer forensics, they would head up this segment of work. If you do not have members of your team trained in this area, you should decide whether it would be advisable to provide this training to staff or hire an outside computer forensics expert. Outside consultants can be helpful in this case for the simple fact that they work in this arena day in and day out and are most likely more up to date and experienced in this area than staff that occasionally goes to training and rarely (if ever) puts that training to use. The decision is yours based on the skills, expertise, and budget of your company. Having in-house expertise can be a good first step and you can always hire an outside expert on an as-needed basis.

Keep in mind that you have defined maximum tolerable downtime (MTD) and other recovery metrics. A review of these should be included as part of the assessment and stabilization procedures so that plans and actions can accommodate these requirements.

Resolve. After determining the nature and extent of the incident, the CIRT can determine the best resolution and implement it. Resolution may involve bringing an offending host up on an isolated network, taking disk-based snapshots of the offending system to preserve any digital evidence, eradicating the malware or virus, identifying and mitigating all vulnerabilities that were exploited, resetting passwords or removing rogue accounts, restoring from backups, updating operating systems or applications, modifying permissions, or changing settings on servers, firewalls, or routers. In addition, additional monitoring should be implemented to look for future related activity.

Review. Once the event has been resolved, the CIRT should convene a meeting to determine how the incident occurred, what lessons were learned, and what could be done to avoid such a problem in the future. Within the scope of a BC/DR plan, this might involve understanding how the recovery process worked, understanding how to improve risk mitigation for similar threats in the future, and what could be done differently in the future to decrease downtime, decrease impact, and improve time to resolution. Other topics that should be discussed include any improvements to evidence gathering and handling, required incident reporting (internal and external), and any improvements which could have helped detect the vulnerability sooner.

REAL WORLD**Computer Emergency Response Team**

There are numerous terms and acronyms floating around regarding computer emergencies, computer incidents, and computer security. The grandfather of them all, however, is the concept of computer emergency response developed by the Software Engineering Institute at Carnegie Mellon University. We mentioned this resource earlier in the book and thought this would be a good time to mention it again. The Web site has a vast array of information and resources you can access. When developing your BC/DR plan for the IT portion of your business, read up on the latest trends and knowledge on the Web site at www.cert.org ([Carnegie Mellon University's Software Engineering Institute, 2013](#)). Head to this URL for details on creating a CERT team: http://www.cert.org/csirts/action_list.html ([Carnegie Mellon University's Software Engineering Institute, 2006](#)). It's a great resource for IT professionals even outside the scope of BC/DR planning as well.

Computer incident response is an activity that spans DR, business continuity, and normal operations. It is likely the CIRT team will have day-to-day responsibilities as part of standard IT operations or that CIRT activities will be folded into IT standard operating procedures. However, if an earthquake hits the area or a flood shuts down operations, the CIRT's expertise can be put into play immediately as part of the BC/DR response. Be sure to integrate CIRT responsibilities into your BC/DR plans.

The skills of CIRT members should be kept up to date, so they are aware of and can respond to the latest threats, vulnerabilities, and issues on the IT realm. Although training is important for IT staff in general, CIRT members need to be aware of the constantly evolving threats and vulnerabilities. They need to have the tools and skills necessary to recognize and resolve problems in a timely and effective manner. This is accomplished in part through training. CIRT members must also take responsibility for staying up to date on the latest trends by reading technical journals, newsletters, Web sites, blogs, and other related materials.

TIP**National Institutes of Standards and Technology Computer Security Incident Handling Guide**

The National Institutes of Standards and Technology published this guide to help both established and newly formed incident response teams. Head on over to <http://www.nist.gov/index.html> ([National Institute of Standards and Technology, 2013](#)) and search for this guide on the home page. You will find helpful information such as incident response lifecycle best practices, tools and resources for incident handlers, an incident handling checklist, and incident handling scenarios with questions you can use to train your CIRT team.

BUSINESS CONTINUITY

Business continuity begins when DR ends. As we've discussed, it's not a sharp cutover from one phase to the next. Though we've discussed this to some extent throughout the preceding chapters, we haven't really looked at what it takes to move

from the DR phase to the business continuity phase specifically. As with the other topics in this chapter, we've included several business continuity checklists in the Appendix for your reference. We'll review the basics in this section.

The DR efforts include stopping the effect of the disaster and getting basic operations set up. For example, if your building was destroyed, DR would include salvaging anything from the building you could, activating an alternate work site, activating an alternate computing site (may be the same or different than the alternate work site), and setting up and restoring network components, servers, and systems. Now that DR, from an IT perspective, is complete, business continuity kicks in. These steps include managing business processes in work-around mode, if needed, and assessing the status of operations and beginning to normalize operations. For example, it's possible that some systems can be restored almost immediately, whereas other systems may take several days or a week to restore. The workarounds in place may allow some operations to resume but others to remain dormant. Backlogs in some areas are created, data gets out of sync, and the state of the business is perhaps more chaotic now than it was during the disaster when it was clear that no business operations would take place. Therefore, having a plan for business continuity steps is critical to your eventual success.

Part of the challenge of the business continuity phase is determining what should be restored, what should be salvaged, and what should be replaced. There is certainly a time consideration that needs to be factored in along with the obvious financial considerations. Repairing and replacing have their own sets of challenges and the options should be reviewed prior to making decisions to move forward. In order to process all the information needed, the various teams should work together to identify optimal solutions. Some of the factors to be considered include:

- Executive/administrative
- Business operations
- IT operations—infrastructure
- IT operations—end users
- Communications
- Facilities, security, and safety

Since every business is different, the business continuity checklists we've included in the Appendix are fairly generic. They list major activities you should consider including. Not all activities on the list will be appropriate for your organization. There may be areas *missing* from the checklist that you'll need to resume operations at your firm. However, if you start with these lists, there's a better chance you'll include what you need to successfully resume business at your company.

As you'll see in the checklists, the last two activities are reviewing what happened during the disruption or disaster and adding that knowledge to your BC/DR plan. Once your firm gets back to business as usual, no one will have the time to capture these data. It's vital that you capture lessons learned from the incident and build them into your BC/DR plan so that the mistakes made aren't repeated and the innovations or positive

lessons learned can be incorporated. This is part of plan maintenance discussed in detail in [Chapter 10](#), but it also should be part of your BC/DR activities as well.

SUMMARY

In this chapter, you learned about emergency plans and emergency responses that should be included in your BC/DR plan. Emergency response is the initial response to a disaster or disruption. The first response should be to get people out of harm's way and to determine if there are fatalities or injuries. Secondary efforts should be to stop the source of the problem whether that's through calling civil emergency responders (fire, bomb squad, police) or through attempting to address the problem with an ERT (fighting a fire, turning off gas or electric sources, containing hazardous spills, etc.). Emergency responders should be trained in appropriate skills such as safe building evacuation methods, CPR and first aid, firefighting, hazardous material containment, and others. Emergency plans should be well conceived and well rehearsed because people will fall back on their training in an emergency.

The CMT may activate the emergency response or the emergency responders may notify the CMT of an event. In any case, the CMT coordinates emergency efforts and activates the BC/DR plan based on the specifics of the situation. The CMT is also responsible for coordinating recovery efforts and should manage these activities through the business continuity stage. Roles and responsibilities should be well defined to avoid confusion or working at cross-purposes. Activities the CMT typically manages can include the emergency and disaster response, activating alternate work sites and facilities, managing corporate communications, interfacing with insurance and legal representatives, and working with the finance department. You can define other appropriate activities for your CMT to reflect the specifics of your business.

Because disasters are by their very nature chaotic events, it helps to have checklists you and your team can use to manage activities in the aftermath of a major disaster or disruption. We've included several checklists in the Appendix of this book, so you can easily refer to them and use them in your planning activities. DR tasks fall into two major categories: activation and recovery. Activation includes all activities related to assessing a situation and determining what recovery plans should be implemented as well as taking initial steps toward that end.

Within DR, there are specific IT recovery tasks that should be performed as well. Separate IT recovery checklists should be created so that you have a clear plan about how to recover from various events. These checklists should include information regarding the MTD and other recovery metrics that have been established. The lists also should include timelines, milestones, and dependencies that need to be addressed. Some companies form CIRTs or computer emergency response teams (CERTs) to respond quickly and effectively to computer-based incidents. The activities of the CIRT occur in the day-to-day operations of the company (outside the BC/

DR domain) and are also part of BC/DR activities. Defining how the CIRT should operate and interact with your BC/DR plan is vital to ensure an effective response.

Business continuity activities begin after recovery efforts have concluded, though there is usually some overlap. Business continuity activities include the limited resumption of business operations, typically in manual or work-around mode. These activities pose a unique set of challenges from an IT and operations perspective because data must be managed differently until IT systems are fully back online and normal operations can resume. The business continuity checklist should include steps needed to resume limited operations, it should identify requirements and dependencies, and it should include timelines, milestones, and checkpoints. The resumption of normal business operations typically occurs when the company either reoccupies its original facility and all equipment is back up and running or when the company decides on a permanent business location (which may be the alternate site or newly acquired site). Criteria for determining the cutover to “normal operations” should be developed and the CMT should hand over operations to the management team toward the end of the business continuity phase. Clearly defining this cutover as well as roles and responsibilities will help prevent confusion during this last phase of activity.

KEY CONCEPTS

Emergency management overview

- Emergencies are chaotic events that require a coordinated response.
- Lack of a coordinated response after Hurricane Katrina exacerbated the problems.
- Contact emergency responders first but understand what their priorities will be in the aftermath of a serious event.
- Companies should be prepared to be somewhat self-sufficient in the immediate aftermath of an event.

Emergency response plans

- Emergency response plans deal with protecting people first, property second.
- Emergency responses should attempt to contain, control, or end the emergency. This includes evacuating buildings, fighting fires, turning off utilities, and other response activities.
- ERTs should have the skills required to address the specific needs of your company’s operations.
- Training is imperative for ERT members. Training should be refreshed and tested periodically.
- Training for ERT members may include firefighting, CPR, first aid, hazardous material containment, and other skills appropriate to the location and nature of your business.

- Emergency response checklists help keep people calm and focused on next steps. Develop emergency response checklists in conjunction with expertise from your ERT and local civil emergency responders (fire, police, hazmat, bomb squad, etc.).

Crisis management team

- The CMT may activate the emergency response or it may be activated by the ERT.
- The CMT manages, directs, and oversees the DR efforts.
- CMT responsibilities include emergency and disaster response as well as coordinating efforts related to alternate facilities and work sites, communications, human resources, insurance, legal, and finance.
- CMT roles and responsibilities should be clearly delineated.
- MTD and other recovery metrics should be well understood by the CMT and addressed by recovery plans.

Disaster recovery

- Activation checklists can be used to determine if, how, and when to activate the BC/DR plan. In some cases, activation of part of the plan may be warranted.
- Clear activation checklists help responders understand what steps to take and help them make better decisions in the confusion that surrounds major disasters or disruptions.
- DR checklists should include MTD and other recovery metrics, so the CMT can make decisions appropriate to these requirements.
- DR checklists should address the safety and well-being of personnel first, then address physical facilities, buildings, equipment, and other business assets.

IT recovery

- Having clear and concise service levels and step-by-step application recovery procedures expedite recovery operations according to business requirements.
- Review your IT recovery checklists to determine what pre-IT recovery information must be readily accessible and part of the BC/DR plan, prior to actual IT recovery procedures.
- Every company should have a CIRT that responds to incidents related to IT equipment.
- Incidents may be unusual activity, intentional or unintentional breaches, hardware failures, and so on.
- CIRT activities are both day-to-day and part of BC/DR activities.
- The responsibilities of the CIRT include monitoring, alerting, mobilizing, assessing, stabilizing, resolving, and reviewing all IT-related incidents (incidents as defined by the team).
- CIRT skills should be kept up to date, so they are aware of and can respond to the latest threats, vulnerabilities, and issues on the IT realm.

Business continuity

- Business continuity activities typically involve the resumption of limited business operations.
- These activities typically involve manual and work-around systems, while equipment and IT systems are being fully restored.
- The decision to move to a permanent facility, whether returning to the original location, staying at the alternate site, or acquiring a new location, typically triggers the final stage of business continuity and signals the resumption of normal operations.
- Business continuity checklists should be used to ensure that required systems are in place and functional. Checklists should also contain references to timelines, milestones, dependencies, and other business metrics.
- Once business continuity activities end and normal business resumes, the BC/DR teams should review lessons learned so they can be incorporated into the BC/DR plan.

References

- Carnegie Mellon University's Software Engineering Institute. Action list for developing a Computer Security Incident Response Team (CSIRT); 2006. Retrieved May 26, 2013, from Carnegie Mellon University's Software Engineering Institute, http://www.cert.org/csirts/action_list.html.
- Carnegie Mellon University's Software Engineering Institute. CERT; 2013. Retrieved May 26, 2013, from Carnegie Mellon University's Software Engineering Institute, www.cert.org.
- National Institute of Standards and Technology; 2013. Retrieved May 26, 2013, from U.S. Department of Commerce National Institute of Standards and Technology, <http://www.nist.gov/index.html>.
- Ward A. CIO decisions conference; 2006. Retrieved May 26, 2013, from Tech Target, <http://media.techtarget.com/digitalguide/images/Misc/AwardMississippi.pdf>.

This page intentionally left blank

Business Continuity and Disaster Recovery for Small- and Medium-Sized Businesses

IN THIS CHAPTER

- Overview of SMB disaster recovery
- SMB disaster preparedness: Survey results
- SMB IT disaster recovery strategies
- SMB IT DR case studies
- Summary
- Key concepts

OVERVIEW OF SMB DISASTER RECOVERY

In this chapter, we will explore traditional as well as emerging IT disaster recovery strategies for small- to medium-sized businesses (SMBs). In addition, you will learn how several SMBs are implementing a variety of IT DR strategies in order to meet their DR requirements.

One of the most common reasons cited by executives for not funding BC/DR planning efforts is that they see it as a very expensive insurance policy for risks which haven't been identified or characterized in terms of likelihood or business impact. Before implementing any recovery strategies discussed in this chapter, it is imperative that you do the following first:

1. *Perform a risk assessment for your SMB.* If you don't understand the unique set of threats and vulnerabilities specific to your company, you will likely fail at implementing an effective DR strategy. [Chapter 4](#), Risk Assessment, is a great place to start.
2. *Perform an impact analysis for your SMB.* If you are unable to quantify the impact of unplanned outages to the company's bottom line or reputation, you will not be able to determine your DR requirements or know the correct budget for implementing a recovery strategy. [Chapter 5](#), Business Impact Analysis, can help you put your BIA together. Furthermore, the section titled "Example of Business Impact Analysis for Small Business" in [Chapter 5](#) describes specifics for a hypothetical SMB.

3. *Determine your DR requirements.* Requirements, such as MTD, recovery time objective (RTO), WRT, and RPO, need to be fully understood for all IT systems and data before deciding on an appropriate recovery strategy. Again, [Chapter 5](#), Business Impact Analysis, can help you quantify these DR requirements. Without an understanding of real requirements, you will likely fail at DR planning and spend too much or too little time, money, and resources on protecting your SMB's IT assets.

Looking forward, we assume you already understand the critical concepts and terminology from [Chapters 4](#) and [5](#), and you already completed a risk assessment, including a BIA, for your SMB. The importance of spending time on these efforts *first* cannot be overstated. Once your critical functions and the supporting IT infrastructure have been identified and the impact of an outage to your critical business processes is quantified using a dollar value or rating, a recovery strategy can be properly developed to help prevent or mitigate losses from a disaster. This is also when we need to start considering any existing contingencies or redundancies already in place. For example, if a critical application is hosted by a service provider and under a service-level agreement (SLA), it is probably safe to say that little to no recovery strategy is required for that application. This is one of the benefits of utilizing Software-as-a-Service (SaaS) applications in the cloud.

However, a recovery strategy is required for applications which support critical functions that lack provisions to keep those applications operational. An application with an RTO of within 5 days may do just fine with a tape backup off-site rotation process, but an application that needs to be up within an 8-hour business day might require remote data replication and/or standby IT systems at a recovery site.

Outsourcing disaster recovery is also a viable strategy. Companies that cannot afford the cost of developing their own recovery strategy may consider paying for managed or outsourced DR services or paying for a DR-as-a-Service (DRaaS) subscription. The key is to always remember that the total cost of a recovery strategy should never exceed the losses it is designed to prevent.

Also in this chapter, we will discuss common disaster recovery strategies as well as the advantages and disadvantages of newer cloud DR strategies for SMBs. A specific recovery strategy is determined by an organization's anticipated financial losses if critical functions are unavailable, as well as the time needed to recover necessary applications. Since all companies, regardless of size, will have different DR requirements for different IT applications and data sets, it is important to remember that there is no economical "one size fits all" approach. Therefore, we will also discuss relative cost of each strategy, keeping in mind the lowest cost recovery strategy which meets RTO/RPO requirements is always preferable for a particular IT application, and the most economical plan will likely involve a mix of recovery strategies. First, we will take a look at some statistics on SMBs and disaster preparedness.

SMB DISASTER PREPAREDNESS: SURVEY RESULTS

According to a 2012 Symantec Corp. disaster preparedness survey of more than 2000 SMBs who employ between 5 and 250 employees, widespread use of mobile devices, cloud, and virtualization was found. The study included 2,053 organizations in 30 countries, although not all the respondents were Symantec customers, according to the company. According to the survey:

- About two-thirds of SMBs said they trusted their ability to restore data from their backups. Forty-one percent said they were “somewhat” confident, and 24% said they were “extremely” confident to restore data from backup. Another 25% said they were “neutral” on their backups, while 8% were not very confident in their backups. Two percent—or about 40 of the respondents—said they were “not at all” confident in their backups.
- More than 20% of respondents were “not very” prepared or “not at all” prepared for DR, while 31% said they were neutral. Another 36% of respondents replied they were either “somewhat” or “extremely” prepared.
- Twenty-two percent of respondents replied that they don’t have a DR plan, nor will they create one. By comparison, 26% replied they had a plan. Another 33% are discussing whether to create plan, and 19% are creating a DR plan, according to the study.
- Thirty-five percent of SMBs are using mobile devices to access business information, and another 34% have taken advantage of server virtualization.
- Cloud implementation was close for public or private—public cloud use was reported to be 40%, and private cloud use was at 43%, according to the study.
- In terms of adopting server virtualization and public cloud services, 34% of IT executives said that the ability to quickly recover from a disaster had a “moderate to large” effect on their decisions. Similarly, 36% reported the same for mobility solutions and 37% let those factors guide their private cloud strategies.
- A substantial majority, 71%, said server virtualization improved on their capability to get backup and running in the wake of a disaster. For private and private clouds, 43% and 41% said the same, respectively. Mobile solutions improved on the disaster preparedness of 36% of respondents ([Symantec, Inc., 2012](#)).

These findings are especially important in light of the fact that one study found that, after Hurricane Katrina, less than 26% of businesses reopened in the City of New Orleans after 4 months; after 10 months, the number wasn’t that much better—only 39% ([Lam et al., 2009](#)).

ON-PREMISE DISASTER RECOVERY

On-premise disaster recovery for SMBs is typically the most expensive of all DR options because you typically have to plan to have an alternate DR site ready with the necessary power, environmental controls and spare compute, storage and

network capacity sitting idle during normal operations. Even if an alternate DR site isn't required, you still have to incur up front capital costs for things like additional hardware, additional software licenses, backup media, physical space, environmental controls, and the like. Moreover, operating expenses are also higher due to the additional labor and hardware/software maintenance required to support the in-house DR equipment and processes.

Although an entirely on-premise DR solution may be too costly, there are common on-premise DR investments that typically make sense for most SMBs because they are relatively low cost in terms of the benefit they provide. For example, preventative measures should always be implemented if you have on-premise IT production systems in order to thwart common threats which present a high risk of unplanned outage. Common on-premise preventative (i.e., risk mitigation) measures include:

- Disk RAID/mirroring technologies for critical servers and workstations
- Internet firewalls
- Surge protectors and uninterruptible power system (UPS)/backup generators for critical in-house backend systems
- Fire alarms and extinguishers near computer equipment
- Antivirus/malware prevention software installed on every computer

There also may be additional on-premise risk mitigation measures which make sense in limited disaster scenarios, such as local data backup to tape or disk, where backup media are rotated off-site at a remote location periodically. Or, you may choose to regularly back up to local media for limited disasters and also replicate your backup data to a cloud provider over the Internet, ensuring both file encryption and secure encrypted transmission protocols are used in order to prevent unauthorized access. Either way, it is important to note local or remote data backups alone are typically never an adequate DR solution. Even if you are a small office/home office (SOHO) business, a single human-caused or natural disaster can wipe out your entire facility in an instant and leave you with no IT hardware or facility to restore to, in order to meet your most stringent RTO.

One question to answer with on-premise DR is, "Might I be overspending on DR?" If you have designed an entirely on-premise DR solution that treats all IT systems the same, the answer is probably yes. For example, if your impact analysis determines there are only two applications that need to be restored within 12 hours in the event of a disaster, but you have over-designed it so that all 10 applications are available within 12 hours, think about where you can reduce or transfer costs to derive greater benefit. Are you paying for spending more time on DR processes that is best used elsewhere? Are you paying yearly hardware maintenance on DR equipment? Are you paying for additional software licenses, facility space, power, etc., for DR equipment? Are you paying more to store backups or archive data that are not needed? Can you consolidate servers and reduce active network ports? Are your production servers underutilized, and not virtualized and consolidated? Are you utilizing compression and deduplication technologies before purchasing additional

storage? Are you utilizing WAN acceleration before you spend extra money each month to upgrade your WAN links?

For SMBs, it may be possible to derive IT cost savings from existing operations in order fund new BC initiatives, such as implementing an improved recovery strategy for critical applications or having a third party perform a risk assessment and impact analysis so you can see where your gaps are first.

SMB case studies

There are a number of very useful examples of how small and medium businesses have used on-premise disaster recovery to addressed business continuity and recovery after a disaster. In this section, we'll look at two SMBs and their experience after a disaster so that you can better understand what worked in the hopes of better preparing your business for a similar event.

Hurricane Sandy, which made landfall in 2012 just south of Atlantic City, New Jersey, brought an 820-mile wide path of tropical storm-force sustained winds to the East Coast of the United States—more than double the landfall size of Hurricanes Issac and Irene combined. Thousands of homes flooded and more than 100 people died. 8.1 million homes lost power, many for days and weeks afterward. In New York City, gasoline rationing was in effect for the following 15 days. Despite this grim reality, businesses in the area that had preplanned for such disasters were in better shape than others to bounce back and survive. The next two brief case studies are excellent examples.

High availability at 24 Seven Talent

24 Seven Talent, an international staffing company for creative industries, lost power at its downtown Manhattan headquarters on the evening of Oct. 29 and did not regain it until Nov. 3. The office had closed Monday, Oct. 29 as a precaution, but the IT director needed to perform payroll, the company's main IT job, the following day. Because paying its staff is critical to its operations, 24 Seven handles it internally instead of outsourcing it to a company, such as ADP or Paychex. With staffers around the world expecting checks to go out on Oct. 30, the IT director put the company's disaster recovery (DR) plans into effect that morning. When they knew it would be a serious issue, that Tuesday, Oct. 30, around 1 p.m., they started bringing up servers at their DR center in their Los Angeles office. They can never miss payroll by more than a day because they would lose goodwill with their employees, which drives their revenue. Even though New York employees might understand if they did not get paid during Sandy, their other employees around the world wouldn't understand and the impact to their business would be unacceptable.

24 Seven has Dell EqualLogic SANs in its New York and Los Angeles offices and also maintains Quorum onQ high-availability appliances at both sites. They also keep a check printer off-site that was retrieved and moved to a shared office space the company maintains at another site in Manhattan. The Los Angeles office brought up two database servers required to process payroll using onQ appliances, and they used

remote access servers from the relocated office in Manhattan to get the payroll done on time and print the checks to mail. 24 Seven licensed the onQ appliances earlier in October, but had time to test the failover and fallback processes before the storm hit. They tested each recovery node to make sure it would come up OK, and they tested the synchronization between offices. During the storm, everything came up right away, according to plan. Working with the staff in LA, they were able to bring everything up within an hour ([Raffo, 2012](#)).

Affigent fails over before the storm

Affigent LLC, a technology consulting firm for government agencies, escaped the brunt of Hurricane Sandy at its Herndon, VA, headquarters, but failed over to its Chicago secondary data center as a precaution on the first day of the storm. Through its managed service provider (MSP) Integrity Virtual IT, Affigent redesigned its infrastructure with an eye on DR in 2011. Affigent now uses Zerto Virtual Replication to protect data on its SAN at Integrity's Reston, VA-based data center. Affigent's business operations director said he was prepared for the worst because of advance warnings of Sandy, and the management team decided over the weekend they would begin failing over Monday afternoon Oct. 29 unless the storm took a turn out to sea. The final decision came Monday morning.

Affigent's offices never lost power, but their offices would have been up and running in any case. They executed the flip over from the primary site to the DR site Monday afternoon. They had an hour downtime as planned. It took 30 or 40 minutes to move from one data center to the other, and the other 20 minutes were used to test if the applications were performing as they were supposed to. Within the hour, they were fully operational at the recovery site. Affigent ran its IT from the Chicago site for nearly 3 days until switching back on the night of Oct. 31, with that process also taking about an hour to switch and test all the applications. Affigent takes a better-safe-than-sorry approach because it can't afford much downtime. The firm bids on its contracts, often on tight deadlines. Any outage is a big deal for them since their business is transaction-based. They have to get their quotes out, and their customers don't waive deadlines for those. If they don't hit their deadline, they lose the deal by default. If there's a large procurement on the street and they need to answer it and miss the deadline, it could mean the loss of millions of dollars of potential business. Even though the storm didn't cause loss of power in their Virginia office, enacting their DR plans was a precautionary move and gave them greater confidence if other disasters hit. If they lose connectivity, they know they are able to execute from their recovery site. If they had an unplanned event like a power loss, they would still be able to initiate transfers from a remote site ([Raffo, 2012](#)).

USING A CO-LOCATION DATA CENTER FOR DISASTER RECOVERY

Co-location centers (also referred to as co-los or carrier hotels) are a type of data center where multiple customers install network, server, and data storage devices, and interconnect to a variety of telecommunications and other network service

provider(s). Today, co-location centers provide Internet access as well as other types of voice/data services. Depending on a company's size and IT requirements, a co-location facility can become the company's data center, provide a secondary site to the headquarters' data center that supports only certain critical systems, or provide a disaster recovery facility. This last option assumes the co-location site is sufficiently distant from the company's main location so that it will not be affected by the same disaster.

The value of co-location data centers in a disaster

Companies in both the private and public sectors are recognizing the benefits of co-locating their mission-critical equipment in a suitably equipped data center. Companies can save time and cost by sharing data center infrastructure resources, and high capacity network access. Significant benefits of scale (needed for large power and mechanical systems) result in large co-location facilities, typically 50,000-100,000 square feet. With IT and communications facilities in safe and secure locations, companies of all sizes benefit from improved system response times and the freedom to focus on their core business. These facilities also provide a secure disaster recovery capability so companies can locate IT backup assets, such as network services and data storage, in off-site locations.

Tips for selecting a co-location provider

It's important to choose a co-location provider wisely since there are many options to consider. When choosing a co-location provider, here are some considerations.

- *Choose a top quality Internet network.* Ask the co-location provider(s) about their Internet network connection size and details.
- *Choose a state-of-the-art facility.* Make sure it has highly scalable with fast connections to the leading Internet backbones, redundant UPS and generator-backed electrical power, redundant HVAC systems, and 24/7 on-site support.
- *Choose a provider who's been around for a while.* Find a co-location provider that has proven itself over time, especially with BC/DR incidents.
- *Choose a provider with a good financial background.* A financially sound company allows for better pricing and overall technical security because there are no hidden/excess charges attributed to alleviating company financial burdens. Choose a provider that has been consistently profitable for many years.
- *Choose a provider with no extra fees.* Look for providers that offer free network cross-connects per customer cabinet and offer free IP addresses with their service. Power for your co-located servers and equipment can often be included with co-location space without any hidden costs. Find a provider that will give you a fair rate on all the services and that does not rely on unnecessary costs.
- *Choose a provider with a large, redundant backbone.* Choose a Tier 2 or Tier 1 service provider, keeping in mind that the "tier" is largely misused as a marketing

term. By definition, a Tier 1 data center doesn't pay transit fees or settlements to reach the Internet, and they typically have very few peers. However, some Tier 2 networks are significantly larger than some Tier 1 networks and are often able to provide better connectivity at similar Internet speeds. A Tier 2 connected facility with good peering is frequently much closer to most end users than a Tier 1.

- *Look into what security the provider offers.* This includes digital surveillance cameras throughout the facility, card key or biometric locks at every entrance and exit, an enforced access list, and locking cabinets.
- *Look into whether the company specializes in co-location and business continuity/disaster recovery, or something else.* A company that specifically sells co-location and BC/DR services is technically built to handle the necessities: maximum Internet speed, expansive space, security, and technical support.
- *Look into the type of power protection the provider has.* Providers should have continuous redundant UPS and generator-backed electrical power where backup battery banks are always online to keep the power on.
- *Look into the provider's future plans.* Successful co-location providers can handle customer requirements fairly easily. Research the pricing structures for future upgrades with various providers to know how you will be charged for additional business continuity/disaster recovery services and Internet bandwidth as you grow.
- *Know their customers.* Ask for a list of customers when researching co-location providers. Brand-name customers are a good sign. Speak to the provider's customers for their comments.
- *Choose a co-location provider with internal equipment space.* For maximum security, it is best to find a provider that offers secure locking cabinets to avoid any shared technical issues or even possible problems with theft.
- *Choose a provider with several locations.* Co-location providers that offer worldwide services may have a stronger backbone and can provide your firm with global BC/DR support not possible with a smaller provider.

What does a co-location center cost?

Monthly costs for co-location centers are based on numerous factors, such as space required, power, need for Internet access, bandwidth, and the need for IP addresses. Small data centers (under 400 square feet of space) could be as low as \$1500-\$2500 per month. Larger installations (more than 5000 square feet) will range from \$25,000-\$35,000 per month. Be sure to have your initial and long-term requirements carefully defined and visit several providers to get the best price. Using a co-location service for expanding your BC/DR capabilities is a worthwhile strategy if you choose to operate and maintain your own DR hardware and software and do not have an alternate site for DR. Providers are located in most major and mid-sized U.S. cities and offer a wide range of services. This next case study explores one example of how an SMB balances cost of a co-location facility with its own internal expertise and capabilities to provide a workable solution that meets its business needs.

SMB case study: Balancing internal capability and cost with co-location data centers for DR

Poway, CA-based Mitchell Repair Information Company LLC or Mitchell 1, a Snap-On company, specializes in automotive repair manuals and software management systems for automotive repair shops. In addition to its online resources and software for mechanics, it also staffs a 50-person call center with expert technicians as a resource for customers who have questions about repairs. The company claims that despite the increasing popularity of completely outsourced or cloud disaster recovery services, deploying its own equipment in a SunGard co-location data center has proven the right mix of hosted and do-it-yourself disaster recovery (DR) and data center load-balancing for the company.

About 4 years ago, the company began a relationship with SunGard Availability Services to place servers and NetApp Inc. storage gear owned by Mitchell 1 at one of SunGard's data centers in Scottsdale, AZ. Today, four NetApp FAS2040 disk arrays replicate data from remote offices to a 100 TB (terabytes) FAS 3160 array at its main data center, where the remote office disk arrays are also managed remotely. All told, the organization has between 90 and 100 TB of data. SunGard is also contracted to provide facilities for call center employees in the event of a primary site outage. While 100 TB is no small amount of data, at 350 employees, 200 of which are sales representatives spread around North America, the organization considers itself an SMB. None of their remote offices were equipped to act as DR location to host all their data from their 3000 square foot data center at headquarters. It was estimated two of them even had the right kind of air conditioning. At the same time, purchasing an entire second data center just to have something sitting waiting in case of a disaster was not palatable to the organization. As a smaller business, they can't afford to set up \$300,000-\$400,000 worth of facility space, software, and networking hardware to support an idle DR site.

When they entered into the relationship with SunGard, cloud-based disaster recovery had yet to become an industry buzzword, but wholly managed disaster recovery services were available at the time. Today, outsourcing management of data replication and storage to a service provider completely for disaster recovery is seen as having cost benefits, but the business is unwilling let go of that part of IT's role. The company says it all depends on what your core competencies are. For them, their call center is important, and their ability to provide information to their customers quickly through telephony and storage connectivity is their core competencies. Still, the company says it can be difficult as a relatively small business to get the best customer service from co-location providers. The company went with SunGard because of its Information Availability for Small and Midsize Business Program. They admit they are not AT&T or American Airlines, but SunGard worked closely with them to offer a solution that met their requirements.

That said, there are some aspects of SunGard's pricing the company says are better suited to larger enterprises with deeper pockets. For example, SunGard changed billing on power distribution units (PDUs) from a usage basis to a per-device basis.

Therefore, if the company has to add a PDU, they now have to pay an additional \$570 a month instead of just paying for the equipment once and the total monthly power usage for the rack. The company notes if they were a bigger company, that amount of money would be a drop in the bucket, but SMBs like themselves will begin to question these price hikes. SunGard claimed they expanded their pricing practices from circuit-based pricing to KW-based pricing in order to help customers under specific circumstances better manage their power costs. SunGard claimed it makes it easier for some customers to manage the number of circuits they provision and better utilize their KW power use ([Pariseau, 2010](#)).

DISASTER RECOVERY IN THE CLOUD

Cloud computing, along with mobile and tablet devices, accounts for much of the high-tech buzz these days. But when it comes to hype, the cloud seems to absorb more than its fair share, which has had the unintended consequence of sometimes overshadowing its real utility. The primary difference between on-premise DR or use of a co-location facility, and cloud DR, is that cloud DR specifically implies that the outsource provider owns the underlying compute and storage hardware (and possibly software, as well) and that you access these resources via the Internet using secure, encrypted transmission protocols, or via a dedicated connection you pay for. This arrangement is known as Infrastructure-as-a-Service or IaaS. In addition, cloud providers may also own and lease you the required software platform, such as the operating system, Web server software, run-time programming language software, and the like. This is known as Platform-as-a-Service or PaaS. Moreover, the cloud provider may also own and provide you access to their software application over the Internet. This is known as Software-as-a-Service or SaaS.

Although the concept—and some of the products and services—of cloud-based disaster recovery is still nascent, some companies, especially SMBs, are discovering and starting to leverage cloud services for DR. It can be an attractive alternative for companies that may be strapped for IT resources because the usage-based cost of cloud services is well suited for DR where the secondary infrastructure is parked and idling most of the time. Having DR sites in the cloud reduces the need for data center space, IT infrastructure, and IT resources, which leads to significant cost reductions, enabling smaller companies to deploy disaster recovery options that were previously only found in larger enterprises.

Some of the primary benefits of employing cloud DR in your overall DR strategy include the following:

- *Pricing is transparent and subscription-based.* Pricing includes all the software, infrastructure, and services to deliver the solution. You are typically charged per gigabyte of data, per server, or for a combination of the two. The only cost not included is the cost of network connectivity. You pay for only the servers you want to protect.

- *Deployment is fast and easy.* Most of the recovery configuration can be done online, because there's no need to reserve identical hardware, set up proprietary links, or negotiate your specific SLA. Since the backup is to virtual volumes and servers, you simply have to ensure that the right virtualization layers are in use. However, services are typically limited to your x86 server environments.
- *Oversubscription risk is minimized.* In traditional managed DR services, the provider subscribes several clients to the same IT resources, closely manages the oversubscription ratio, and avoids subscribing clients from the same region to the same equipment. But there's a chance that multiple, simultaneous disasters will be declared, in which case you won't get access to the IT equipment you've spent thousands of dollars a month holding in reserve. While the same can still be true with cloud DR services, the risk is minimized because far more customers can be packed onto the same physical IT infrastructure.
- *The penalty for rehearsing your DR plan is reduced.* What good is a DR plan if you don't rehearse it to make sure it works? Traditional DR service providers recognize this but have to schedule rehearsals, reserve equipment, and often be on call for you during the rehearsal. All this preparation costs money and is typically above and beyond the DR services contract. With cloud DR services, there's usually minimal or no prep required, allowing you to rehearse more easily and at much lower cost.

Despite its benefits, disaster recovery in the cloud isn't a perfect solution, and its shortcomings and challenges need to be clearly understood before a firm adopts it as a solution. Security usually tops the list of concerns:

- Are data securely transferred and stored in the cloud?
- How are users authenticated?
- Are passwords the only option or does the cloud provider offer some type of two-factor authentication?
- Does the cloud provider meet regulatory requirements?

Also, since clouds are typically accessed via the Internet, bandwidth requirements also need to be clearly understood. There's a risk of only planning for bandwidth requirements to move data into the cloud without sufficient analysis of how to make the data accessible when a disaster strikes:

- Do you have the bandwidth and network capacity to redirect all users to the cloud?
- If you plan to restore from the cloud to on-premises infrastructure, how long will that restore take?

Reliability of the cloud provider, its availability, and its ability to serve your users while a disaster is in progress are other key considerations. The choice of a cloud service provider or MSP that can deliver service within the agreed terms is essential.

According to a 2012 survey on SMB cloud adoption, a significant increase in paid cloud services over the next 5 years among SMBs is predicted. The research

conducted by Edge Strategies includes survey responses from IT decision-makers or influencers at more than 3000 SMBs in 13 countries. According to survey results, paid cloud services are expected to double in 5 years, while the number of the world's smallest companies using at least one paid cloud service will triple in the next 3 years. In addition:

- Cloud computing is able to deliver more of what SMBs need—cheaper operations and faster, better fusion of vital information to virtually any device. In fact, the research finds 59% of companies currently using cloud services report significant productivity benefits from information technology, compared with just 30% of SMBs not yet using the cloud.
- Despite a sluggish global economy, 63% of SMBs using cloud services today expect to grow in sales in the next 12-18 months, while 55% believe technology will power their growth. SMBs worldwide are embracing cloud services to reap those benefits and stay ahead of competitors—50% of SMBs say cloud computing is going to become more important for their operations and 58% believe working in the cloud can make companies more competitive.
- Security is a priority but no longer a main concern. Only about 20% of SMBs believe that data are less secure in the cloud than they are in their on-premise systems. Thirty-six percent overall and 49% of larger SMBs actually think that data are as secure in the cloud as in their own systems.
- Local is better when it comes to service providers. Most SMBs feel it is important to buy services from a provider with a local presence, and 31% feel this is critical ([Edge Strategies, 2012](#)).

Disaster recovery in the cloud options

When looking at cloud options for BC/DR, there are many different ways to slice and dice the use of cloud. As was stated earlier, SaaS is one of the fastest growing segments of cloud IT. With SaaS, your third-party provider typically has developed their own software and is offering it to you on a subscription-based pricing model, as opposed to perpetual license model (where you install it at your site and have rights to use the software on your own hardware in perpetuity). With SaaS, the dependent IT hardware and underlying infrastructure which runs the software is provided to you, managed by an external third-party software provider and typically accessed securely over the Internet using a Web browser. In addition, the provider manages both the primary and backup (or DR) instances of both their software and your data. If you suffered a disaster, you would simply need to get back on the Internet with a common Web browser at any alternate location to access the software and data again. If your cloud provider's primary location suffers a disaster, they are responsible for recovery of your data to one of their operational sites within agreed upon service levels. With your data hosted externally, there are legal and privacy implications to consider and it is critical you understand the terms of use or contractual obligations before you sign up. As with all cloud IT services, access to the Internet or a private

network connecting you and the cloud provider is an essential component of accessibility. That said, SaaS certainly offers one of the best DR solutions for SMBs with limited resources, even if availability of your IT solution is dependent on a third-party Internet or network connection and a third-party MSP.

The second sphere of cloud IT services includes offerings such as IaaS or PaaS. In both cases, you own and manage the application software and/or data, and the cloud IT provider owns the resident hardware and underlying infrastructure. These offerings are essentially one step removed from SaaS and provide things like backup storage and/or alternate compute facilities for you to use in a DR scenario. PaaS differs slightly from SaaS in that PaaS implies you need a specific compute environment to run your software and data from their site in a DR scenario (where they own and provide the licensed operating system, storage, or Web platform you need). To make things more complicated, the industry has developed other specialized terms for what are, essentially, IaaS and PaaS offerings, such as DRaaS and RaaS (Recovery as a Service). IaaS and PaaS offerings are typically employed for DR purposes when you manage the production instances of the software and underlying hardware at your own primary site, but *in lieu* of an alternate DR site you own or lease, you keep backups of data and/or supporting virtualized operating systems at the third-party providers' site in case of a disaster at your primary site. **Table SMB.1** compares and contrasts different approaches for disaster recovery strategies in the cloud.

Table SMB.1 Comparison of Cloud-Based DR Approaches

	Managed Primary and DR Instances	Cloud-Based Backup and Restore	Replication in the Cloud
Instances	<ul style="list-style-type: none"> Salesforce.com E-mail in the cloud Other SaaS 	<ul style="list-style-type: none"> On-premise in the cloud Cloud to cloud IaaS 	<ul style="list-style-type: none"> On-premise in the cloud Cloud to cloud PaaS
Benefits	<ul style="list-style-type: none"> Fully managed DR 100% Usage based Least complex 	<ul style="list-style-type: none"> Only requires cloud storage Cloud virtual machines are optional Usually less complex than replication 	<ul style="list-style-type: none"> Best RTO and RPO More suited to support application-consistent recovery
Considerations	SLAs define access to production and DR instances	Less favorable RTOs and RPOs than replication	Higher degree of complexity
Implementation	N/A	Backup applications and appliances	<ul style="list-style-type: none"> Replication software Cloud gateways Cloud storage software

Managed applications and managed DR

As was stated earlier in the SaaS example, an increasingly popular option is to put both primary production and disaster recovery instances into the cloud and have both handled by an MSP. By doing this, you’re reaping all the benefits of cloud computing, from usage-based cost to eliminating on-premises infrastructure. Instead of doing it yourself, you’re deferring DR to the cloud or MSP. The choice of service provider and the process of negotiating appropriate SLAs are of utmost importance. By handing over control to the service provider, you need to be absolutely certain it’s able to deliver uninterrupted service within the defined SLAs for both primary and DR instances. The relevance of SLAs with a cloud provider cannot be overstated; with SLAs, you’re negotiating access to your applications.

A pure cloud play is becoming increasingly popular for e-mail and some other business applications, such as customer relationship management (CRM), where Salesforce.com has been a pioneer and is now leading the cloud-based CRM market.

Back up to and restore from the cloud

Applications and data remain on-premises in this approach, with data being backed up into the cloud and restored onto on-premise hardware when a disaster occurs. In other words, the backup in the cloud becomes a substitute for tape-based off-site backups.

When contemplating cloud backup and recovery, it’s crucial to clearly understand both the backup and the more problematic restore aspects. Backing up into the cloud is relatively straightforward, and backup application vendors have been extending their backup suites with options to directly back up to popular cloud service providers such as AT&T, Amazon, Microsoft Corp., Nirvanix Inc., and Rack-space. Cloud gateways, such as F5 ARX Cloud Extender, Nasuni Filer, Riverbed Whitewater, and TwinStrata CloudArray, can move data deduplicated (or deduped), compressed, and encrypted into the cloud and allows setting retention times of data in the cloud. They straddle on-premises and cloud storage, and they can keep both on-premises data and data in the cloud in sync.

The challenging aspect of using cloud-based backups for disaster recovery is the recovery. With bandwidth limited and possibly terabytes of data to be recovered, getting data restored back on-premises within defined RTOs can be challenging. Some cloud backup service providers offer an option to restore data to disks, which are then sent to the customer for local on-premises recovery. Another option is to additionally maintain a large on-premises cache of recent backups that can be used for local restores.

Depending on the data to be restored, features like compression and, more importantly, data dedupe can make restores from full systems in the cloud to on-premises infrastructure a viable option. A case in point is Michigan-based Rockford Construction Co., which uses a StorSimple appliance for cloud-based protection of its Exchange and SharePoint infrastructures. In the event of a disaster, they pull virtual machines (VMs) from the cloud; with StorSimple’s deduplication, they are able to pull down one full VM copy and only the differences for others.

Back up to and restore to the cloud

In this approach, data aren't restored back to on-premises infrastructure; instead, they are restored to VMs in the cloud. This requires both cloud storage and cloud compute resources, such as Amazon's Elastic Compute Cloud. The restore can be done when a disaster is declared or on a continuous basis (prestaged). Prestaging DR VMs and keeping them relatively up to date through scheduled restores is crucial in cases where aggressive RTOs need to be met. Some cloud service providers facilitate bringing up cloud VMs as part of their DR offering.

Replication to VMs in the cloud

For applications that require aggressive recovery time and recovery point objectives (RPOs), as well as application awareness, replication is the data movement option of choice. Replication to cloud VMs can be used to protect both cloud and on-premises production instances. In other words, replication is suitable for both cloud-VM-to-cloud-VM and on-premises-to-cloud-VM data protection. Replication products are based on continuous data protection (CDP), such as CommVault Continuous Data Replicator, NetApp SnapMirror, or object-based cloud storage such as EMC Atmos or the Hitachi Content Platform (HCP).

The cloud greatly extends disaster recovery options, yields significant cost savings, and enables DR methods in SMBs that were previously only possible in larger organizations. It does not, however, change the DR fundamentals of having to devise a solid disaster recovery plan, testing it periodically, and having users trained and prepared appropriately.

Protecting branch offices with cloud disaster recovery

Disaster recovery for remote and branch offices (ROBOs) has always been a challenge for SMBs. Branch offices are often collections of point-solution technologies built up over time to include one-off hardware platforms and/or aging user desktops. Efforts to simplify branch offices involve reducing the number of platforms or centralizing backend services, but they are often stymied by their impact on user experience and productivity. The IT consolidation wave of the past decade also shifted focus to the data center and the server infrastructure, both of which are more easily tweaked and typically better managed than remote offices, especially in smaller enterprises.

As they look out to the remote office infrastructure today, IT departments are increasingly looking to emerging cloud computing solutions as a way to provide better availability in remote offices today. Cloud computing can keep the need for additional manpower, servers, and data storage to a minimum. But can the cloud offer a viable solution for remote office disaster recovery? The best answer is probably "partially." Disaster recovery goes beyond just data backup and server protection and encompasses a complex mix of technologies, processes, and compliance issues, such as connectivity, multisite data replication, and workload redundancy, that must

be orchestrated at each remote office. Thus, the cloud may or may not be suitable for all DR issues at your remote site.

However, new cloud disaster recovery offerings are appearing at a brisk pace such as services offered by Simply Continuous. Simply Continuous combines both data protection and workload protection by replicating data and VM images between a branch Data Domain appliance and the Simply Continuous data center. In event of disaster, the replicated data are ready to go, and the most current version of a customer's application servers can be quickly restored from virtual hot standbys to bare metal. Moreover, all replicated data are heavily deduplicated, making efficient use of limited WAN links.

As disaster recovery vendors continue to improve their cloud disaster recovery products, you should also prepare your branch office to be ready for cloud disaster recovery. The following sections summarize the critical steps you need to take before you take your ROBO to the cloud.

Virtualize and consolidate servers

The first step in readying the branch office for the cloud should be to break as many hard links between applications, data, servers, and networks as possible. Virtualization technologies exist across the IT stack and deliver two critical elements: encapsulation and mobility. Any service that you would like to move to or protect in the cloud must be both platform and location independent.

Virtualizing branch office servers will allow you to take advantage of advanced workload protection features provided by hypervisor platforms. In a VMware environment, these include snapshots, high-availability (HA) clustering, distributed resource scheduling (to place workloads automatically on the optimal server), site recovery management, and even fault tolerant “lockstep” execution, which protects against any individual server failure with virtually no downtime. Once virtualized, server workloads can also be replicated in real time to a central data center or to a cloud service.

Such solutions for virtual workload CDP are available from several vendors, such as FalconStor Software and InMage Systems, and are offered both as technologies you deploy in your environment or via cloud service providers. Although server consolidation increases the risk of a single hardware failure affecting multiple applications, the broad range of workload protection technologies for virtualized environments, such as HA clustering, more than compensates for this increased business risk. Plus, the wealth of provider offerings available for cloud protection of virtual workloads ensures that prices will continue to come down, as will the risk of provider lock-in.

Virtualize and streamline data storage and backup

Similarly, storage virtualization in the remote office not only delivers new capabilities for data protection but allows IT departments to explore cloud storage offerings not available for branches that rely solely on local file servers for data and/or tape backups for disaster recovery.

First, if your data protection strategy in the branch is primarily tape-based, you should explore disk-based replication options. In the past, disk-to-disk backups may have been cost prohibitive, which kept many branch offices dependent on tape for DR. But the future of disaster recovery is disk-based replication, and the falling cost of higher density disk storage combined with the use of data deduplication and compression technologies can significantly reduce the upfront cost of new storage infrastructure by slashing capacity requirements.

To do this effectively, you should build a test environment in which you migrate some of your branch backups from tape to disk, then deduplicate and replicate these backups to a central facility. This will enable you to become familiar with the technology and establish acceptable RTOs and RPOs. You'll need to have these requirements in place, well documented and well tested, before you can compare the cost benefits and availability trade-offs of any eventual move of your replicated data to a cloud provider.

Once more data are backed up to disk, you can explore emerging cloud-based file storage gateways, object storage services, and application-specific data archiving services, such as those from Asigra Inc., Iron Mountain Inc., LiveOffice, Nirvanix Inc., Robobak, and Symantec Corp. The key is to create a virtualized storage environment in the branch that supports incremental, experimental movement of different data types and backup sets to the cloud. It might make sense to archive e-mail in the cloud first, for example, to prove the cost benefits and validate recovery SLAs, before moving on to other data types.

Virtualize applications and desktops

Applications and user desktops are also essential elements to examine when readying a remote office for cloud disaster recovery. Application delivery is arguably the most important function of remote office infrastructure and often the most challenging aspect of DR planning. Disaster recovery planning falls generally into two major categories: where should applications reside for highest availability, and how will users access them in the event of disaster?

For maximum resiliency, hosted applications delivered in a SaaS model can insulate the remote office and remote user the most from failure. The service provider market for office productivity application hosting is maturing rapidly, and the days of local Exchange and SharePoint servers in remote offices are likely numbered.

For those applications that cannot be outsourced, or that you are not ready to outsource, various flavors of application virtualization are available from vendors such as Citrix Systems Inc., Microsoft, and VMware. These include application streaming and hosted desktops, which can be deployed standalone or as part of a more comprehensive desktop virtualization strategy. However, it's important to compare the costs of virtualizing applications yourself (and putting in place the required desktop virtualization infrastructure) to the cost of outsourcing your desktops completely.

Vendors such as Desktone offer desktop virtualization in the cloud, which removes the need for you to license the virtualization platform or host and replicate virtual desktops yourself. Again, it's important to evaluate the trade-offs and costs for your particular branch requirements. It might make sense to implement a limited amount of your own internal desktop/application virtualization technology to establish cost benefits, explore ROI, and validate user experience under controlled conditions and within your corporate firewall. After you have implemented your virtualization technology, you can then move your working architecture to a service provider when feasible. Or, if your performance requirements and current cost structure are well understood, it might be more efficient to explore a cloud offering directly, without the experimental phase.

Deploy application acceleration and WAN optimization

Lastly, regardless of how much storage you move or what percentage of your applications you outsource to the cloud, the viability of any cloud-based solution for remote office disaster recovery will depend on the performance you can achieve over the WAN. WAN performance will dictate how often and how much data you can replicate, and which applications you can serve up from a disaster recovery site.

Keep in mind that network performance will make or break a cloud-based DR strategy, whether it's on the enterprise WAN behind the firewall or the public Internet, and whether you're replicating live data, recovering backup sets, opening a shared PowerPoint file, or running a remote display protocol to a thin client.

Also, application acceleration technologies and WAN optimization should be a part of any cloud-based service. The leading vendors of WAN optimization have historically relied on purpose-built hardware appliances to deliver both generalized TCP acceleration and application-specific acceleration, but this market segment is also virtualizing. Virtual appliances from vendors such as Blue Coat, Certeon Inc., and Expand Networks allow customers to deploy WAN optimization anywhere they run a virtualized server, whether that is at a data center, a remote office, or at their cloud service provider.

Several vendors also offer mobile worker solutions that enable WAN optimization directly to a user laptop. So, whatever mix of on-premise and cloud-based solutions make the most sense for your remote office DR strategy, your users can enjoy optimized network access from wherever they are.

Overall, before exploring cloud-based disaster recovery for remote or branch offices, your IT infrastructure should be as virtualized as possible, highly consolidated, and streamlined. Storage virtualization will enable you to explore cloud disaster recovery services incrementally and at different levels of the IT stack, while keeping the rest of the infrastructure in place. Also, server consolidation will simplify the number of resources to plan for and manage in the cloud. And, unless you've optimized your storage and server utilization by eliminating as much redundancy as possible before moving resources to the cloud, you're unlikely to see a compelling payback from the effort.

SMB case studies

There are many examples of SMBs using the cloud in order to meet (and even exceed) disaster recovery objectives at a lower cost than hosting internally or using a co-location facility. In these next seven brief examples, you'll see how SMBs have weathered snowstorms and hurricanes with improved cloud DR capabilities, as well as how several SMBs are preparing for future disasters at a lower cost with newer cloud technologies.

Snowmageddon and Snowpocalypse

Most SMBs that employ cloud IT use it as one of the tools in their disaster recovery plan. For some companies, the cloud itself has become the sole DR strategy in their disaster recovery plan. MacNair Travel Management, based in Alexandria, Virginia, arranges travel for corporate clients. In 2010, the company was hit by two major storms (which the COO called Snowmageddon and Snowpocalypse), dumping about 55 in. of snow in the Washington, DC area, that could have crippled their business. During both storms, not a single employee made it into the office. MacNair uses all cloud services for business operations, for all employees. The company uses a service called Cetrom IT, which houses all the company applications in a network operations center. Cetrom handles the data backups and duplicates data between two facilities.

"We can access our applications, operating systems and data anywhere at any time with only an Internet connection and browser," the COO said. "Nothing short of a nuclear holocaust can shut us down. Not being dependent on a single location or data/voice carrier, and having full, operational backup, is why the cloud is perfect for continuity of operations plans. Clearly the best disaster recovery plan is one that all but eliminates the operational impacts of a disaster before it happens."

While such a disaster recovery strategy depends entirely on the cloud, MacNair admits the cloud is not entirely foolproof. The company still asserts that there needs to be an overall disaster recovery plan for the business: Where will the employees work? How will the physical building be restored? Which IT services can be suspended while critical systems are restored? Yet, the overarching theme from their perspective was that the cloud is a critical component in disaster planning, it relieves most of the tension with IT services, and it provides a new level of business continuity ([Brandon, 2011](#)).

Amazon Web Services to the rescue

The IT manager at New York City architectural firm Diller Scofidio + Renfro was in the middle of a company-wide migration from Exchange 2003 to Gmail when Hurricane Sandy hit. Prior to knowing of Sandy's arrival, they began setting up the accounts and migrating older messages in preparation. Sandy interrupted their migration. The building's 31-foot, block-long basement was filled with water, and it actually made it up about 4 feet into the lobby above. The damage to the building

was enough that they didn't have any power at all until 5 days later. As a result, both UPSs in the server rack soon died and their servers went offline.

The partial migration to hosted Gmail turned out to be an advantage. After the hurricane, when the extent of damage all over the city was clear, it was easy to make the call to change the location of mail delivery and have people operate from partially migrated mailboxes instead of waiting for power to their servers. IT staff had migrated most of their documents already to Google Apps by the time the storm arrived, so that made it easier for them to continue the migration from home where they still had power.

Several cloud-based services also helped get the company operational again. Using Amazon Web Services, the company was able to get employees access to needed apps. They ended up setting up a server at AWS and installing the license manager for Autodesk products on it (AutoCAD, Revit, 3DS Max). By opening the right ports to the Internet, people who had laptops and hadn't checked out licenses ahead of time could change their license manager settings to the AWS server's IP address and get a license. IT staff also used AWS servers as remote desktops to work from.

A cloud storage gateway from Panzura also proved vital. The gateway is typically used to archive data to the cloud, but they were able to leverage it to make an emergency copy of recently used data as Sandy approached. Panzura also was able to set up a DR site for them to allow access to the firm's files and systems. It took about 2 days for Panzura to get everything up. This wasn't a normal service they offered at the time, so there was a bit of pleading involved ([Lynn, 2012](#)).

LAUSD implements snapshot-based cloud backup

A 2012 Spiceworks survey of 1500 SMB professional found that a quarter of survey participants were using an MSP for online backup ([YouSendIt, 2012](#)). Despite the tangible benefits of cloud DR, SMBs aren't giving up all their data. Many are still backing up data locally and using cloud providers as a storage vault. Some organizations are using cloud storage as an alternative to tape for protecting data in remote sites and eliminate tape in branch offices, including the Los Angeles Unified School District (LAUSD) and Los Angeles-based engineering consulting firm Psomas.

The LAUSD's facilities division has placed TwinStrata CloudArray Virtual Appliances in 15 remote locations across the district to back up 80 TB of primary storage to the Amazon Simple Storage Service (S3) cloud. The public cloud backup project was paid for as part of a 10-year, \$20 million bond project, and the LAUSD estimates it will save \$283,000 over 5 years. Most of the savings come from eliminating tape and using lower cost commodity servers. The district loaded TwinStrata software on Dell PowerEdge R210 file servers running VMware ESXi. Each device presents itself on the network as an iSCSI host and is attached to a Linux-based file server running Samba to emulate a Windows environment. The CloudArray virtual appliances take snapshots from local hard drives on a daily basis and send them to Amazon S3 cloud storage. If they need to restore a document that is corrupted, they can restore from snapshots as simply as they would open a folder. By moving

snapshot copies into public cloud storage, the facilities division within LAUSD eliminated the use of Symantec Backup Exec software and tape at each site.

“This is strictly mapping drives to a file share,” their IT Director said. “As iSCSI storage drivers, there is no heavy lifting. It’s a way to present storage to a file server. We can restore the data from the cloud to any location. We no longer have backup. We snapshot the data and we can roll back to any point in time. We pay for storage as we need it. If I need 10 terabytes, I pay for 10 terabytes.”

LAUSD says users access their files the same way as if they were stored locally. The District was attracted to TwinStata because it supports iSCSI and it is a virtual appliance so they could install it as software instead of buying another physical box. “This is our first move into the cloud,” their IT Director said. “At the end of three years, we will get new equipment and we will not have to deal with any data migrations” ([Lelii, 2011](#)).

Psomas moves DR to the cloud

The Los Angeles-based engineering consulting firm Psomas turned to Riverbed Whitewater backup gateways, which provides LAN-type access to public cloud storage for data protection. Psomas, which employs 500 people, replaced tape at 11 sites with one Whitewater cloud storage gateway and 10 virtual appliances. The company claimed they didn’t like tape because it costs too much and you have to buy them in bulk, manage secure physical storage of the tape, rotate the tapes periodically, etc. The company has reduced backup costs by about 40% since they started rolling out cloud devices in March. Before using the cloud, Psomas would send a driver to each location to swap out tapes.

Psomas still uses a dedicated backup server running Symantec Backup Exec. The company’s data are backed up to the Backup Exec server, which mounts the backup location to the Whitewater appliances. Whitewater dedupes and encrypts the data and stores them on to the Amazon S3 cloud. If an office stops operations for any reason, the firm could recreate a virtual Whitewater in a read-only capacity at a separate office and then run restores from the cloud using Backup Exec. “We have a much smoother disaster recovery process,” the CIO said. “We can get to any data from any office because the data is in the cloud. If we lose office A, we can run restores from office B” ([Lelii, 2011](#)).

Private cloud DR plans help BUMI

During Hurricane Sandy, the downtown Manhattan office of BUMI (Back Up My Info) had 35 feet of sea water in the building. Fortunately, BUMI, a backup and DR service provider, uses third-party data centers in Toronto and Kelowna in Canada to store and replicate customer data with NetApp storage and Asigra backup software. When the disaster hit their office, they invoked the BUMI cloud recovery plan that they had built the prior year. They took backups in their Toronto data center and started up a virtual environment to replicate their local environment using Citrix clients that their team worked off of. Once their Citrix environment was up in Toronto, they were then able to work through restoring their servers.

BUMI employees worked from their homes to restore customer data remotely for clients in the New York metropolitan area. Many of their local customers had sites outside of New York that they used to recover to. Some of their IT staff had no power at home but could access BUMI remote servers through their cell phones, for as long as they lasted. The company sent Cisco IP phones to their employees at home via FedEx that they could charge if they had power. Since the Cisco IP phones can plug-and-play anywhere there is an Internet connection, they were an invaluable resource for communication during the recovery operations. The small BUMI IT staff of nine was not able to return to their office until December. As a result of the lessons learned during Sandy, many of them now work from home which the company calls the “new normal” ([Raffo, 2012](#)).

Sprott switches course to cloud DR service provider

The VP of IT at Canadian financial services firm, Sprott, was charged with assuring business continuity prior to 2010, partly in response to regulatory pressure but also because the business needed to operate reliably. They have portfolio managers and real-time traders, so the systems need to be up and running when the markets are open.

They started down the road of piecing together a disaster recovery system that would employ virtualized servers, running on racks in a remote data center. But then the VP got a call from a company called Geminare that had created just the sort of setup he had in mind, and they were offering it as a bundled service. Geminare partners with telecommunications and hosting companies that want to offer DRaaS. They provide the network and server infrastructure, and Geminare provides the software to manage the failover and recovery process. Geminare invested in making sure their service can meet the security and audit trail requirements of regulated industries like financial services, even while enjoying the economies associated with cloud computing.

Sprott pays about 800 Canadian dollars per server per month (close to U.S. \$800) to replicate critical servers for e-mail, BlackBerry service, and file storage to Bell Canada’s version of the Geminare service. Sprott’s VP says the firm’s trading platform isn’t included because it’s currently outsourced, but he plans to bring it back in-house and add it to this backup plan. The data are transmitted over a virtual private network (VPN), an encrypted connection over the public Internet, where a pricier disaster recovery service might use a private telecommunications line. This is a continuous replication process, rather than a periodic backup, so the off-site copy of the data is never more than a fraction of a second behind.

In a live test for Sprott’s management, the VP was able to unplug a file server, then walk to his desk and manually trigger a failover to the remote copy. The VP got two calls after he turned it off within 60 seconds from users, but then one of the users told him it was back up while on the phone call—all within 30-45 seconds. Users had no idea they were now doing work in a data center 30 km away. Similarly, if the Sprott offices were to burn down, employees could access these applications from home ([Carr, 2010](#)).

University turns to cloud backup for data protection

Maryville University faced high costs and many troubles when it first tried to implement data backup to a remote site. The university enrolls about 3800 students at its 130-acre campus in Town and Country, MO, about 20 miles outside of St. Louis. Their initial attempt at backing up nearly 4 TB of data off-site was time consuming for the three people in the school's network services division staff, whose responsibilities also include managing the data centers, Internet access, infrastructure, and other tasks.

The school initially spent about 2 years trying to operate a remote backup location at Columbia College, located more than 110 miles west, but the 4-hour round-trip travel time for IT staff and the technology used going back and forth made the effort difficult. Initially, they had replaced their older IBM SAN with a newer NetApp SAN, and they took the old IBM equipment to the off-site location. But making a heterogeneous SAN connection between those two and getting a good backup was troublesome at best, including keeping the VPN connections running and getting the data transferred in a timely fashion. They tried to patch and bandage it all together, but it never worked the way they wanted, reliability was a problem and it took a lot of staff time to remediate ongoing issues. The school's new NetApp Fabric MetroCluster SAN spans both the administration building and the library on campus. In order to fix the issues they experienced replicating to the older IBM SAN at Columbia College, they would have had to replace the IBM SAN with another NetApp SAN in order to use the NetApp data protection tools for data synchronization for a remote solution. When they realized the cost was going to be in the area of \$125,000-\$175,000, in addition to yearly maintenance around 20-25% of the purchase price, that was the impetus for looking at alternatives to purchasing and managing their own hardware.

dinCloud came recommended to Maryville University from Los Angeles-based En Pointe Technologies, and Maryville ended up using dinCloud's "dinBackup" solution, which is aimed at "price-sensitive" customers and is meant to be used with a customer's existing on-site backup solution, plus includes disaster recovery and other services. dinCloud was very willing to sit down with Maryville IT staff and work out how data are going to be shared, how they would be encrypted, and who would be responsible for getting them from point A to point B. The company helped the school throughout the process. In order to perform due diligence with vendor selection, the University talked to a couple different vendors. However, they ended up choosing dinCloud because they said their people were very knowledgeable and very flexible in creating a solution that would work for them.

Once they signed the contract, the school had a rather tough time getting the VPN connection set up to dinCloud's site. They had about 500 Mbps of bandwidth spread out among three ISPs (Internet Service Providers), which was plenty for what they were trying to accomplish considering they were only backing up daily incremental changes to data once the initial replication had completed. dinCloud helped them work out a couple of issues between their ISP subnets and dinCloud's in order to correct the problem they first experienced, and dinCloud also helped Maryville IT staff configure their primary NetApp storage so that data at the primary site could be replicated to the dinCloud site using NetApp's SnapMirror and SnapShot data protection technologies.

Now that historical copies of data were being backed up to dinCloud's site successfully, the school began the process of preparing a full DR strategy with dinCloud. Maryville didn't have a need to keep weeks or months of archive data, but they did need a way of restoring data from the latest backup at the DR location should a disaster strike at their primary location on campus. So, Maryville began using dinCloud managed services to stand up backend infrastructure servers, like DNS (Domain Name System), in order to prestage necessary network services in the event a disaster struck and they needed to activate their DR plan to begin restoring systems and data. DNS, like directory servers, DHCP servers, etc., can be stood up in advance in an inactive state at a DR location so that recovery time is minimized when it comes time to begin restoring application servers and data.

With dinCloud as a partner, the school has been able to save thousands of dollars purchasing hardware and maintenance by transitioning to cloud backup and is investigating whether to use dinCloud services for disaster recovery, as well. By not purchasing and installing their own DR storage hardware, Maryville estimated it saved approximately \$40,000 per year on avoided maintenance costs in addition to staff labor on travel, managing the secure VPN, and managing the old IBM SAN hardware at the other university location. Based their cost analysis, the University claimed to be saving more than three-quarters of that total cost compared to the cost of dinCloud. Moreover, with dinCloud assisting with the VPN connection and data replication off-site to their location, the University claimed their new solution has since been reliable and worry-free ([Hilliard, 2013](#)).

SUMMARY

SMBs face a unique set of challenges when it comes to disaster preparedness. In order to create a disaster recovery plan for SMBs, it is important to understand how disaster preparedness is being accomplished at smaller organizations in light of the fact that disasters can strike anyone at any time. In this chapter, we discussed why risk assessment and impact analysis remain critical to SMB survival as a first step in preparing for BC/DR, we learned about relevant statistics on the current state of SMB disaster preparedness, and we demonstrated how SMBs across many different industries are using both traditional and newer cloud-based recovery strategies to enhance their DR effectiveness on a tight budget.

KEY CONCEPTS

Overview of SMB disaster recovery

- Performing a risk assessment and impact analysis, and deriving RTO and RPO DR requirements are just as important for SMBs to complete prior to developing or improving any IT recovery strategies.

- Regardless of the size of the organization, the cost of a recovery strategy should never exceed the losses it is designed to prevent.
- Existing contingencies, such as SaaS-based business applications under an SLA, may mean no recovery strategy is needed.
- Outsourcing disaster recovery, such as managed services or DRaaS, may be a viable option for SMBs that cannot afford the cost of developing their own strategy.
- Recovery strategies for on-premise IT applications will differ depending on anticipated financial losses and time to recover.

SMB disaster preparedness: Survey results

- A 2012 survey of over 2000 SMBs in 30 countries who employ between 5 and 250 employees found some important statistics.
 - Two-thirds of SMBs trust their ability to restore data from their backups.
 - One-third of SMBs said they were prepared for DR.
 - Nearly one-quarter of SMBs said they don't have a DR plan nor will they create one.
 - Over one-third of SMBs are using both mobile devices to access business information and taking advantage of server virtualization.
 - Approximately 40% of SMBs are using cloud technologies, both public and private.
 - Of those SMBs using server virtualization technologies, over one-third said the ability to quickly recover from a disaster had a significant effect on their decision and over 70% said it improved their recovery capability.
- Only 39% of businesses in the City of New Orleans reopened 10 months after Hurricane Katrina struck.

On-premise disaster recovery

- On-premise DR is typically the most expensive recovery option and more specific to stringent RTO and RPO requirements.
- Regardless of which recovery strategy you choose, common on-premise preventative (i.e., risk mitigation) measures are still wise, such as A/V, backup power, fault tolerant hardware for critical servers and workstations, Internet firewalls, and fire extinguishers.
- Local or remote backups alone are typically never an adequate DR solution.
- SMBs should examine if they're overspending on DR or low-value risk mitigations activities, such as with on-premise DR solutions that treat all IT applications the same regardless of RTO/RPO requirements, so that they can better utilize limited DR resources for their most critical business processes.
- Case studies demonstrate how SMBs are using on-premise DR for high availability.
 - High availability at 24 Seven Talent
 - Affigent fails over before the storm

Using a co-location data center for disaster recovery

- Co-location facilities allow space and power to be rented at an alternate DR site, for a company's own DR hardware and processes, and provide Internet and as well as other types of voice/data services.
- Co-location facilities may reduce time and costs for implementing recovery strategies through sharing of resources and benefits of scale.
- Before choosing a co-location facility, you should understand options such as level of redundant Internet/network connectivity, financial background, fixed and variable fees charged, location and type of backup power used, customer references, and security operations.
- Co-location facilities can cost anywhere from a couple thousand to tens of thousands of dollars per month, depending on space, power, and network/Internet redundancy requirements.
- A case study demonstrates how an SMB is using co-location facilities for recovery of critical IT applications as well as an alternate DR facility for their call center.
 - Balancing core competencies and cost with co-location data centers for DR

Disaster recovery in the cloud

- Cloud service providers provide their own network and server infrastructure, even software, for you to use under a subscription-based pricing model, i.e., you only pay for what you use.
- Cloud services vary depending on need and include IaaS, PaaS, SaaS, and even DRaaS.
- Usage-based cost of cloud services is well suited for DR where secondary infrastructure is parked and idle during normal operations.
- Other benefits of cloud DR include reduced time to deploy, less risk of oversubscription of resources compared to co-location, and lower costs when it comes to rehearsing your DR plan.
- Despite its benefits, two primary concerns of cloud DR remain: security and sufficient network bandwidth for restore operations.
- Options for cloud DR include (1) managed applications and managed DR, (2) back up to and restore from the cloud, (3) back up to and restore to the cloud, and (4) replication to VMs in the cloud.
- Cloud computing can improve protection of ROBO by improving availability and reducing the cost of additional IT manpower, servers, and data storage.
- Preparing a ROBO for cloud recovery involves several steps: (1) virtualizing and consolidating servers, (2) virtualizing and streamlining data storage and backup to disk, (3) virtualizing applications and desktops, and (4) deploying application acceleration and WAN optimization.
- A recent study suggests SMB cloud adoption the world's smallest companies using at least one paid cloud service will triple by 2015, 50% of SMBs believe

cloud computing will become more important to their operations, and only 20% of SMBs continue to believe data are less secure in the cloud.

- Several case studies demonstrate how SMBs have used specific cloud DR technologies and managed services to mitigate BC risks and improve their IT recovery strategies during recent natural disasters.
 - Snowmaggedon and Snowpocalypse
 - Amazon Web Services to the rescue
 - LAUSD implements snapshot-based cloud backup
 - Psomas moves DR to the cloud
 - Private cloud DR plans help BUMI
 - Sprott switches course to cloud DR service provider
 - University turns to cloud backup for data protection

References

- Brandon J. How to use the cloud as a disaster recovery strategy; 2011. <http://www.inc.com/guides/201106/how-to-use-the-cloud-as-a-disaster-recovery-strategy.html>, [Retrieved May 26, 2013], from Inc. Magazine.
- Carr DF. Preparing for the worst, on a budget; 2010. <http://www.forbes.com/2010/09/27/internet-microsoft-cisco-technology-disaster-recovery.html>, [Retrieved May 26, 2013], from Forbes.
- Edge Strategies. Edge strategies; 2012. <http://www.edgestrategies.com/component/k2/item/117-just-released-2012-microsoft-edge-technologies-smb-cloud-adoption-study.html>, [Retrieved May 27, 2013], from 2012 Microsoft/Edge Strategies SMB Cloud Adoption Survey.
- Hilliard J. Missouri University turns to cloud backup service for data protection; 2013. <http://searchdatabackup.techtarget.com/news/Missouri-university-turns-to-cloud-backup-service-for-data-protection>, [Retrieved May 26, 2013], from SearchDataBackup.
- Lam NS, Pace K, Campanelle R, LeSage J, Arenas H. Business return in New Orleans: decision making amid post-Katrina uncertainty; 2009. <http://www.plosone.org/article/info%3Adoi%2F10.1371%2Fjournal.pone.0006765>, [Retrieved May 27, 2013], from PLoS One.
- Lelii SR. Firms see public cloud storage as tape alternative in remote sites; 2011. <http://searchdatabackup.techtarget.com/news/2240106167/Firms-see-public-cloud-storage-as-tape-alternative-in-remote-sites>, [Retrieved May 26, 2013], from SearchDataBackup.
- Lynn S. Hurricane Sandy: lessons in disaster recovery; 2012. <http://www.pcmag.com/article2/0,2817,2411966,00.asp>, [Retrieved May 26, 2013], from PC Magazine.
- Pariseau B. Balancing core competencies and cost with colocation data centers for disaster recovery; 2010. <http://searchdisasterrecovery.techtarget.com/news/1507824/Balancing-core-competencies-and-cost-with-colocation-data-centers-for-disaster-recovery>, [Retrieved May 27, 2013], from SearchDisasterRecovery.
- Raffo D. Disaster recovery plans prove valuable in dealing with Hurricane Sandy; 2012. <http://searchdisasterrecovery.techtarget.com/news/2240172242/Disaster-recovery-plans-prove-valuable-in-dealing-with-Hurricane-Sandy>, [Retrieved May 27, 2013], from SearchDisasterRecovery.

Symantec, Inc. 2012 Disaster Preparedness Survey; 2012. <http://www.symantec.com/content/en/us/about/media/pdfs/b-smb-disaster-preparedness-report.en-us.pdf>, [Retrieved May 27, 2013], from Symantec.

YouSendIt. SMBs spend more for online cloud backup as IT budget expands; 2012. <http://www.yousendit.com/resource-center/2012/05/smbs-spend-more-for-online-backup-as-it-budgets-expand/>, [Retrieved May 26, 2013], from YouSendIt.

Training, Testing, and Auditing

9

IN THIS CHAPTER

- Training for emergency response, disaster recovery, and business continuity
- Testing your business continuity and disaster recovery plan
- Performing IT systems audits
- Summary
- Key concepts

INTRODUCTION

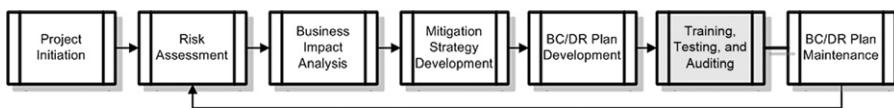
At this point, you have your business continuity/disaster recovery (BC/DR) plan pretty well defined and ready to go. The next step in the process, as shown in [Figure 9.1](#), is training, testing, and auditing. Training includes training staff on their roles and responsibilities related to the BC/DR plan as well as training them in the specific skills they'll need to carry out their roles effectively. Testing is the process of testing the plan, and there are various methods for doing so that we'll discuss in this chapter. Finally, there is the process of auditing the IT systems that form the foundation of most BC/DR plans.

There's an interrelationship between testing, training, and auditing as shown in [Figure 9.2](#). Performing one impacts the other two—when you test the plan, you're training and auditing to some extent.

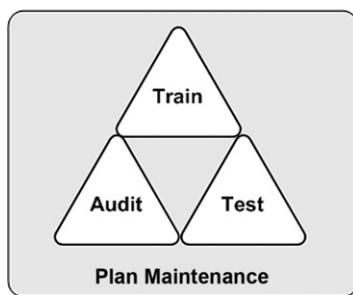
Training, testing, auditing, and plan maintenance are all bound together. Testing the plan trains staff and maintains the plan. Training staff tests and maintains the plan. As you train staff and test your plan, you will likely find areas that require modification. These modifications are made through the change management process defined as part of the plan maintenance phase. The information you glean from training and testing can be extremely useful in honing your plan in advance of a disruptive event. Testing and training go hand in hand, so let's begin by discussing training. We'll discuss plan maintenance in more depth in [Chapter 10](#).

TRAINING FOR DISASTER RECOVERY AND BUSINESS CONTINUITY

There are two distinct parts of disaster recovery and business continuity training. The first is the actual physical response to the disruption or emergency. That might involve evacuating a building if there's a fire, grabbing a fire extinguisher to douse

**FIGURE 9.1**

Business continuity and disaster recovery project progress.

**FIGURE 9.2**

Training, testing, and auditing activities.

a fire in the server room, or finding the water main if there's flooding inside the building. These actions all require some basic training, so responders know what to do and how to do it safely. There's little point in a responder grabbing a fire extinguisher and subsequently being burned by the fire because someone did not know how to properly use the equipment or extinguish a fire. That's one aspect of training. The second aspect of training has to do with ensuring that the various response teams know how to implement the BC/DR plan and that they have the skills needed to do so. For example, you might want to provide periodic training for your IT staff so they can stay up to date on the latest threats and security measures or training for alternate BC/DR staff on performing a system restore and verification routine.

Emergency response

Your BC/DR team should have an emergency response team (ERT) identified and these team members should be trained in appropriate emergency response activities. Each company should identify the likely emergency responses needed and provide training in these activities. If your firm is located in an area prone to flooding, earthquakes, hurricanes, or tornados, you should provide training in emergency response related to these events. In addition, basic first aid and CPR training should be part of all emergency responders' training, and some companies find it useful to provide this training to all employees.

The specialized skills for the ERT might include firefighting techniques or building evacuation procedures, for example. These specialized skills require training in

order to protect the safety of the responders and to enable the responders to be effective. As mentioned in [Chapter 8](#), your local fire or police department may provide this type of training or may be able to recommend firms that provide this type of training.

Your BC/DR plan should include the designation of an ERT as well as a list of required training/skills, certification requirements (if any), as well as periodic refresher courses. The ERT leader should be responsible for managing this. He or she should ensure team members have the training and/or certifications required and should arrange for the periodic testing and refreshing of these skills.

We discussed training needs for emergency responders in [Chapter 8](#), so we mentioned it here briefly, primarily as a reminder to you to address and include emergency training in your plan. Let's focus now on disaster recovery and business continuity training.

Disaster recovery and business continuity training overview

Disaster recovery is a crucial step that can mean the difference between the company's eventual recovery and failure. Training can help improve the chances for eventual success. Disaster recovery and business continuity training includes defining the scope and objectives for the training, performing a needs assessment (gap analysis), developing training, scheduling and delivering training, and monitoring/measuring training. In this section, we'll discuss disaster recovery and business continuity training as one since they are so closely related. However, as you develop your training plans, you may find it helpful to separate these two phases out so you can pinpoint distinct training needs. Remember, too, that you may choose to perform training while testing your plan. It depends largely on how you approach your testing. We'll discuss testing in detail later in this chapter, so you may revise your thinking on this once you've read through the entire chapter.

Training scope, objectives, timelines, and requirements

Ideally, you should develop a training project plan that ties in with the BC/DR project plan. The training plan should include a statement of scope (what *is* and *is not* included) as well as a list of high-level objectives. These objectives might be parsed out to include objectives for each of the implementer groups (emergency responders, crisis management team (CMT), damage assessment team, disaster recovery team, etc.). In addition, the timelines for training various teams should be developed. Keep in mind that some people may be members of more than one team, so training schedules and training subjects should take that into consideration. Then, develop requirements for training. One of the easiest ways to make sure training meets its stated objectives is to clearly define the objectives and then list the requirements to meet those objectives. For example, suppose you want to provide training for your computer incident response team (CIRT). For simplicity's sake, we'll use a very limited set of objectives, but it will give you a good idea of how to approach this section of the project. The data are organized in [Table 9.1](#) for your reference.

Table 9.1 Sample CIRT Training Outline

Topic	Details
Scope	Train all net admins on monitoring network traffic for security-related issues. Does not include training net admins on how to set up auditing or enabling log files for security monitoring.
Objectives	<ol style="list-style-type: none"> 1. Develop awareness of current security threats. 2. Develop understanding of log files to monitor. 3. Understand what to look for in log files. 4. Understand how to investigate suspicious log file entries, data, or trends. 5. Understand how to respond to suspicious network activity.
Timeline	Initial training will be developed and delivered within 30 days. Training is a 2-hour session. Refresher courses will be held quarterly for 30 minutes. Attendance by all net admins is required.
Requirements	<ol style="list-style-type: none"> 1. Locate latest threat data and trend information. 2. Location of (specified) log files. 3. Ability to read and understand log entries. 4. Ability to understand and spot trends. 5. Ability to take (specified) action to address suspicious or malicious network activity.

This example is simply to demonstrate that you should develop scope, an objective statement, a timeline, and a set of requirements for your training. It also shows you that you can do this relatively quickly and that it doesn't have to become a massive project itself. As you test your project plan, you'll also find areas that should be addressed by training, so you will likely need to revise these plans once or twice as you go through the training and testing phases.

Performing training needs assessment

The needs assessment phase is essentially a gap analysis. You should review current skill sets against required expertise to carry out various functions and determine what sort of training would best fill the gap. In many cases, training needs become evident during the testing of the plan. Later in this chapter, we'll discuss specific steps you can take to test your plan. As you test your plan, you'll see areas where specialized or updated skills and knowledge will be required to successfully execute the plan. You can make note of these potential skill gaps during your plan testing and circle back to include these in your training plans. Remember, a training needs assessment should be performed on the same periodic basis as your plan testing schedule or on some other periodic basis. People leave the company, are promoted, or change jobs. You need to ensure that at any given moment, your organization has the skills it needs to implement your BC/DR plan successfully. In many cases, a company's routine training plans will cover many (if not all) of the essential skills, but any skills that would not normally be covered through routine training should be flagged for special consideration.

TIP**Critical Cross-Training**

If you work in a small company, you may need to cross-train people to perform mission-critical functions if your BC/DR teams are not large enough to reduce the risk of small companies. Also, teams should be familiar with other teams' tasks, objectives, and requirements so that teams can cooperate in a seamless fashion in the chaotic aftermath of a serious disruption.

Developing training

Many companies have limited time or funds available for training, much less for BC/DR training. However, many studies support the thought that companies that train their employees benefit not only from improved productivity but greater loyalty as well. Targeted training to maintain or improve skills, especially those related to mission-critical business functions, can be accomplished relatively quickly and often at a reasonable cost. As with other risk factors in BC/DR planning, the risk of having untrained personnel can easily be mitigated through training, and it may also help drive productivity within the organization. (*Hint:* That's the business case you use to get your BC/DR-specific training budget approved.)

REAL WORLD**The ROI of Training**

Many companies have little time or money for training, especially if the company is under tight financial constraints. Many top-level managers look at the line items with an eye toward the bottom line, and training is one of the items that get slashed early in the budget-tightening process. However, experts agree that might not be the best long-term move.

"There is evidence that suggests that training can have productivity payoffs," says Robert D. Atkinson, vice president of the Progressive Policy Institute and director of the Technology & New Economy Project. "Training can have positive ROI (return on investment) because it can lead to productivity improvement" ([Atkinson and Castro, 2008](#)).

"There's also a lot of evidence that when companies introduce new technology the benefits of that technology are significantly enhanced if companies concurrently train their workers" ([Quast, 2012](#)).

Granted, training costs have to be aligned with organizational and financial constraints, but most companies can find creative ways to develop and deliver cost-effective training. The proliferation of online training courses along with local resources makes finding affordable training easier than ever.

When developing training, create clear, specific, measurable outcomes. A measurable outcome means that it either *was* or *was not* accomplished. Either Jill can restore the database from backups using the written procedures or she can't. Either Tony can safely shut power off to the manufacturing floor or he can't. Also keep in mind that not all training for your BC/DR plan will be extensive training. Some may be as simple as showing Tony where the power shut off is and how to perform a

power shutdown for the manufacturing floor. Other training, such as how to restore various IT systems that are closely integrated or interconnected, may require training in several knowledge areas as well as hands-on experience (ideally in a similarly configured lab environment) performing the activities in the requisite order. When appropriate, problems should be designed into the training so students can also learn how to troubleshoot and think creatively when things don't go according to plan.

Training should provide some sort of materials (printed, soft copy, Web based, etc.) that capture and reinforce the skills and knowledge presented. The training should also be designed to use several elements such as written, classroom lecture, hands-on (lab), and field (exercises). The more ways you use to deliver training, the more likely it is students will absorb it. Finally, use a final quiz or exam to ensure students have grasped the key concepts and can apply them appropriately. The final test or exam should reflect the training outcomes identified.

In the next section of this chapter, we'll talk about training staff on the BC/DR plan. The outcomes and other deliverables for BC/DR training should be developed as with any other type of training.

Scheduling and delivering training

Scheduling and delivering training is a secondary challenge after getting the training budget approved. These days, you can often find various training programs online that people can attend on their own schedule. If you use a flexible online learning system (either your own or an external one), be sure to set timelines and test for knowledge along the way. For example, if you decide that some of your network admins should attend an online course provided by a third-party training provider, you should develop some method of assessing whether or not the net admins learned what they should have. Some online courses are better than others, and some test knowledge better than others. Be sure to verify the quality of the training in advance and find ways to verify that students learned the required materials. If training is developed and delivered in-house in a classroom or lab setting, it may be a bit more difficult to manage. If you develop training that moves quickly, is interesting, engaging, and relevant to the students, it's much more likely you'll be able to get students to attend your training sessions. If necessary, you may need to call upon the organizational clout of your project sponsor to help you get the training scheduled and delivered in a reasonable timeframe.

TIP

Gaining Consensus on Training Timetables

Since some of the training will be specific to BC/DR, you may find people saying, in essence, "It can wait, there's no rush." You'll have to find creative ways to counter that, but one way that might work is to say, "If you knew that the building would burn to the ground next week, would you want this training to have already happened?" In most cases, the answer is yes. Since fires are the most common business disaster and can occur completely without warning, you might be able to gain consensus on a reasonable training timetable. If you can tie your BC/DR training into other business objectives, you may have an even greater chance of success.

Monitoring and measuring training

The first step in monitoring and measuring training is the development of clear objectives and outcomes for the training. If you don't know what should be accomplished in training, you won't be able to determine if the training was effective.

Exams and hands-on demonstrations of skills can be extremely effective in testing and verifying knowledge. For physical skills such as using a fire extinguisher or performing CPR, both a test of knowledge and a demonstration of skills are best. The same is true for some types of "logical" skills such as restoring a server or verifying user permissions. In some cases, the best you'll be able to do is verify that the training occurred and that several basic concepts were retained by students. An example of this might be restoring an enterprise resource planning (ERP) system that cannot be easily recreated in a lab setting.

Monitoring also involves ensuring key personnel have actually attended required training and have not somehow accidentally fallen through the cracks. If staff members leave or move into different positions, replacements need to be trained, so you need to develop some method of periodically checking your key BC/DR staff positions and ensure individuals are still in place and ready to perform their assigned BC/DR duties. These vary widely from one company to the next. You may be able to work with your HR group if they have an established system for tracking employee training and certification in place.

TRAINING AND TESTING FOR YOUR BUSINESS CONTINUITY AND DISASTER RECOVERY PLAN

There are four basic ways to train staff regarding the BC/DR plan, and these also simultaneously test the plan. These are paper walk-throughs (or tabletop exercises), functional exercises, field exercises, and full interruptions. Regardless of how you implement it, you need to cover specific elements in your training. Team leaders, in particular, need to know how and when to activate the plan as well as how to notify, assemble, and manage their teams. Specifically, they need to know how to:

- Use the plan effectively.
- Understand their individual and team roles and responsibilities.
- Notify, assemble, and manage their team members.
- Operate as a cross-functional team member.
- Communicate effectively across organizational boundaries in a stressful situation, often without the aid of common communication tools such as phones, e-mail, or other devices.

The most basic part of the training is understanding the plan and how to utilize it. That includes understanding how and when to activate it and how to implement the steps defined. If your BC/DR plan ends up being 50 pages long, you can be sure that no one will take time to read it if the building is on fire. The role of training is both

to familiarize people with the plan elements and processes and to reinforce the basic knowledge of the plan. In an ideal scenario, the plan document is accessible immediately upon notification of a disruptive event and someone starts managing the plan. However, in the real world, there's a small probability that things will progress in an ideal manner. Therefore, having a team well versed in the initial steps of the plan will provide an effective early response. Be sure that your training objectives reflect the specific knowledge you need students to gain such as how to use the plan, what the boundaries of their assigned roles are, and so on. Clear, specific, and measurable outcomes for BC/DR plan training are as important as for any other type of training.

Everyone involved with the BC/DR implementation needs to understand their specific roles and responsibilities once a plan is activated. Training should address both the BC/DR process itself as well as the specific skills needed by team members to be effective in their designated roles. For example, a database administrator may be part of the IT damage assessment team. She may be an outstanding DBA but may not have the specific skills to know how to approach the IT damage assessment process. She should be trained in the process of performing the IT damage assessment as well as in the overall BC/DR process. That way, she will understand how and when the IT damage assessment is performed, how it impacts other BC/DR activities, and how to perform the duties of that role. Another example is an administrative assistant who is also tasked with being the crisis team coordinator. He might have the skills to manage multiple tasks at once, communicate and update people effectively, and so on, but he needs to understand the specific roles and responsibilities of the coordinator role. If there are tasks within that role he doesn't understand or know how to do, appropriate training needs to be provided. He may not know, for example, how to use emergency communication equipment such as walkie talkies. A simple thing to learn, perhaps, but not something you want to take time to teach him in the midst of a serious emergency.

Team leaders head up their individual teams (be sure to assign alternates or backups for key roles) and they must also be able to work effectively as part of the ERT or CMT. That means there has to be a leader assigned or selected for the CMT. Without such a designation, it's likely there will be confusion or perhaps a bit of jockeying for position. Leaders like to lead. Leaders can be extremely effective members of a team if they are confident the team has a competent leader. Otherwise, they'll naturally try to step in to fill the gap. That's fine if only one person steps up, but it's a problem if four or five (or more) people step up. Therefore, understanding roles and responsibilities is a key part of the initial training.

Many companies will implement a CMT comprised of leaders of other teams. This structure means that departments that have little interaction during normal business operations may have to work closely together during an emergency. It may even mean that someone higher in the organizational hierarchy is reporting to someone lower in the hierarchy during the emergency. Think of this scenario. Perhaps you

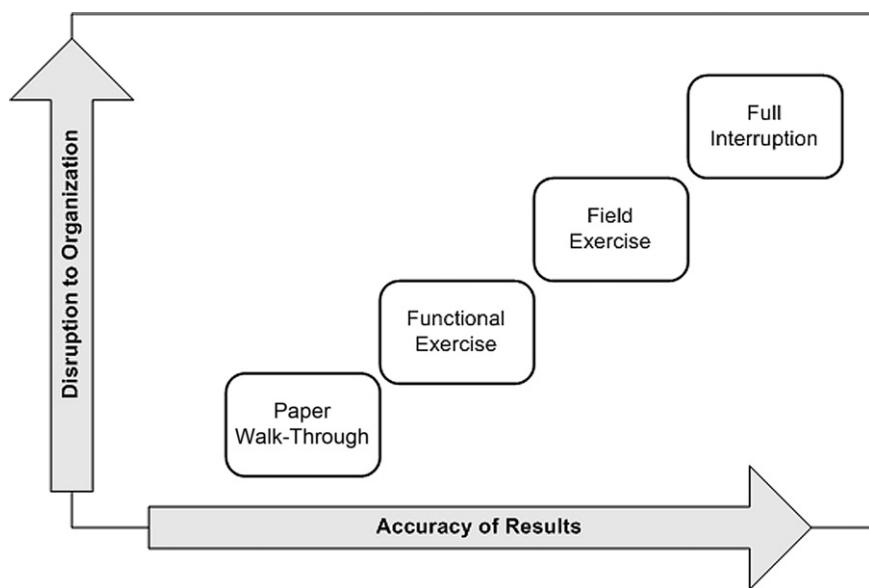
have an area director on your CMT because she understands operations. Suppose the person designated to head up the CMT is the Facilities manager because he has experience in CMT as well as in several related certifications. In the early stages of a disruptive event, the Facilities manager, as head of the CMT, is directing all activities, including those of the director of operations. This may be an appropriate situation but clearly, everyone has to be comfortable with this structure. The director has to be comfortable taking orders, temporarily, from the Facilities manager. There are numerous scenarios you can construct in which various levels of the organization have to work together seamlessly without anyone pulling rank inappropriately. Your training should address these cross-functional needs, define lines of authority and decision-making, and ensure that all team members are comfortable with the decision-making structure of the BC/DR process.

Finally, training should address the communication needs across the organization. As we've discussed previously, there are numerous communication needs throughout the life-cycle of a disaster and the team should understand this. The training should address the various communication groups (groups to whom the CMT should communicate), the appropriate frequency and content of the communication, and the appropriate distribution mechanism. Remember that during a disruption, your teams may not have access to standard communications equipment so communications plans and training should address various contingencies.

Now that we've looked at basic training elements, let's look at four commonly used methods of training, to which we referred earlier. These are the paper walk-through, the functional and field exercises, and full interruption. [Figure 9.3](#) depicts the relative accuracy and organizational disruption each type of test generates. The least disruptive type of test is the paper walk-through, and it's the one most organizations do. The results from a paper walk-through are obviously going to be less accurate than functional or field tests. However, paper walk-throughs, if done well, can still yield extremely helpful results that can be incorporated into the plan to incrementally improve it.

Paper walk-through

In most companies, if you can manage to schedule a paper walk-through of your BC/DR plan once a year, you've scored a major victory. As gloomy a prediction as that is, it reflects the reality in today's organizations. However, if you've managed to get approval to put together your BC/DR plan, you can make a pretty strong case that without a walk-through, you'll never know if it works or not. It's like carrying a spare tire that's flat—it's of absolutely no consequence until you need it. You want to know if your BC/DR plan will work if needed, and the only way to determine that is to test it out. A paper walk-through will take time to step through but it's time well spent. There are eight discrete steps you can take to run an effective paper walk-through. These steps also apply to the other types of training (functional, field, etc.).

**FIGURE 9.3**

Relative disruption and accuracy of BC/DR plan test methods.

Develop realistic scenarios

The first step is to develop realistic scenarios for your walk-through. You should develop scenarios based on those risks determined by your assessment to be the highest risk, highest likelihood, and highest impact. Although it may be interesting or fun to walk through some oddball scenario (space aliens land and their magnetic field erases only the zeros on all disk drives), it's not particularly useful. Focus on the things most likely to occur. Start with a fire in the building, since statistically speaking, that's the disaster most likely to strike businesses. Also create scenarios that involve your highest risk/impacts. Remember, you will likely need to perform several walk-throughs based on various threats. However, it is possible after you've run through several scenarios that your team is familiar enough with the process that future walk-throughs can use a single scenario that covers the all the bases. Ideally, you'll perform a paper walk-through for each of your major risks. Given the time and budget constraints most of you are facing, that's probably not realistic, but it at least can be held as the ideal.

Develop evaluation criteria

The key to any successful test of your plan, whether it's a paper walk-through or a full interruption, is to have criteria by which you'll evaluate the success of that training. We'll discuss test criteria in a bit more detail later in the chapter as well. For your paper walk-through, you might develop criteria that include:

- How well participants were able to follow and utilize the plan
- How well participants were able to communicate across team lines
- How well the checklists or defined steps worked to achieve the stated objectives
- How confident participants felt with their implementation of the plan
- How confident participants feel about implementing the plan in the future

Provide copies of the plan

Members of the CMT should be given the latest copies of the plan in advance of the walk-through. The hope (but usually not the reality) is that they'll look through the plan prior to the walk-through. However, the likelihood is they will not, so your training and testing need to work on the assumption that prior reading or familiarization will not occur (despite what people might claim). In addition, individual team members that might be participating, such as members of a damage assessment team or an ERT should be provided their section of the plan. If helpful, you may want to create a flowchart of your plan's processes in order to help individual team members visually see and understand how things should proceed. This often helps individuals understand their roles within the larger plan and operate more effectively as part of the larger team. [Figure 9.4](#) shows a portion of a sample flowchart. The adage, "A picture's worth a thousand words," is very true in this case. Checklists and simple flowcharts can be helpful in an emergency if staff is familiar with how they work and how to utilize them.

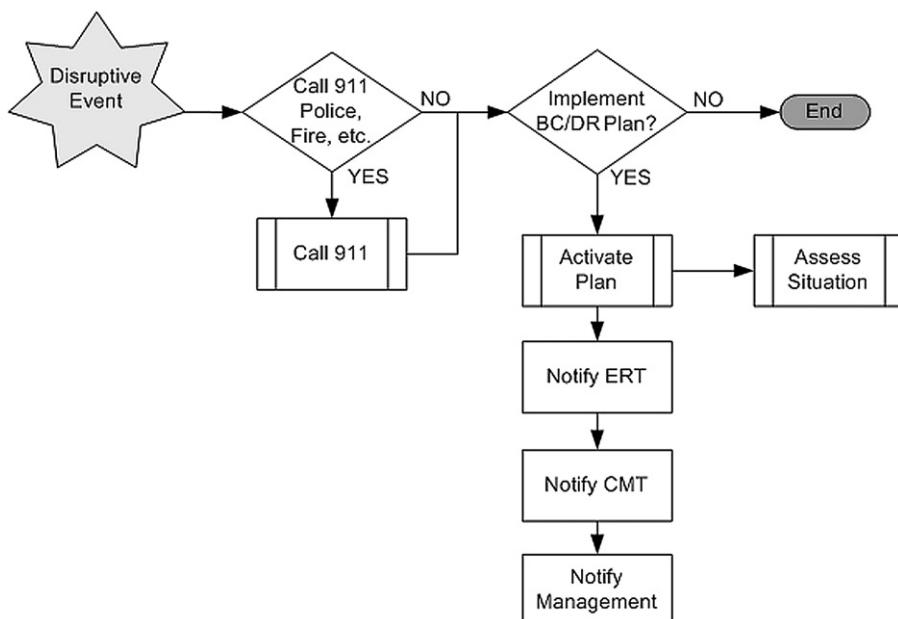


FIGURE 9.4

Sample flowchart of BC/DR plan (partial).

Divide participants by team

If your walk-through includes members of different teams, having them sit together can help the flow of the walk-through. If they need to confer or make notes among themselves, they can do so more effectively by being in close proximity to one another. It also helps reduce cross-talk and interruptions. Be sure to have alternates attend the training and work alongside their counterparts. If you have vendors you've designated as team members, they should also be included in the training.

Use checklists

If you have checklists for your key processes (such as those shown in the appendix materials), be sure to provide copies of these checklists and ensure the team uses these checklists. If they find steps that are out of order, missing, or redundant, they can correct the checklists quickly. Like flowcharts, using checklists will also help maintain direction and forward progress during the walk-through.

Take notes

Someone should be tasked with keeping notes about the overall flow, level of readiness, gaps in the plan, ambiguities, procedural errors, etc. If you run the walk-through with various teams, each team should be responsible for keeping notes on their process and their section of the plan as well.

Identify training needs

As you train staff in the use and implementation of the plan, you should specifically keep an eye open for additional training needs. Be sure to ask training participants to make a note of any skills they believe they need in order to effectively carry out the BC/DR plan. Those closest to the job are in the best position to identify skills gaps and you can develop a list of training needs from these run-throughs. Of course, you might end up with a long wish list, so you'll have to prioritize and sort through the training requests to determine what is high priority and what can wait (or is not needed).

Develop summary and lessons learned

After the walk-through, you should compile and summarize the notes collected. You should summarize the lessons learned from the exercise and schedule a follow-up meeting. This follow-up meeting should be held a day or two after the walk-through (i.e., not immediately following the walk-through, but not 4 weeks later) so that participants have a chance to think about the walk-through and bring their thoughts, suggestions, and feedback to the follow-up meeting. You can use the data collected from this process to modify future walk-through sessions and to modify the BC/DR plan as needed.

An annual walk-through of the plan is often used as a combination of plan familiarization, training, and testing. In some cases, that may be adequate, but this type of exercise is really the bare minimum. Also, be sure to flag your team members in some manner so that if someone leaves or is promoted, for example, you can either notify the alternate or designate and train a replacement. One of the biggest risks you face to

your plan is people not being familiar enough with it to implement it properly when needed. This happens for a variety of reasons and a regular training schedule can help reduce that risk.

Functional exercises

Functional exercises are used to actually test some of the plan's functionality. In most cases, if you want to test all the functionality, you'll plan field or full-scale interruptions, discussed in the next sections. However, it's often helpful and adequate to perform a paper walk-through along with functional exercises. Functional exercises train staff in critical procedures or functions needed to respond to and address the disruption.

Typically, functional exercises make use of scenario-based scripts and run for 2-3 hours. The team is divided into two groups. Alternates make an excellent second group for training purposes. A script starts off the sequence of events, which typically takes about 15-20 minutes. The ERT and CMT teams have to respond to the scripted events using their training and BC/DR plan. The second group, we'll call them the alternates here, act as nonteam members. For example, if the scenario includes evacuating the building, alternates may behave as employees might—panicking, not following instructions, and so on. If the scenario involves assessing injuries, alternates can have scripted injuries the ERT team has to deal with. The alternates use a menu of responses or events based on the specific scripted scenario to prompt the team members. The goal of this type of functional training is to get members to work as a team, to help members understand their roles and responsibilities, and to communicate effectively under stressful conditions.

TIP

Focus on Desired Outcome

If confusion crops up during the functional exercises, be sure to stop the exercise and clarify. Although it may break from the realistic scenario you've created, the primary purpose is training and testing the plan. If gaps or errors become obvious or there is massive confusion during the exercise, stop and address it immediately. It might mean spending a couple of minutes clarifying roles and expectations or making notes about areas of the plan that need modification. The few minutes you spend clarifying can make all the difference in the confidence and competence of staff if they are ever called upon to put their training to the test. The same holds true for field exercises, discussed later.

As with any other type of training, you should have clear objectives and outcomes identified for functional exercises. For example, if you're going to teach staff how to restore a database from the cloud pulled across the Internet from a remote data vault, you should list the key knowledge you expect staff to gain. This might include:

- How to determine that the database needs to be restored (i.e., is the local copy destroyed, corrupted, offline, etc.)

- How to access the data vault backups (location, login credentials, accessing data, etc.)
- How to restore the data (what order, what locations, what settings, etc.)
- How to verify the restore (verification of file names, sizes, locations; sample test scripts, etc.)

A functional test of the BC/DR plan follows the same path. If you want to test some of the functions of your plan, develop step-by-step instructions and have participants use those steps to test the function. As we've mentioned, testing the plan is a great training tool and functional exercises go a long way toward both ends.

Field exercises

Field exercises involve fairly realistic exercises based on likely scenarios. You've undoubtedly seen stories on these kinds of exercises on your local news stations. From time to time, local emergency responders exercise their skills by practicing scenarios. If you would like to practice your emergency and disaster recovery response using full-scale field exercises, you may be able to coordinate such exercises with your local emergency responders. They may welcome the opportunity to test their skills and to help train your staff in the process. If so, you have an excellent resource at your disposal that will not only test and hone your skills but provide valuable input into your disaster planning.

Most companies barely have the time or resources to do an annual paper walk-through of their plan, so it's not likely you'll be able to run through a real-world scenario. That said, if your company works in a dangerous industry (hazardous chemicals, explosives, power, etc.), you may want (or be required by law) to perform field exercises to assess and improve readiness. It's not until a situation is unfolding, even in a simulated manner, where some problems with a plan come to light. As useful as paper walk-throughs and functional exercises can be, they may still leave knowledge gaps or plan problems that you just won't know about until a real situation presents itself. Field exercises can reduce the risk of plan gaps but at a much greater expense of time and resources. For some companies, this investment makes sense.

Full interruption test

Like a field exercise, a full interruption test can be for the organization or just for specific systems within the organization. It activates all components of the plan and interrupts all mission-critical functions. The full interruption test will also activate the alternate work sites or facilities and off-site storage facilities, and the plan is actually implemented in whole. This type of full interruption test can be announced or unannounced. Clearly, an unannounced test simulates a real disruption or disaster more accurately than an announced test, but is also more disruptive.

Most companies are unlikely to be willing to disrupt their operations long enough to perform a full interruption test. However, there may be instances when a full

disruption of a single business unit (rather than the whole company) is an acceptable trade-off for the knowledge and readiness that can be achieved through this type of realistic simulation.

TIP**Documenting the Recovery Process**

Companies often have to perform actual recovery operations from isolated unplanned outages throughout the year, unrelated to larger disasters. In fact, many government regulations take this reality into account and allow required DR testing to be documented *after* recovery from an actual incident occurs. When an unplanned outage occurs, take the opportunity to hold a postmortem, shortly after recovery operations are complete when everyone can easily remember details, and document what occurred, what went well, and what didn't. Compare the actual recovery process to the applicable parts of your DR plan and use the postmortem as an opportunity to test, train, and update (if necessary) your BC/DR plan based on the actual events that occurred and the lessons learned. If you don't have the resources to schedule actual field exercises or full interruption tests, this is the next best thing.

Training plan implementers

If you have specific personnel designated as plan implementers, you may want to develop a specific training session for these staff members. They should understand exactly what their roles are and how to implement the plan, should it be necessary. Because the situation in the aftermath of a serious disruption or disaster is extremely stressful and chaotic, plan implementers should rehearse implementing the initial steps of the plan frequently enough that they're very comfortable with it. They should know by rote what to do, who to contact, and what steps they need to take in several likely scenarios. This memorization and practice of key first steps will help them if they are called upon to implement the plan. As we mentioned earlier, people fall back on their training in an emergency, so the plan implementers should be extremely comfortable with their responsibilities in this regard to prevent a total breakdown of the plan in the aftermath of a serious event.

TESTING THE BC/DR PLAN

There are numerous reasons for testing the plan. The obvious reason is to make sure that the plan will work in the event of a real disruption or disaster. However, the underlying reasons that testing helps the plan work more effectively is that testing serves these purposes:

- Checks for understanding of processes, procedures, and steps by those who must implement the plan
- Validates the integration of tasks across the various business units and management functions

- Confirms the steps developed for each phase of the plan's implementation
- Determines whether the right resources have been identified
- Familiarizes all involved parties with the overall process and flow of information
- Identifies gaps or weaknesses in the plan
- Determines cost and feasibility

As you read through the training section of this chapter, it probably became clear to you that training and testing a BC/DR plan are closely integrated. One way of training staff on the implementation of the BC/DR plan is to test the plan (and training will test the plan). If you choose to test your plan through BC/DR training, be sure to include the items listed here as objectives or deliverables for your training.

TIP**Test Off-Site Resources**

If you have designated an alternate site, off-site data storage, cloud storage, or backups, these should be tested for failover capabilities periodically. Don't wait for disaster to strike to test these important capabilities.

Understanding of processes

The processes, procedures, and steps taken by the various team members once the plan is activated (including how and when to activate the plan) should be the primary outcome of the testing phase. This phase should uncover any missing processes. It should also identify and verify processes and their interdependencies. Mission-critical functions should be restored first and the plan processes should address these priorities effectively.

In addition, the linear progression of the plan itself (first do this, then this) should be understood by participants. By walking through these processes, participants both learn the processes and can verify that they make sense. Often, a BC/DR plan is created by a specialized team of subject matter experts, but it's not until people are called upon to implement the plan (who may not be the same SMEs) that flaws are found. Any problems found with the plan through this phase should be noted and the change management process should be used to modify the plan appropriately. We'll discuss change management in [Chapter 10](#).

Understanding the processes also includes understanding the work-arounds and manual processes that should be implemented during BC/DR activities. If you've identified moving to manual systems or work-arounds if certain systems fail, these processes and procedures should be identified, tested, and verified. In addition, they should be looked at from the perspective of how manual processes might interact with automated systems. In some scenarios, you might have one or two key systems down and other systems still up and running. How will the manual and automated systems interact, how will manual processes be tracked and managed, how will work-arounds impact systems still running? These are the kinds of questions that

must be addressed when examining the processes of the BC/DR plan. All work-arounds, manual processes, and associate forms and paperwork should be included in this test phase.

Validation of task integration

Any walk-through or test of the plan should involve key personnel from mission-critical business functions as well as members of the BC/DR team. During the validation of task integration, these business subject matter experts will be best able to identify if the tasks are listed in the right order, with the right dependencies, with the right requirements, or resources, and such. The integration of tasks is often where plans fail in implementation due to the complexity of most businesses today. This is particularly true when looking at IT systems, which are at the heart of most recovery efforts. If tasks are not properly identified and sequenced, it can take hours, days, or weeks to uncover the source of the problem. The time and place to do this is in the plan testing phase, not during an emergency.

Confirm steps

In addition to testing the tasks and their integration, the testing should confirm each of the steps delineated in the plan. This confirms that all necessary steps are listed and in the correct order. It's often when you're walking through the plan step-by-step that you discover errors or omissions. If you're fortunate enough to have captured the correct data the first time around, this step will confirm that your plan is as complete as possible.

Confirm resources

At each step during the testing, you should ask and answer, "What resources are required to perform this step?" When you're thinking through scenarios, it's easier to identify needed resources. These might include people, skills, equipment, and supplies. It doesn't do much good to teach employees how to administer first aid if there are no first aid kits in the building. This step of the testing should look at needed resources for each step. For example, you need to be sure that the resources are not simultaneously required by two different teams or in two different places, just as you would in any other type of project resource management plan. If you do not have those resources at the time of the test, you should flag these steps as incomplete or in need of resources and create an action item to obtain these resources as soon as possible.

Familiarize with information flow

Communications are extremely important during a business disruption or disaster and are very difficult to maintain in those circumstances. This section of the test identifies who needs to know what and when. It identifies where information must flow

and how it will flow. It identifies information needs for the mission-critical business functions as well as for the ERT and the CMT groups. As staff become familiar with the flow of information through the BC/DR plan, they are more likely to have a heightened awareness of this flow during an actual event. Some communications will inevitably break down during a disaster, but the training you provide here by testing the information flow of the plan will help reduce the likelihood of a serious communication and information flow breakdown. In addition, the heightened awareness of information flow here helps build awareness of information flow through the organization on a normal day-to-day basis. This can help bridge communication gaps that currently are impacting operations and productivity.

The other type of information flow you need to address is the flow of data through IT systems and the organization. As you test your plan, you can identify how data flow through systems and determine whether your disaster recovery and business continuity plans addresses this appropriately. In large companies, there are numerous data and IT systems interdependencies that have to be identified. Testing your plan can help you look at data flow in light of BC/DR activities and make necessary adjustments.

Identify gaps or weaknesses

As you test the plan using checklists, paper walk-throughs, and simulations, the plan's gaps and weaknesses, if any, should become evident. It's usually not until we put something into a realistic scenario that we can see whether or not there are any problems. If you identify gaps or weaknesses, these can be addressed through modifications to the BC/DR plan. Omissions are often spotted as well—What *is* the number to call to replace your servers? Who is the contact person to report injured staff who can't report to work? Other details can be missed during the creation of the plan, such as where licensing information is stored or whether a particular backup will run on a new server or CPU type. The technology issues can be massive and overwhelming and though you probably can't test every scenario, you can test the most likely ones.

Determine cost and feasibility

It's difficult to completely understand potential costs of implementing the plan when you're creating it. You can create realistic scenarios and estimate potential costs, but as you test the plan, you're likely to understand more fully the potential costs for implementing, managing, and maintaining the plan. This information can be helpful in finalizing your plan or in revising your plan to meet your company's budgetary constraints. In addition, the overall feasibility of the plan will be tested. Again, it's relatively easy to think that someone could perform steps in a particular order or achieve certain milestones in a particular time frame when you're developing the plan. When people actually put parts of the plan to the test, it's likely that some aspects are simply impossible to implement or manage as expected. The feasibility of

the various steps, processes, and work-arounds is tested and can be revised to reflect the reality of the situation rather than the perfection of the situation on paper.

By testing the plan through training and through looking at these specific issues, you will have the best possible plan in place short of actually putting it to the test. Of course, the irony of the situation is that despite your best efforts on the BC/DR plan, you hope you never need to find out how good that plan is. Having trained and tested using the methods described in this chapter, along with any training and testing methods appropriate for the unique needs of your organization, you increase your odds of successfully pulling your company through a major (or minor) disruption or disaster. We all know that few things in life mirror the perfect world of planning. The following conversation with a seasoned BC/DR executive sheds light on the difficulties of implementing and managing BC/DR planning in the real world.

REAL WORLD

Overcoming Challenges with BC/DR Planning

Debbie Earnest, an experienced IT professional, has a background in manufacturing, infrastructure, and software. She managed a DR group for about 18 months, so she's been on the front lines of BC/DR planning. She's currently working for a major B2B software services company based in the United States. She was kind enough to take time out of her busy schedule to sit down and talk with us about her experience with business continuity and disaster recovery planning and implementation.

What Are the Significant Challenges in BC/DR Planning?

Many companies are in a bit of denial. Everyone says they need an ERP system with data flowing seamlessly through the company. That's great on paper, but how do you create that? Any hiccup upstream affects multiple systems downstream. The complexity of systems integration and interoperability is difficult in normal day-to-day operations, never mind in the midst of a crisis.

This complexity becomes a significant challenge in BC/DR planning that can quickly become overwhelming. When you begin looking just at mission-critical functions, there are so many interdependencies and so many points of failure that it becomes difficult to figure out where to start or how to cover them all. You can spend X dollars on disaster recovery planning and systems and you may still not be able to recover. That expenditure is then seen as a waste of money and, of course, that comes with its own set of problems. Even though your plan may not have addressed just one of a thousand failure points, if the one you missed is the one that comes into play, your plan may fail despite your best efforts.

BC/DR should really not be driven by IT, but in reality, it is. Companies cannot function without IT systems and IT staff is used to thinking about what could go wrong and how they should plan to avoid it. They are pretty good about risk management because they know that even a corrupt database can cause an outage for a period of time, or a fire in the UPS in the data center can cause a disruption. Many companies are so large or so complex, you just can't do business on paper anymore. Even trying to set up viable work-arounds or manual methods is next to impossible.

Another significant impediment to BC/DR planning is corporate mergers. It's difficult enough to develop a sound BC/DR plan for one company, but when you have the day-to-day IT tasks coupled with the tasks of integrating two disparate technology systems, BC/DR planning is almost impossible. There's no real clear solution to this problem other than to continue to build BC/DR systems into your plans as you move forward.

Perhaps the biggest problem is the budget. Unfortunately, when companies are looking for places to tighten their belts, they usually start cutting the BC/DR staff and activities. I worked

Continued

REAL WORLD—cont'd

for a company that was doing about \$1 B annually and when things got tight, they began eyeing the dedicated BC/DR jobs for elimination. Those people saw the writing on the wall and all eventually left the organization. This exemplifies the problem. Companies may think BC/DR is a great idea, but when it comes to including it in the budget and defending it at budget meetings, it doesn't happen.

What Advice Do You Have for Those Trying to Develop BC/DR Plans?

Companies must figure out what is absolutely critical. Business leaders often can't identify critical components—to them every system they work with is critical. Therefore, the best approach is to say, "OK, this system goes down. What happens on Day 1? What happens on Day 2? Day 3?" By asking them these kinds of scenario-based questions, you can discern the relative priorities of the various systems. In some cases, the best you can do is develop a BC/DR plan that addresses the top three business functions and even then, it still may not be adequate. Again, it goes back to the number of failure points that exist in the organization. In some companies, it's manageable. In large corporations, it's pretty much impossible to cover everything.

The goal, from my perspective, is to never get into a disaster situation—build in safety valves along the way. The first line of coverage is to build it into your systems. IT people are used to thinking about downtime and outages and have developed almost an instinct for providing the first line of DR defense—primarily stemming from the rigorous availability demands from companies today.

In BC/DR planning, you can try dividing it into two basic levels: Level 1 = data loss and Level 2 = building loss. Since IT staff is pretty good about figuring out how to avoid data loss, the Level 1 defense can be the best line of protection. If you have sound methods in place for avoiding data loss, you are reducing your risk significantly. Identify what the Level 1 systems are and how they provide protection.

You also have to look at alternate sites in advance, if that's going to be part of your Level 2 plan. To try to get an alternate site after a disaster will take you twice as long and cost twice as much, so planning in advance is definitely the preferred approach.

Finally, you have to test and practice the plan. In some companies I've worked in, we simply did a paper walk-through of the plan once per year and revised it accordingly. Although that may not be ideal, it's about as much as you can squeeze out of some organizations for BC/DR purposes.

From Your Perspective, What's the Bottom Line?

The real issue is time and money—there's never enough of either. There is no perfect BC/DR plan, but having one is better than not having one. You have to ask, based on your company, what is the bare minimum? At the very least, plan for that. Then set expectations so no one is looking for perfection, it just doesn't exist.

Test evaluation criteria

Before embarking on the testing phase, you should develop clear evaluation criteria for your tests. In many cases, the easiest way to create test criteria is to go through the various checklists or steps in your BC/DR plan and create corresponding questions. Let's look at an example involving the notification step in the activation of the plan.

1. Was the primary team member able to begin the notification process successfully?
2. How many team members were contacted?

3. How long did it take to notify team members?
4. Were there any missing or incorrect phone numbers?
5. How many team members were contacted via their primary methods vs. alternate methods?
6. How many team members were not on the notification list?
7. Were there any names on the notification list that should not have been?
8. Would this have worked if phone systems were out?

You can create a set of questions for each phase of the plan and use these to evaluate the test results. You can then measure the performance against the ability to complete each step, the thoroughness of each step, the effectiveness of each step, and the accuracy and validity of each step.

Recommendations

Based on test results, you should develop recommendations. These recommendations may result in modifications to the BC/DR plan, but they may result in modifications to other areas as well. For example, you might find areas in which staff needs additional training. You might find through these tests that there are areas of the business not included in the plan that should be or that there are operational changes that are recommended based on the test results. Recommendations for each team as well as for each phase of the plan should be developed. Be sure to include a process for incorporating recommendations so they are actually utilized and not overlooked.

PERFORMING IT SYSTEMS AND SECURITY AUDITS

By definition, an audit is the systematic examination against defined criteria. If your company is required to comply with laws or regulations, you have no doubt been through rigorous audits. The audits you perform to conform to these regulations may help in your BC/DR planning and may need to be included in your plan. For example, if you must comply with HIPAA (Health Insurance Portability and Accountability Act) standards, your BC/DR plans must address these issues and your audit of the plan has to include these parameters as well. Your audit should include both business continuity and systems audits.

IT SYSTEMS AND SECURITY AUDITS

Auditing IT systems involves a set of tasks that help reduce the risk of an intrusion or attack. Audits are concerned primarily with ensuring the company maintains data confidentiality, integrity, and availability, because these are the areas that typically come under attack. In some cases, this can disable a company's critical business functions; in more extreme cases, it disables the company's entire operations and

creates a significant legal or financial liability for the firm as well (see [Chapter 2](#) for more on the legal implications of data security).

An IT systems audit typically focuses on conducting a systematic evaluation of the security of various IT systems by measuring how well it conforms to established criteria or requirements. It includes an assessment or review of the network and systems' physical configuration and environment, the configuration of the software, the handling (storage, transport, access, etc.) of data, sensitive data in particular, and user access. Security audits are often performed in conjunction with compliance efforts, though even companies not subject to compliance regulations should undertake periodic IT audits.

Hardening systems is a risk mitigation strategy that is employed by virtually every company using IT systems today. Hardening systems, as you're probably aware, consists of taking actions to minimize the attack footprint of a system or network. This includes actions such as removing network protocols not in use, disabling ports or services not being used, removing unused user accounts, reducing permissions to the least possible, and automating the updating of antivirus and antispyware data files, to name just a few examples.

With respect to BC/DR planning, systems auditing should include several key elements. These include:

- Ensuring IT risk mitigation strategies are in place and properly implemented/configured.
- Ensuring systems identified by the BC/DR plan are still in place and functioning.
- Identifying areas where new technology has been implemented and may not be incorporated into the BC/DR plan.
- Identifying areas where technology has been retired or modified, resulting in the need to revise the BC/DR plan.
- Reviewing the processes identified in the BC/DR plan with respect to IT systems to ensure the steps and processes are still correct, complete, and relevant.
- Verifying that the IT incident response team (CIRT, CERT, or whatever term you use) is intact and has a clear understanding of roles, responsibilities, and how to implement the IT-specific segments of the BC/DR plan.
- Reviewing data regarding various systems to ensure they are still compliant with the BC/DR plans. These systems include operating systems, networking and telecommunications equipment, database and applications, systems backups, security controls, integration, and testing. Any of these areas is subject to frequent change. An audit can help assure the BC/DR plan will still work if implemented.

This is not an exhaustive list, but it provides examples of what types of data an IT audit within the scope of a BC/DR plan might include. The key is to identify how IT systems have changed (or remained the same) and assess how and where that impacts the BC/DR plan. Most IT systems are not static and even gradual changes over time can end up creating a significant change to the way a BC/DR plan must be implemented. Referring to the interview with IT professional Debbie Earnest earlier in the chapter, you can see that with the complexity of systems, the proliferation

of corporate mergers and acquisitions, and the ever-changing technological landscape, your best bet for keeping your BC/DR plan up to date will be through the IT audit process. Periodic auditing is an excellent operational practice for IT and it doesn't take much more effort to include a check of key elements from the BC/DR plan during these audits. We'll discuss maintaining the BC/DR plan in more detail in [Chapter 10](#), but keep in mind that IT audits are the easiest way to maintain the BC/DR plan from an IT perspective primarily because they involve a periodic review that is likely already part of your standard operating procedures. Adding a few extra steps to your audit plan is easier than trying to perform a fully separate BC/DR audit every quarter or every year. It's also easier to address gradual changes as they occur than to try to assess how much change has occurred since the prior year's review of the plan.

SUMMARY

Training and testing your BC/DR plan are tightly integrated activities. Training staff for the specific roles, responsibilities, and actions they take during the implementation of the BC/DR plan also tests the plan. On the flip side, testing the plan trains staff in the implementation and management of the plan. Therefore, these two activities should be viewed as a whole and plans for training and testing should be complementary rather than redundant.

Training activities should be defined for emergency responders. These skills often are taught by community organizations such as the local fire department or other local organizations. Skills include building evacuation, firefighting, and first aid. Training should include safety procedures as well as instruction on the use of specialized equipment. These skills should be reviewed and refreshed periodically through exercise, drills, and simulations, if possible.

Training for business continuity and disaster recovery is a slightly more difficult undertaking. Training can take any of several forms and the training activities are also plan testing activities, so there's a great deal of overlap. Training for BC/DR should include training team members on their specific roles and responsibilities during the implementation of the BC/DR plan. It should also include training on specific skills needed to effectively implement and manage the plan. Cross-functional teamwork and communications should also be part of the BC/DR training.

In order for the training to be effective, you should develop clear, specific, and measurable outcomes for your training. This should include scope of training, requirements for training, and learning outcomes expected. You may need to perform a training needs assessment before developing the training requirements. As you test the plan, you'll also identify areas that may require additional staff training, and these can be added to your training requirements. Developing the training can be done in conjunction with developing the testing plan for your BC/DR plan in order to achieve

some efficiency in your efforts. Finding time to schedule and deliver training is a challenge in most organizations, so if you can find a way to tie these efforts or outcomes into larger business objectives, you might have greater success. The results of training activities should be monitored and measured to ensure the training achieved its objectives and that revisions to the training based on input and feedback can be incorporated in the next iteration.

Testing the plan helps train team members on the use of the plan, on their specific roles and responsibilities, and on communicating across the organization. Testing the plan will also help you identify processes, procedures, steps, or checklists that are incorrect, have gaps, or require revision for some reason.

There are four primary ways plans are trained and tested, though there are an infinite number of variations. A paper walk-through is the easiest and least disruptive way to test your plan, but it yields the least accurate results as compared to other methods. However, because it is least disruptive, it *is* the easiest for most organizations to implement and the results can help improve the quality of the BC/DR plan significantly. Functional exercises test subsections of the plan and the functionality of various components. An example of a functional exercise is having IT test the steps in the BC/DR plan related to restoring a server from remote backups. These types of tests can help uncover problems that would otherwise go unnoticed, but they take more time and resources to perform than paper tests. Field exercises and full interruptions certainly provide the most realistic simulations, but most companies will be reluctant to plan and pay for this type of training. In some types of industries, this type of exercise is a requirement either for health and safety reasons or due to legal or regulatory requirements. Regardless of which type of training and testing you undertake, you should pay special attention to the skills and training needs of the plan implementers. They should be well versed in how to activate and implement the plan so that they can do so relatively easily if a disruption or disaster occurs.

Testing the plan checks for understanding of the processes, procedures, and steps defined. It validates the integration and dependencies of tasks across various business and functional units. It also helps determine if the right resources have been identified for the various steps. Ultimately, it familiarizes the implementers with the entire process and uncovers potential gaps, errors, or omissions. Finally, the cost and feasibility of implementing a plan can be better assessed through testing.

IT systems and security audits are typically part of company's standard IT operating procedures and they may be required by law or regulation (HIPAA, etc.). In addition, BC/DR-specific IT audit tasks can be included in standard auditing procedures to reduce the amount of additional work that might be required to test the BC/DR plan. Some of the elements you might choose to audit in this manner include ensuring the IT risk mitigation strategies have been implemented per the BC/DR plan, ensuring the processes and procedures for IT work-arounds are feasible and meet requirements and identifying changes to technology that impact (or are impacted by) the BC/DR plan.

KEY CONCEPTS

Training for emergency response, disaster recovery, and business continuity

- Training, testing, and auditing are tightly integrated activities used to validate the BC/DR plan.
- Emergency responders should be trained on the specific skills needed to respond to emergencies. This includes safety procedures and the use of specialized equipment.
- Disaster recovery and business continuity plan training should begin with a definition of the scope, objectives, and requirements for the training.
- A needs assessment should be performed and results from plan testing should also be used to identify training needs.
- Training should be monitored and results should be analyzed so any changes to future training or to the BC/DR plan itself can be made through the change management process.
- Training also includes how to activate, implement, and utilize the BC/DR plan effectively. It should help team members understand their specific roles and responsibilities within the constraints of the plan. It should help them with cross-functional teamwork and communications as well.
- There are number ways to train and test a plan. The four most common methods are paper walk-through, functional exercise, field exercise, and full interruption. These methods train participants while simultaneously testing the plan.

Testing your business continuity and disaster recovery plan

- Testing a BC/DR plan often is done in conjunction with training exercises such as the paper walk-through, functional or field exercises, or a full interruption. Testing helps uncover areas of the plan that require revision.
- The plan test should assess the processes defined to determine if they will work as specified and if they are feasible.
- The test helps identify task integration and dependencies to determine if there are gaps, errors, or omissions in the steps identified in the plan.
- Testing helps train participants in the information flow that is required throughout each step or phase of the BC/DR plan.
- A good BC/DR test plan should have well-defined scope, requirements, outcomes, or objectives.
- One of the objectives of plan testing should be an assessment of the cost and feasibility of the overall plan. Any weaknesses in this area will require a revision to the plan to better align with the constraints of the organization.
- BC/DR planning is a difficult task that may not cover every single point of failure. Level 1 plans address data loss and from an IT perspective, these are the easiest to address.
- Don't aim for perfection; try to cover the basic needs of your mission-critical functions.

Performing IT systems audits

- IT audits are performed as part of most company's standard IT operating procedures and may be required by law or regulation.
- IT systems audits focus on conducting a systematic evaluation of various IT systems and this information can be incorporated into the BC/DR plan.
- Changes to IT technologies should be incorporated into the BC/DR plan.
- Auditing with an eye toward BC/DR requirements can be incorporated into standard operating procedures to reduce the impact of BC/DR work on the IT department.

References

- Atkinson R, Castro D. Digital quality of life; 2008. Retrieved May 25; 2013, from The Information Technology and Innovation Foundation: <http://www.itif.org/files/DQOL.pdf>.
- Quast L. Want your company to succeed in the future? Invest in employee skills training like Deloitte LLP; 2012. Retrieved May 25; 2013, from Forbes.com: <http://www.forbes.com/sites/lisaquast/2012/05/14/want-your-company-to-succeed-in-the-future-invest-in-employee-skills-training-like-deloitte-llp/>.

BC/DR Plan Maintenance 10

IN THIS CHAPTER

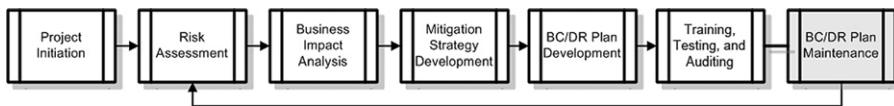
- BC/DR change management
- Strategies for managing change
- BC/DR plan audit
- Plan maintenance activities
- Project close out
- Summary
- Key concepts

INTRODUCTION

Maintaining the plan you've developed may end up being the biggest challenge you face in the entire business continuity and disaster recovery plan process. If you found lack of enthusiasm or outright resistance to the BC/DR process, you may find that support for maintaining the plan simply vanishes. Many people assume that once the project is complete, they can simply chalk up another successful project and move on, but that's far from true. Maintaining the plan is essential to continued readiness.

However, there is some good news amidst this gloomy outlook. First, you actually *have* a plan to maintain. People within the organization have participated in evaluating the business, developing mitigation strategies, and perhaps even testing the plan. They're familiar with the components of the plan and may have some sense of ownership for the continued readiness of the organization. The other good news is that, as we've discussed throughout this book, there are many areas in which you can incorporate BC/DR strategies and activities in your standard operating procedures. For example, many of the IT strategies implemented to provide continuous (or very high) availability are strategies that are also BC/DR risk mitigation strategies. We've pointed out that it's extremely helpful to incorporate BC/DR strategies in your operational plans whenever possible to reduce the outright resistance you may face to BC/DR planning. This may be the one most critical point in maintaining your plan: operationalize everything you can.

In this chapter, we'll discuss various considerations for maintaining your BC/DR plan, especially in the face of indifference or resistance. As you can see from [Figure 10.1](#), we're in the last phase of our BC/DR planning project.

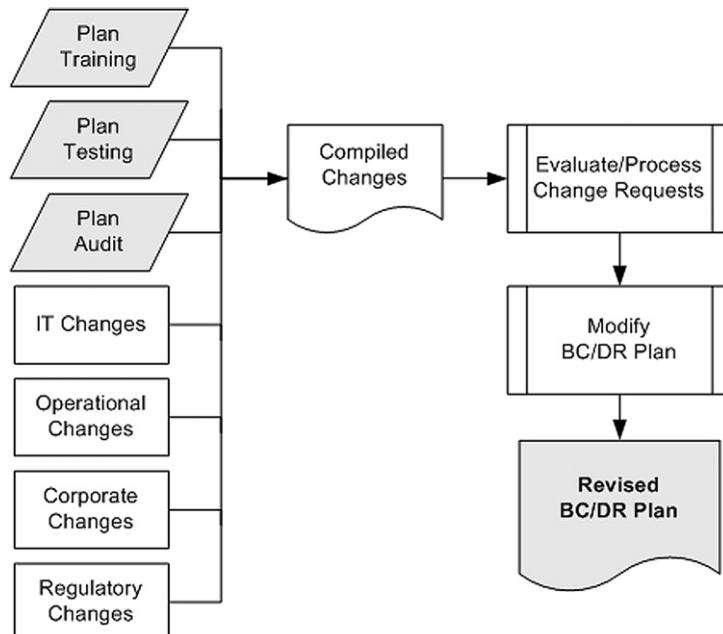
**FIGURE 10.1**

Last phase of BC/DR planning.

BC/DR PLAN CHANGE MANAGEMENT

Change is constant in organizations—change in operations, change in technology, change in personnel, change in regulations—the list goes on. You might be wondering how you can possibly reflect these changes in your BC/DR plan without having a full-time dedicated BC/DR team. It is challenging, but there are a few strategies you can use to reduce the complexity and enormity of the task. Change management has several discrete steps, as depicted in [Figure 10.2](#).

As you can see, the first step is to monitor changes. There are numerous sources of change that we'll discuss shortly. The next step is to decide how the changes impact your BC/DR plan. Not all changes have an impact on your plan, but you need to assess change before you can make that determination. If a change impacts your

**FIGURE 10.2**

Change management steps.

plan, the next step is to determine how to address the change in your plan. This typically involves cycling back and performing a modified version of your risk assessment, business impact analysis, and mitigation strategy development. This iterative process can be accomplished relatively quickly in many cases, but your assessments will have to specifically look at the suggested change and the impact on the entire plan.

We've discussed plan training, testing, and auditing in [Chapter 9](#), so let's continue now by looking at how these inject change into the BC/DR plan and then we'll examine other sources of change that impact a BC/DR plan. You'll find a checklist for change management tasks in [Appendix G](#), as well.

Training, testing, and auditing

In [Chapter 9](#), we discussed the activities related to developing, delivering, and evaluating training. You learned that training often involves testing the plan, and that testing the plan trains staff on how to implement the plan and carry out the tasks assigned. Changes will naturally come out of these processes, and that's part of the purpose of training and testing. It's difficult, if not impossible, to develop a perfect plan the first time through. It's not until you try putting the plan to work that you discover steps out of order, errors, omissions, or redundancies. As you deliver your training and perform your testing, you should capture a list of changes that need to be made to the BC/DR plan. These changes should be submitted for review. Not all requested changes should be made for a variety of reasons. We'll discuss the change review process in the section entitled "[Strategies for managing change](#)" later in this chapter.

Changes in information technologies

The IT audit discussed in [Chapter 9](#) is one of the ways you can keep track of changes to IT, but clearly this area is the one most subject to change and risk. You and your IT team are more than likely extremely familiar with reviewing and assessing change—from the location and duties of various servers to the implementation of new applications to the reorganization of existing infrastructure. As you know, even the most innocuous changes can suddenly inject all kinds of problems into your network and systems. As you continue to manage your day-to-day IT operations, you should consider including an additional step in some of your processes that remind you to assess the process against BC/DR. For example, you likely have a process for evaluating the implementation of new technology. Consider adding one step in the process that says, "Assess impact of this new technology on BC/DR plans." It is a deceptively simple step, and admittedly, it can open up a whole set of problems or questions you'd like to avoid. The flip side is that if two or more technologies are being considered, there may be one that contributes to BC/DR more than the others. In that case, you might be able to build in additional BC/DR capabilities with little effort.

As systems are upgraded, swapped out, modified, or retired, be sure to include a line item task to consider the impact on BC/DR plans. In some cases, this will be simply an item to be checked off. In other cases, you might discover that changing a system will have a large impact on your BC/DR plans. In those cases, you'll have to balance the potential change (for better or worse) against other alternatives. Regardless of your final decision, be sure to flag these changes so the BC/DR plan can be updated as a result.

CRITICAL CONCEPT

Incorporating BC/DR Plan Review into IT Changes

IT systems are at the heart of most BC/DR plans. As a result, changes to IT systems often have the biggest impact on the BC/DR plan. For most organizations, the easiest way to make sure IT changes are reflected in the BC/DR plan is to keep a list of IT changes and a brief assessment of the impact on the BC/DR plan. As the periodic review or audit of the BC/DR plan occurs, this list of IT changes can be incorporated. It might be as simple as keeping the list of changes in a spreadsheet or document in the same folder as the BC/DR plan. Since IT changes so frequently, the first questions to be asked should be, "How will this change enhance or degrade our ability to recover from a significant outage?" If the change will enhance it, you're set (though you still need to take an integrated or holistic look at the change and how it impacts other parts of the organization and the BC/DR plan). If the change will degrade your ability to recover from a significant outage, you need to assess whether this is a wise move or whether there are other options available that will meet your needs and be neutral or positive as it applies to BC/DR.

One of the easiest ways to incorporate BC/DR change management into your organizational processes is to add a line item to your change request. Assuming you use a change management system of some sort, add a line that asks "What is the impact to BC/DR infrastructure, architecture, or plans?" That way, each time a change request is submitted, the submitter and the approver must think through how it impacts BC/DR. If there is an impact, that change request can be flagged and added to a periodic review of the BC/DR plan. This way, no changes are ever made without at least giving some thought to the impact on BC/DR plans. While not foolproof, it goes a long way toward helping to keep your plan current.

Changes in operations

During your risk assessment, you determined the mission-critical business functions that needed to be addressed in your BC/DR plan. Clearly, operations are not static, and changes over time to operations may impact the BC/DR plan. Reorganization, expansion, new departments, new facilities, and new management structures can all impact operations in a variety of ways. In some cases, changes in operation happen slowly over time and these changes may go unnoticed as it relates to the BC/DR plan. The BC/DR plan audit (discussed later in this chapter) can be an effective method of reviewing operations against the BC/DR plan. If the business's mission-critical operations have changed over time or if the processes used to accomplish these functions have changed, the BC/DR plan is at significant risk of failure and should be revised. For example, if your company has slowly moved from bricks-and-mortar retail to e-commerce, many key processes may have changed. If the mix has shifted slowly over time, you might not notice it until you test the plan or perform a BC/DR audit. If you have been expanding storage or adding new lines of applications, servers, or

business, these slow-but-steady changes can sometimes be incorporated without thought to bigger picture items like BC/DR readiness. Obviously, the key is to be sure your BC/DR plan addresses your mission-critical business functions and if those shift over time, your plan needs to be updated. Changes to operational processes should be implemented as needed, but it would help if your operations staff understood that any changes to their key processes should be flagged so the BC/DR team can review the impact of those changes on the plan and revise as needed.

Corporate changes

Corporate mergers, acquisitions, spin-offs, restructuring, and other types of corporate changes can have a major impact on the BC/DR plan. As these changes are considered and discussed, the BC/DR team should assess the potential impact to the plan. Of course, in many cases, these activities are not publicly announced until the deal is sealed, so your team may be caught off guard. These kinds of changes are among the most challenging to deal with from a BC/DR perspective. IT staff will have a big enough challenge figuring out how to incorporate the required IT changes for daily operations much less trying to figure out how all this impacts BC/DR activities. The best you can do most of the time is to continually look to incorporate BC/DR activities into your normal operations and planning activities and to continually look to protecting *data* first. If you know with certainty that your critical data are safe, putting systems in place to access and utilize that data can be secondary during times of turbulent or unexpected change. Sometimes, the BC/DR elements can be addressed through standard IT planning processes with an additional line item task. Assessing how the plans impact BC/DR may help the team choose from among several viable alternatives or it might point out a path that optimizes immediate BC/DR capabilities.

CRITICAL CONCEPT

IT Project Planning: Keeping Your BC/DR Plan Current

In addition to integrating BC/DR plan maintenance into your operational change control processes, you should also add the following two tasks to all new IT project plans:

1. Planning phase: assess scope of change to BC/DR plan and develop BC/DR change request, if applicable.
2. Release or close-out phase: update BC/DR plan documentation, if applicable, after change request is approved and before release to production.

How will the new IT application or service impact your risk assessment and impact analysis? If introducing a new or substantial change in technology, will risk mitigation activities need to change? Will recovery procedures need to be retired, created, or updated? Will vendor contact lists and callout trees need to be retired, created, or updated? Will service level definitions need to be updated with the new application or service? These are all questions you should answer during your project planning phase. In addition, work estimates, cost and schedule to complete BC/DR plan assessment, and updates should be factored into your project plan. This way, you minimize the number of updates you have to make during periodic review of your BC/DR plan and your plan remains current based on projects coming out of the pipeline.

Legal, regulatory, or compliance changes

Changes to the legal, regulatory, or compliance landscape will certainly trigger required changes to your BC/DR plan. For example, if laws change regarding data security, you will have to review your BC/DR plan to determine whether your existing plan meets these new requirements or whether you'll need to implement additional tools, technologies, or processes. As with other changes, it's sometimes as simple as looking at the current BC/DR plan and determining that no change is needed. Other times, a major change may require you to cycle through all phases of the BC/DR project planning stages and create a plan for implementing required changes. In most cases, changes in this arena will impact operations or IT, and the impact to the BC/DR plan will be addressed through those channels.

Strategies for managing change

Two key strategies for managing change are having a process for monitoring and a process for evaluating change requests. It's usually easier to monitor change and respond to it as needed over time rather than sitting down once a year and trying to remember (or determine) what's changed since your last review of the plan. The easiest way to monitor change throughout the organization, as it relates to BC/DR plans, is to include an additional step or two in standard operating procedures. These steps can be as simple as "Determine impact, if any, on BC/DR plan. If impact exists, submit BC/DR change request to [insert position responsible for managing BC/DR change requests]."

REAL WORLD

Removing Roadblocks

Most IT professionals are accustomed to dealing with change requests. In the BC/DR process, there are really two separate and distinct activities: change notifications and change requests. Change notifications are those changes that are being made, regardless of impact to the BC/DR plan. These include changes to the organization, personnel, operations, or the larger regulatory environment. These changes need to be addressed by the BC/DR plan. Change requests are elements that trigger changes to the BC/DR plan. In some cases, a change notification triggers a change request. Other times, a change notification does not trigger a change request. You may choose to take these two functions out and ask your operations staff to incorporate a change notification process. In this way, they can notify the BC/DR team of change. The BC/DR team can then evaluate that change and generate a change request for the BC/DR plan, if appropriate. The rationale behind dividing this process in two in this manner is that operations staff might resist the use of a "change request" because, from their perspective, the change is not being requested, it is being implemented. Therefore, the use of the term change notification may help reduce resistance within the organization to the process of keeping the BC/DR team up to date. A simple change in terminology may significantly reduce resistance to the process of keeping your team up to speed on organizational changes that may impact the BC/DR plan.

Monitor change

Implementing processes for monitoring change can make your job of maintaining the BC/DR plan much easier. Develop processes that can be incorporated into everyday workflows so that as changes occur, they can quickly be assessed for their potential impact on the BC/DR plan. If the change has no impact, it can be ignored (from a BC/DR perspective). If the change will have an impact, a change request should be submitted to the BC/DR team. (*Note:* We'll use the term *change request* to keep it simple, but it will refer to either a change request or notification.) Remember, a change request may be just a matter of noting that the leader of the Emergency Response Team has changed. This change request should trigger the appropriate revision to the BC/DR plan including contact names, phone numbers, and team rosters. The same is true of other types of changes. If the IT group is implementing a new application or standing up a new server technology, there may be a change request generated to note the new technical specs of the application or server in the event of an outage, or it may trigger a quick review of the specs for servers at the alternate computing site to ensure the alternate site still meets BC/DR needs.

People

People leave organizations, get promoted, or move into different jobs. A periodic review of changes to the organization can help you determine if there have been personnel changes that impact your plan. This can be part of the BC/DR plan audit, discussed later in this chapter.

Process

Changes to processes should be monitored as well. Subject matter experts or members of the BC/DR team can be tasked with monitoring changes to key processes and flagging changes for BC/DR review. Many corporate processes remain fairly unchanged over time; however, some companies that are in high growth mode or that are streamlining operations, for example, might have significant changes to their daily operations. Changes to mission-critical functions should be reviewed with the highest priority since these changes could potentially cause the BC/DR plan to fail if implemented without these changes.

Technology

Changes to IT have been discussed, but some technology may fall outside the scope of IT management. If your company works with scientific equipment, manufacturing equipment, medical equipment, or other specialized technology, changes in this arena should be monitored and assessed to determine whether the BC/DR plan requires modification. Often changes in technology create changes in processes, so the trigger for review and modification may come from either area. However, a process for triggering a review should be included in your technology implementation plans to make BC/DR plan maintenance as low as possible.

REAL WORLD**Integration and Complexity**

In healthcare IT, there are many systems that are interconnected to provide patient care. The Electronic Medical Record (EMR) is typically the “parent” system with many “child” systems feeding or being fed from it. Billing and hospital revenue is one feeder system. Medical imaging is another feeder system. These interconnections make BC/DR plan maintenance challenging. For example, a surgical team purchases a new device that creates diagnostic images. Those images now need to be integrated into the EMR. They are stored on vendor-supplied storage racked in your data center and managed remotely by the vendor. How does this impact your BC/DR plan? Clearly, these are the kinds of continuous changes BC/DR teams must monitor. In this case, the first task is to ensure the safety of the data, so creating an off-site backup schedule would be a top priority. Next, determining how that data are integrated into your systems and how you would recover from that backup should something take your data center offline. This is an example of how you’ll need to think through steps to keep your BC/DR plan current while dealing with constant change. Tip: Always keep your data safe first and then determine next steps.

Evaluate and incorporate change

The change review process should be well defined for your BC/DR plan and someone should be specifically responsible for processing change requests. In some cases, this is the BC/DR project manager, in other cases, it may be a role assigned to a team member or it may be managed through some other existing process. Regardless, remember the project management adage: Every task must have an owner. If no one on your team is specifically tasked with this deliverable, it will not get done and it’s the single most important facet of keeping your BC/DR plan up to date.

Most project managers use a change management process for managing their projects and the same types of processes are useful here. As you know, not all changes requested can or should be implemented into a plan. Additionally, even if a change should be made to a plan, there are numerous considerations before incorporating the change into the plan. If you have a standardized change management process that you’ve worked with successfully in the past, you may want to use it here. Be sure to review your process to ensure it’s appropriate to change management in the BC/DR process.

Any changes that are required by law, regulation, or compliance must be made, though there may be several different approaches to incorporating the change that will meet the requirements. In that case, further analysis may be required. Ultimately, for each change you consider, you need to determine the impact on the other elements of the BC/DR plan. For example, if your company moves to a new location, you need to assess the threats again. There may be a chemical processing plant in the new neighborhood that you have to consider. It might be that your business moved in order to get away from the constant threat of hurricanes, but now is subject to earthquakes or flooding from a nearby river. Some changes increase your risks; other changes reduce your risks. Some changes may have a strong effect on the business impact analysis outcomes; others may have no effect at all. This means that all approved changes should be incorporated in the training, testing, and auditing processes and procedures.

Here are some points to consider for a periodic process to manage change:

1. Compile all change requests and prioritize based on potential risk, vulnerability, impact (if applicable).
2. Determine if any change requests are required for legal, regulatory, or compliance reasons. If so, flag these as required changes.
3. Review compiled change requests, review for redundancy, relevancy, etc. Revise compiled list as appropriate.
4. Prioritize compiled list. For each item, determine how the change impacts (or is impacted by):
 - Selected risks and threats
 - Threat vulnerability
 - Business impact analysis
 - Risk mitigation strategies
5. Assess potential cost, risk profile (does it inject or reduce risk?), desirability, feasibility, and interaction with other elements of the plan.
6. Determine if change request should be incorporated, delayed, rejected, or closed.
7. For each change request incorporated, document impact to BC/DR plan in detail. Advise change requestor of change acceptance, if appropriate.
8. For each change *incorporated*, determine need for additional training or testing activities. Trigger notification for training, testing, or auditing if appropriate.
9. For each change *delayed*, document reason for delay and how change will be processed later. Communicate decision to change requestor, if appropriate.
10. For each change *rejected* or *closed*, document reason for denying change. Communicate the status of the change with the rationale to the requestor, if appropriate.
11. For all approved changes, make revisions to BC/DR plan, note change in plan, and notify plan stakeholders of plan revision, if appropriate.

BC/DR PLAN AUDIT

You might wonder why you would audit your BC/DR plan if you're also performing training and testing. The plan audit is a process in which you review the BC/DR plan against specific requirements. For example, you may review it against the organization's business practices, objectives, strategies, or changing financial situation. You may also review the plan against external constraints such as legal or regulatory requirements such as HIPAA or PCI requirements.

The audit does not test the plan. From an audit perspective, there is no assurance that the steps and processes included in the plan will work. The audit does not train people in the use of the plan or in the skills needed to implement and execute the plan. The audit is a more impartial review of the plan to assess whether it meets the

company's overall needs. An audit should be performed as a standard project and an audit plan should be created. This plan should include, at minimum:

- Audit scope, timeline, requirements, and constraints
- Review of corporate risks and risk management strategies including BC/DR
- Review of business impact
- Review of BC/DR plan development activities
- Review of BC/DR plan test plans and activities
- Review of BC/DR plan training plans and activities
- Review of BC/DR change management and plan maintenance processes

This assists in maintaining the plan because gaps or weaknesses in any of these processes or activities can be spotted and addressed. Reviewing these elements may result in the generation of change requests that should be processed by the BC/DR team. You should develop an audit checklist so you can periodically review the plan and use a standardized method each time. It will also simplify the task for you after the first audit.

PLAN MAINTENANCE ACTIVITIES

There are a number of activities beyond change management that can help you keep your plan up to date and ready to go. We've listed a number of these activities here, and of course, if you think of others that will help your team, ensure you add them to the list.

1. If the plan is revised, the BC/DR team members (or those who should have the latest copy of the plan) should be notified in a timely manner.
2. The plan should use a revision numbering system so team members know whether they have the latest version of the plan.
3. Review, update, and revise key contact information regularly. This includes staff, vendors, contractors, key customers, alternate sites, and facilities, among others.
4. Create a BC/DR plan distribution list that is limited to authorized personnel but that includes all relevant parties. This distribution list should include off-site and remote facilities that may be used in the event of BC/DR plan activation.
5. Be sure there are up-to-date copies of the BC/DR plan off-site in the event the building is inaccessible. Alternatively, be sure a copy is secure but accessible in the cloud and provide secure access to these documents.
6. Be sure there are up-to-date paper copies and/or CDs/DVDs/thumb drives of the BC/DR plan on-site in the event IT systems go down. If these contain sensitive information such as key codes, passwords, or other credentialing data, ensure they are encrypted or kept in a secure location that would be accessible during a disaster.
7. Implement a process whereby all old versions of the plan are destroyed or archived and new versions replace them. This helps avoid a scenario where team members are working from different versions of the plan.

8. Always check soft copy and remote storage copies of your plan when changes are made to the plan. If you store copies off-site or at your alternate work site, these versions should be updated any time the plan is modified.
9. Whenever significant changes are requested or implemented, test the plan. This will ensure there are no new areas of concern and will help train staff on the changes.
10. Integrate BC/DR considerations into operational processes to reduce plan maintenance efforts in the future.
11. Assign responsibility for managing BC/DR change notification and requests to someone on the BC/DR team. The project management adage that “a task without an owner won’t get done” is especially true here.
12. Document plan maintenance procedures and follow these procedures to avoid introducing additional risk into the project. Use periodic prescheduled meetings to ensure these events occur on a regular basis.
13. Incorporate training into the change process so changes to people, process, and technology that are incorporated into the BC/DR plan also trigger changes to training plans.
14. Include BC/DR plan testing, training, auditing, and maintenance activities in your IT or corporate budget for future activities related to BC/DR.

PROJECT CLOSE OUT

At this juncture, you should be ready to close out your BC/DR project. If you’ve been working through each step as you’ve read through these chapters, you should have a fairly comprehensive and rigorous BC/DR project plan in place. If you decided to read the material, create the project plan, and then initiate project work, you now have a workable roadmap for how to proceed. In either case, the result should be a clear, comprehensive, and reasonable business continuity and disaster recovery plan that should address the major threats to your company and mitigate risks to the most critical business functions. You should have developed procedures related to monitoring change, implementing change, and maintaining the BC/DR plan that can be folded into standard corporate operations to reduce the BC/DR effort going forward.

Now that you’ve completed work on your plan, you may be ready to launch into a training or testing activity, or you may be ready to put the whole project away until the next review period. Regardless of what you decide your next steps are, you should take time to do several project close-out activities.

1. Ensure all documentation is complete and finalized.
2. Ensure the BC/DR plan is distributed to appropriate personnel.
3. Announce plan completion to project sponsor and other project stakeholders; gain formal approval or sign-off.
4. Announce plan completion to company to increase awareness and celebrate success.

5. Announce plan completion to regulatory authorities, as appropriate or required.
6. Announce training or testing plans, if appropriate.
7. Hold a project review session to discuss lessons learned and incorporate into process. This should not be held at the same time as a project close out or celebration. This should be a working meeting to capture best practices and lessons learned.
8. Hold project close-out meeting to celebrate completion and recognize individual efforts, as appropriate.
9. Complete any staff reviews related to project work.
10. Submit summary or close out report to project sponsor, executive team, or other stakeholders, as appropriate.
11. Update legal or compliance documentation to reflect BC/DR readiness, as appropriate.
12. Set date for next BC/DR audit, review, testing, or training.

Your BC/DR plan will never be perfect and there may be times when it seems it is never complete. However, if you have taken the time and expended the effort to work through the suggestions throughout this book, you should have a solid BC/DR plan that provides a clear roadmap for staff so they know how to keep your business running even when disaster strikes. Along the way, you and your team may have learned a lot more about your company, how it operates, and what contributes to its success. It is our hope that you will never need to find out just how good your plan is and that your efforts will help improve your business operations outside of the realm of disaster readiness.

SUMMARY

Once your BC/DR plan is developed, you need to implement methods for managing change. This includes monitoring changes to the organization that may impact, or be impacted by, the BC/DR plan. Change to the BC/DR plan comes from a variety of sources, including the training, testing, and auditing activities discussed in [Chapter 9](#). Changes in IT infrastructure, systems, and processes are the most common organizational change and ones that potentially have the biggest impact on the BC/DR plan. Changes in operations can also dramatically impact BC/DR plans. Some operational changes happen slowly over time and may go unnoticed until an audit or plan test. Other changes may be more obvious. In either case, changes to operations should trigger change notifications or change requests. Corporate mergers, acquisitions, spin-offs, and restructuring activities can also have a significant impact on BC/DR plans. In many cases, these changes cannot be anticipated and the BC/DR team may simply have to respond to changes as they occur. Changes in the legal, regulatory, or compliance arenas may trigger mandatory changes to the organization or to the BC/DR plan. These changes should be flagged as required and their impact on the BC/DR plan should be assessed.

Since organizations are always changing, you may find you have more cooperation through creating a change notification process. Since operations staff will implement changes to their processes as they see fit, you may be able to get them to notify the BC/DR team of changes so the team can assess the impact and generate a change request to the BC/DR plan, if appropriate. Another very effective strategy for monitoring change can be to include an additional step in standard operating procedures that include a quick assessment of the potential impact of activities on the BC/DR plan. People, processes, and technology are ever-changing in organizations and developing easy-to-use processes for monitoring change, and the potential impact on the BC/DR plan, can assist in plan maintenance.

When change requests are generated, the BC/DR team should have a clear, consistent methodology for evaluating and incorporating change. Not all changes will impact your BC/DR plan; not all change requests should be implemented for a variety of reasons. Using established criteria to evaluate change requests will help reduce the risk that changing the plan injects into the process. Factors such as cost, feasibility, desirability, interaction with existing processes, and risk impact should be assessed before changes are accepted. If a change is accepted, it should be incorporated into the plan, the plan should be revised, and plan stakeholders should be notified the plan has been revised. Updated copies of the plan should be distributed appropriately, and old versions should be destroyed or archived. If requested changes are delayed or declined, the change requestor should be notified of the decision and the rationale for the decision.

The BC/DR plan should be audited periodically to review it from a business perspective. This audit typically does not evaluate the process nor does it necessarily help in training. Its purpose is to review whether the plan meets a stated set of criteria such as business practices, legal, or compliance requirements. Along with testing and training, auditing the plan helps maintain the plan by identifying areas where the plan is diverging from business practices or requirements. Should problems be found, change requests should be generated, evaluated, and incorporated as appropriate.

There are numerous plan maintenance activities that can be incorporated into standard operating procedures throughout the organization. In addition, there are various steps you can include in your process to help keep the plan up to date. These include triggers for updating staff rosters, contact information, and vendor lists. Creating a method for notifying the team regarding the availability of a revised plan and processes for updating plans at remote sites or off-site storage locations, among others, will help ensure that your most recent version of the plan is available in hard and soft copy, both on- and off-site, to the people who are responsible for implementing the plan, if needed.

Finally, the project should be closed out as you would close out any other project. This might include providing a summary document to your project sponsor and to corporate executives, performing staff evaluations and reviews, notifying the company as a whole that the project was successfully completed, holding a project review session to gather lessons learned, holding a project celebration to recognize individual and team efforts, and most importantly, setting a date for the next BC/DR update, review, audit, or test.

After all your hard work and diligent effort, the best scenario will be that your plan is never implemented. Even though you may not see your plan in action, you may find that the process of creating this plan has vastly improved your knowledge and understanding of your company and perhaps improved some of your company's business processes along the way. Perhaps even more important, you'll know that you've done the best job possible protecting your company's valuable data and helping to ensure the continuity of the business. Congratulations on completing your BC/DR plan.

KEY CONCEPTS

BC/DR plan change management

- Training, testing, and IT auditing are the three primary ways the BC/DR plan is updated and maintained. Each of these activities may generate change requests that help modify the plan in ways designed to improve the effectiveness of the plan.
- Changes in IT are constant and incorporating methods of assessing impact to the BC/DR plan in standard operating procedures will help reduce maintenance efforts.
- Changes in operations may happen slowly over time and be almost imperceptible, or they may happen quickly and in obvious ways. Developing a process for change notification within standard operating procedures can help reduce resistance to plan maintenance.
- Corporate changes include mergers, acquisitions, and downsizing. Corporate changes often are planned behind closed doors and are then announced. The BC/DR team must respond to these changes by evaluating the potential impact to the plan.
- In many cases, the best approach to plan maintenance is to incorporate an additional step or two in procedures so that the potential impact to BC/DR plans can be evaluated.
- Legal regulatory compliance may trigger required changes to the BC/DR plan. These should be flagged for special handling to ensure they are incorporated per requirements.

Strategies for managing change

- Monitoring change in the organization can be a challenging task. Changes to personnel, processes, and technology create constant flux in organizations.
- Developing a change notification process separate from a change request process may reduce resistance to BC/DR plan maintenance activities.
- You should develop a methodology for evaluating and incorporating change into the plan. The process should include evaluation criteria and steps for prioritizing, assessing, and incorporating change.
- Changes that are incorporated should trigger a plan revision and team notification that a new plan version is available. Changes may also trigger the need for additional testing or training. If so, this should be flagged and appropriate activities should be scheduled.

- Changes that are delayed or rejected should be noted and the change requestor should be notified of the decision and the rationale for the decision.

BC/DR plan audit

- A BC/DR plan audit reviews the plan against business practices, objectives, and strategies.
- A BC/DR plan audit does not necessarily test or train the plan. Together, training, testing, and auditing are the three fundamental plan maintenance activities.
- Change in financial, legal, or regulatory environment can be spotted during a plan audit and should be addressed appropriately and immediately.
- Generate change requests for all changes resulting from audit activities.
Determine whether these changes require training or testing.

Plan maintenance activities

- There are numerous activities beyond change management that can help keep the plan up to date. These include simple steps, such as a periodic review of team rosters and contact information, to more complex activities such as developing a change management leader for the BC/DR team who processes change notification and change requests.
- Any time the plan is updated, old copies should be destroyed or archived. This includes hard and soft copies both on-site and off-site, as well as copies at alternate work sites and facilities.
- Team members should be notified any time there is a revision to the BC/DR plan.
- Incorporating various plan maintenance activities into the company's standard operating procedures can assist in keeping the plan up to date.

Project close out

- All project documentation should be finalized and stored during project close out. This may include reports to the project sponsor, corporate executives, or other stakeholders.
- If the plan addresses legal, regulatory, or compliance issues, appropriate steps should be taken to notify stakeholders.
- A meeting should be held to review the project and capture lessons learned. This should be held as a separate meeting, not as part of a project celebration.
- A project close out or celebration can be held to recognize the efforts of individuals and teams for their work on the project.
- The project work should not be closed out until a date for reviewing, auditing, training, or testing the plan is scheduled.

This page intentionally left blank

Risk Management Checklist

A

Risk management includes the three elements of the risk assessment: threat assessment, vulnerability assessment, and impact analysis. This information is the input to the risk mitigation phase that concludes the risk assessment portion of the business continuity and disaster recovery project work.

RISK ASSESSMENT

The first step in business continuity and disaster recovery planning is the risk assessment, covered in [Chapter 4](#). The business impact analysis is covered in [Chapter 5](#). Included here are top-level items that should be included. You can modify this list to suit your specific needs. Refer to the specific chapters for detailed information on these topics.

Threat and vulnerability checklist

This list is provided to spark your thoughts on the types of hazards, threats, and vulnerabilities your organization may face. Use this to start a discussion with your team and create your own list once you've completed your risk assessment ([Chapter 4](#)) and business impact analysis ([Chapter 5](#)).

Natural hazards

Cold weather-related hazards

- Avalanche
- Severe snow
- Ice storm and hail storm
- Severe or prolonged wind

Warm weather-related hazards

- Severe or prolonged rain
- Heavy rain and/or flooding
- Floods
 - Flash flood
 - River flood
 - Urban flood
- Drought (can impact urban, rural, and agricultural areas)

- Fire
 - Forest fire
 - Wild fire—urban, rural, agricultural
 - Urban fire
- Tropical storms
- Hurricanes, cyclones, and typhoons (name depends on location of event)
- Tornado
- Wind storm

Geological hazards

- Earthquake
- Tsunami
- Volcanic eruption
 - Volcanic ash
 - Lava flow
 - Mudflow (called a *lahar*)
- Landslide (often caused by severe or prolonged rain)
- Land shifting (*subsidence* and *uplift*) caused by changes to the water table, man-made elements (tunnels, underground building), geological faulting, extraction of natural gas, and so on

Human-caused hazards

Human-caused hazards, also known as *anthropogenic* hazards, are a bit more diverse in their nature.

- Terrorism
 - Bombs
 - Armed attacks
 - Hazardous material release (biohazard, radioactive)
 - Cyber attack
 - Biological attack (air, water, food)
 - Transportation attack (airports, water ports, railways)
 - Infrastructure attack (airports, government buildings, military bases, utilities, water supply)
 - Kidnapping (nonterrorist)
- Bomb
 - Bomb threat
 - Explosive device found
 - Bomb explosion
- Explosion
- Fire
 - Arson
 - Accidental

- Cyber attack
 - Threat or boasting
 - Minor intrusion
 - Major intrusion
 - Total outage
 - Broader network infrastructure impaired (Internet, backbone, etc.)
- Civil disorder, rioting, and unrest
- Protests
 - Broad political protests
 - Targeted protests (specifically targeting your company, for example)
- Product tampering
- Radioactive contamination
- Embezzlement, larceny, and theft
- Kidnapping
- Extortion
- Subsidence (shifting of land due to natural or man-made changes causing building or infrastructure failure)

Accidents and technological hazards

Accidents and technological hazards often are related to man-made hazards but differ only in that they are usually unintentional.

- Transportation accidents and failures
 - Highway collapse or major accident
 - Airport collapse, air collision, or accident
 - Rail collapse or accident
 - Water accident and port closure
 - Pipeline collapse or accident
- Infrastructure accidents and failures
 - Electricity—power outage, brownouts, rolling outages, failure of infrastructure
 - Gas—outage, explosion, evacuation, collapse of system
 - Water—outage, contamination, shortage, collapse of system
 - Sewer—stoppage, backflow, contamination, collapse of system
- Information system infrastructure
 - Internet infrastructure outage
 - Communication infrastructure outage (undersea cables, satellites, etc.)
 - Major service provider outage (Internet, communications, etc.)
 - Systems failures
- Power grid or substation failure
- Nuclear power facility incident
- Dam failure

- Hazardous material incident
 - Local stationary source
 - Nonlocal or in-transit source (e.g., truck hauling radioactive or chemical waste crashes)
- Building collapse (various causes)

Threat and vulnerability assessment

1. Identify all natural threats relevant to your business.
2. Identify all man-made threats relevant to your business.
3. Identify all IT and technology-based threats relevant to your business.
4. Identify all environmental/infrastructure threats relevant to your business.
5. For each threat, identify threat sources.
6. For each threat source, identify the likelihood of occurrence.
7. Based on likelihood of occurrence, assess company's vulnerability to each threat source.
8. Based on likelihood and vulnerability, prioritize list of threats to company.

Business impact analysis

1. Based on prioritized list of threats, assess impact of each threat on business operations.
2. Based on threats, perform upstream and downstream loss analysis.
3. Prioritize business functions into mission-critical, important, and minor (you can customize categories to suit your needs).
4. For each mission-critical business function, assess the impact of the loss of this function.
5. For each mission-critical business function, assess the impact of various threats to this function.
6. Develop a prioritized list of mission-critical business functions with the highest business impact.
7. For the highest priority functions, identify the recovery time requirements including maximum tolerable downtime.
8. For business systems, business functions, and IT systems, identify the following: business process criticality, financial impact, operational impact, recovery objectives, dependencies, and work-arounds.

MITIGATION STRATEGIES

Risk mitigation strategies are developed after the risk assessment phase is complete. Strategies should be developed based on the mission-critical business functions and the risks to the company. Cost, capability, and recovery times are among the aspects

to be considered. IT systems can be included in the risk mitigation strategies or can be addressed as a separate set of strategies. See [Chapter 6](#) for details.

1. For each mission-critical function, identify risk mitigation strategies for consideration including risk acceptance, avoidance, transference, and limitation.
2. For each mission-critical function, identify the recovery requirements and potential recovery options.
3. For each recovery option considered, identify the time, cost/capability, feasibility, service-level requirements, and existing controls in place.
4. For each mission-critical option, select the optimal risk mitigation strategy.
5. For IT systems, identify mission-critical IT systems, equipment, and data.
6. For each mission-critical IT component, identify risk mitigation strategies.
7. For each risk mitigation strategy selected, develop implementation plan.

This page intentionally left blank

Crisis Communications Checklist

B

It's likely you'll need more than one type of communication plan. This checklist provides the generic elements to consider and you can modify, as appropriate, for each type of communication plan you need to develop. Therefore, this list refers to a single communication plan but should be used for all communications plans you need to develop.

Remember the three rules of crisis communication:

1. Tell the truth.
2. Appoint a single spokesperson.
3. Provide who, what, when, where, why, and how.

COMMUNICATION CHECKLIST

1. Define communications needs.
2. Develop communication plan objectives based on target audience (employee, customer, media, etc.).
3. Identify and detail triggers for activating the communications plan.
4. Delineate all assumptions related to the need, objectives, and triggers for the plan.
5. Develop distribution list and methodology based on likely communications scenarios (i.e., if e-mail or phones are down, how will information be communicated?). Develop list of distribution alternatives. If using cloud-based resources, ensure you have needed usernames and passwords readily (and securely) available.
6. Develop list of all contacts needed for distribution of this plan.
7. List all legal or regulatory constraints that may impact message or timing of message.
8. Develop communication template to assist in crisis communication situations.
9. Develop message content (see next).
10. Identify message and distribution authorization or escalation channels.
11. Establish distribution channels.
12. Identify frequency of communication.
13. Keep communication log.

MESSAGE CONTENT

The template for the message can include specific information that *should* always be conveyed such as corporate commitments, policies, or other data related to the incident. The template also should include areas in which caution is recommended. This might mean not disclosing employee names or home addresses, not releasing names of victims or casualty counts, and so on. Include specific language that can be used as a reminder to provide the who, what, when, where, why, and how of the situation.

1. Disaster declaration statement to be communicated to BC/DR team, employees, investors, shareholders, customers, vendors, contractors, as well as community and media contacts.
2. General disaster information including:
 - a. Notification and clarification of event
 - b. Impact of event
 - c. Current status and condition of people, facilities, and equipment
 - d. Frequency of updates and estimated time of next update
3. Specific information and instructions for various stakeholders and groups including:
 - a. Employees
 - b. Vendors, suppliers, and contractors
 - c. Customers
 - d. Business partners
 - e. Community and media
 - f. Legal and regulatory notification requirements
4. Contact information for additional information (corporate spokesperson or communication team leads, as appropriate).

Emergency Response and Recovery Checklists



WARNING

Nothing in this book, including information in this appendix, should be construed as legal, medical, or emergency advice. The data provided are for your information only and you should seek appropriate expert advice on these matters.

We discussed the different phases of business continuity and disaster recovery in [Chapter 7](#), including activation, disaster recovery, business continuity recovery, and maintenance/review. In this appendix, we've provided numerous checklists to help you sort through the details. You can use these checklists to help develop your plan and also as appendices to your own BC/DR plan to provide people with step-by-step roadmaps for emergency and recovery responses. These checklists contain both general disaster response items and IT-specific response items. You can fine tune these lists to meet your specific needs and to cross-reference with your organization's general disaster management plans.

This detail belongs in your BC/DR plan, but breaking it out into sections in this manner will help you process and manage the massive amount of detail required to address these activities properly. Once you've developed your emergency response and business continuity response data, you can (and should) include it in your BC/DR plan.

HIGH-LEVEL CHECKLIST

This is a basic checklist you can use to identify the primary steps in your response to any serious business disruption or disaster. Modify this checklist to include details pertinent to your company's BC/DR plan. This checklist can be used as a high-level response list and can be used as the basis for developing an action flowchart for response activities. You may choose to refer to additional checklists here to point the teams to more detailed lists in each of the response areas.

Disruptive or disaster event occurs

1. Initial response.
2. Notification.

3. Problem assessment.
 4. Escalation.
 5. Disaster declaration.
 6. Plan activation.
 7. Plan implementation activities and logistics.
 8. Disaster recovery phase implementation.
 9. Business continuity phase implementation.
 10. Resumption and normalization of business activities.
 11. Review of event, revision of BC/DR plan based on lessons learned.
-

ACTIVATION CHECKLISTS

You may find it helpful to develop a variety of checklists, which can be extremely useful in making quick decisions for moving forward. Since you and your team may not have time to rehearse these plans frequently, checklists can help remind you of critical steps to take, regardless of the situation. We've included three short checklists in this section; you can expand upon them as desired.

Initial response

1. Receive initial notification of possible, impending, or in-progress disruption or disaster.
2. Alert appropriate emergency response organizations (fire, police, etc.), if needed.
3. Access BC/DR plan.
4. Notify and mobilize damage assessment team and the crisis management team.
5. Assess damage and determine appropriate BC/DR activation steps.
6. Notify appropriate BC/DR team members.
7. Prepare preliminary event report or log. Communicate with appropriate parties.

Damage and situation assessment

1. Receive initial notification of possible, impending, or in-progress disruption or disaster.
2. Review preliminary event report or log.
3. Assess structural damage, health and safety impact, and risks.
4. Determine extent and severity of disruption to operations.
5. Assess potential financial loss.
6. Determine severity based on predefined categories (see categories described earlier in this section).
7. If impact is minor, take no further action and continue to monitor situation.
8. Prepare final assessment and report, and notify BC/DR teams of findings.
9. If impact is intermediate or major, declare disaster and update event report or log, and communicate with appropriate parties.

Disaster declaration and notification

1. Review disaster-level assessment, impacts, and other data gathered during initial response phases.
2. Activate BC/DR teams if they have not already been activated.
3. Review recovery options based on disaster assessment.
4. Select best recovery options for the situation and begin plan to implement recovery options (see next phase).
5. Notify management and crisis communications teams.
6. Prepare a disaster declaration statement that can be communicated to employees, BC/DR team, and community contacts.
7. Monitor progress.
8. Document results in event log and communicate with appropriate parties.

EMERGENCY RESPONSE CHECKLISTS

There are numerous emergency responses required in the aftermath of an event. This list is not meant to be comprehensive nor should you assume items that may not be on the list are unimportant. In developing your emergency response plans, be sure to utilize local experts including fire, police, and search-and-rescue teams to provide input on what measures you and your company's employees can reasonably take and which measures should be left to trained experts.

Emergency checklist one: General emergency response

1. Determine the nature and extent of the emergency.
2. Identify whether anyone has been killed or injured.
3. If injuries have occurred, dial 911 to report the emergency or dispatch emergency medical personnel, as appropriate.
4. Determine if any danger still exists. If so, take appropriate precautions or measures to prevent further death, injury, or damage.
5. Notify crisis management team.
6. Dispatch appropriate trained medical personnel to assist with triage or to manage the situation until emergency responders arrive.
7. Notify civil authorities regarding the nature and extent of the emergency.
 - Police
 - Fire
 - Search and rescue
 - Hazardous materials team
8. Notify corporate executives.

Emergency checklist two: Evacuation or shelter-in-place response

1. Install, identify, and/or test alarms and emergency signals.
2. Identify parameters that would trigger building or facility evacuation procedures.
3. Identify parameters that would trigger shelter-in-place procedures.
4. Identify evacuation/shelter leaders.
5. Identify evacuation routes and assembly points.
6. Identify building search-and-rescue procedures.
7. Identify procedures for securing and shutting down facility.
8. Identify shelter-in-place procedures and internal assembly points (safe areas).
9. Identify method of ascertaining if anyone is missing or unaccounted for.
10. Identify communication methods and frequency following an evacuation or shelter-in-place.
11. Identify provisions needed for shelter-in-place (food, medical supplies, communications equipment, etc.).

Emergency checklist three: Specific emergency responses

Develop specific step-by-step emergency response checklists for highest risk threats. These will utilize many of the same steps as other responses but should be tailored to these events to provide consistent and fast response procedures for staff.

1. Fire—internal or external.
2. Flood.
3. Earthquake.
4. Hazardous materials spill control.

Emergency checklist four: Emergency response contact list, maps, and floor plans

1. External emergency contact numbers:
 - Police and sheriff
 - Fire
 - Hospital
 - Ambulance
 - Other
2. Emergency response team contact numbers:
 - Emergency response team leader
 - Medical staff
 - Evacuation or shelter-in-place leaders
 - Search-and-rescue staff
 - Crisis team manager and/or corporate executive contact
3. Maps:
 - Evacuation routes and assembly areas
 - Shelter-in-place assembly areas

- Escape routes from site—primary and secondary (may need several options depending on disaster scenario)
- Floor plans
- Location of fire doors and fire extinguishers
- Location of utility closets, circuit breaker panels, and power lines
- Location of gas, electric, and water lines
- Location and nature of hazardous materials

Emergency checklist five: Emergency supplies and equipment

Depending on the size of your company, the location of the facilities, and the nature of the business, you may need other supplies than those listed. Be sure to develop a list of supplies and equipment needed, a schedule for testing needed equipment on a periodic basis, a procedure for performing periodic maintenance on equipment, and a process for performing a periodic inventory count of supplies.

1. First aid supplies (portable kits, additional supplies).
2. CPR training and equipment.
3. Fire suppression equipment (fire extinguishers, etc.).
4. Hazardous materials safety equipment.
5. Hazardous materials containment and clean up equipment/supplies.
6. Water, water purification tablets, and shelf-stable food supplies (for shelter-in-place).
7. Clothing, blankets, and other materials (injuries, cold climates, shelter-in-place).
8. Emergency communications equipment (walkie talkies, batteries, etc.).

RECOVERY CHECKLISTS

The recovery checklists are broken out into numerous separate lists. Modify these lists to suit your organization's individualized needs.

Recovery checklist one: General

1. Perform a quick assessment to determine which members of the BC/DR team are available to assist with recovery activities.
2. Identify any travel needs for BC/DR team members (if some are coming from other sites or locations). Be sure to consider the need for local transportation and lodging as well.
3. Identify who will be working at the original site and who will be working at the alternate site (if applicable).
4. Identify resources required including computer equipment, communication links (Internet, dial up, etc.), communications equipment (walkie talkies, cell phones, land lines, etc.), office equipment, office supplies, BC/DR plans, contact lists, and inventory lists.

5. If needed, arrange for access to site or alternate site for vendors, contractors, or employees traveling in from other locations.
6. Notify and activate alternate work site and/or crisis communication command center. Distribute contact information including location, personnel, and phone numbers to key personnel including management, BC/DR team, crisis management team, and HR as appropriate.
7. Provide local contact information and chain of command information (who should people contact for various recovery needs?).
8. Order replacement computer hardware, software, data, and voice communications equipment.
9. Locate configuration information and most current backups.
10. Order faxes, printers, routers, cabling, copiers, tapes, tape backups, and disk drives.
11. Order forms used in normal course of business. Develop forms needed for recovery operations if they do not already exist.
12. Ship key documents to alternate site.
13. Order stationery, business cards, and other business-specific printed matter, if applicable.
14. Prepare process for receiving, tracking, and dispensing equipment and supplies.
15. Prepare process for receiving and tracking data backups and critical records.
16. Finalize preparations for restoring site or activating alternate site.
17. Document results in event log and communicate with appropriate parties.

Recovery checklist two: Inspection, assessment, and salvage

1. Provide damage assessment team with inventory or list of critical resources at damaged site.
2. Ensure all team members have proper safety equipment and have been trained in or reminded of their proper use.
3. Ensure all team members are aware of proper safety procedures and guidelines.
4. Provide team members with forms or process for assessing and reporting damage.
5. Inspect building and utilities (gas, electric, water).
6. Inspect for hazardous materials, chemicals, or hazardous conditions.
7. Inspect resources and vital records for damage including water, fire, water, dust, ice, or physical damage (crushed, tipped over, etc.).
8. Determine potential for further damage or hazard.
9. Determine potential for salvage and restoration.
10. Determine any timelines that may be relevant (equipment sitting in water, operating in extreme heat or cold, etc.) to the salvage operation and to prevent further damage and deterioration.
11. Record assessments in event log.
12. Acquire salvage and restoration equipment, as needed.

13. Remove hazardous materials, as appropriate.
14. Relocate equipment, records, and other salvaged resources, as appropriate.
15. Perform restoration, as appropriate.
16. Document results in event log and communicate with appropriate parties.

WARNING

Any items on the list may be performed by outside contractors, including those specially trained and certified in handling hazardous materials, chemical spills, and so on. Listing these items here does not imply that your team should perform these tasks, simply that they should be performed by appropriately trained personnel.

This page intentionally left blank

Business Continuity Checklist

D

The business continuity phase follows the disaster recovery phase and is focused on resuming business operations. Operations are not normalized or fully restored during this phase but initial business operations, including those deemed mission-critical, are initiated during this phase. At the end of the business continuity phase, normal business operations should resume, which signals the transition out of the BC/DR plan and back into normal operations.

RESUMING WORK

Work may be resumed on a limited basis in the original building or work location if it can be occupied after the disruption or disaster. If not, an alternate work site (AWS) should have been set up during the disaster recovery phase if this is part of your BC/DR plan. Once set up, the AWS should be brought online so that employees can begin work. Work activities typically resume on a limited basis. The restoration of the original facilities or a decision to permanently use alternate facilities will trigger the move to normalization of operations.

Resuming operations

1. Receive notification that work site is fully set up (disaster recovery phase end point). This can be in-place or at alternate location.
2. Ensure all employees are aware of work location (original site or alternate site).
3. Ensure all employees have equipment, tools, supplies, and resources needed to begin limited resumption of work.
4. Check that computer networks, user computers, and other IT resources are installed, configured, tested, and ready for users.
5. Test communications equipment including phone, Internet access, wireless connectivity, and the like.
6. Provide employees with appropriate site access.
7. Review BC/DR plan to understand which mission-critical functions should begin, in what order tasks should be started, and what dependencies exist.
8. Review BC/DR plan to review maximum tolerable downtime and other key recovery metrics.
9. Develop plan for resuming operations based on outcome of review.
10. Identify areas where manual or work-around methods will be implemented.

11. Identify methods for tracking and managing all manual or work-around procedures that are not part of the standard operating procedures.
12. Identify backlogs that may be created as a result of partial resumption of services. Determine if these backlogs are acceptable and if so, how they will be managed once normalization begins.
13. If backlogs are not acceptable, determine what other systems, processes, or procedures must be put into place to avoid backlogs.
14. Determine the status of elements required to avoid backlog and develop plan to put needed elements in place before resuming activities.
15. Resume limited operations.
16. Monitor results.
17. Begin backup procedures to protect new data or new work product(s).
18. Develop status report for crisis management team.

Human resources

1. Ensure human resources (HR) has accounted for all employees. Appropriate actions should be underway if any employees were killed or injured in the event.
2. Take appropriate measures to ensure HR data are available and have been updated.
3. Begin reviewing personnel issues to resolve problems that stem from the disaster or disruptive event including medical or counseling services, insurance issues, and financial issues.
4. Work with department heads to determine if positions need to be filled.
5. Work with department heads to determine if contractors or temporary workers are needed to assist in the restoration or resumption of work activities.
6. Review and implement payroll process. Distribute updated payroll information to all employees.
7. Develop status report for crisis management team.

Insurance and legal

1. Review insurance and notify insurance carrier.
2. Conduct internal assessment of damage and potential insurance coverage.
3. Identify potential insurance gaps or language that may limit claim.
4. If necessary, contact legal counsel for advice and guidance regarding the disaster event (insurance, other liability, regulatory issues, etc.).
5. Provide copies of event logs, damage assessments, and other pertinent documentation to insurance carrier.
6. Submit appropriate paperwork regarding loss.
7. Prepare appropriate documentation for legal review or regulatory compliance.
8. Develop status report for crisis management team.

MANUFACTURING, WAREHOUSE, PRODUCTION, AND OPERATIONS

Whether or not you move into an AWS, you will need to address issues with manufacturing, warehouse, production, or other operations that normally took place at your original site. If you've made arrangements for alternate sites for these functions, you should modify the list presented earlier (Section “[Resuming operations](#)”) to reflect the specific needs of your manufacturing, warehouse, production, or operations in addition to the tasks listed here.

1. Inspect work site (original or alternate) to determine suitability for resuming operations on a limited basis.
2. Review equipment inventory list to ensure all needed equipment is present and operational.
3. Review materials inventory list to ensure all needed materials are available in sufficient quantities to resume operations on a limited basis.
4. Review manual or work-around methods for managing and tracking inventory, production output, and other data if needed IT systems are not back online.
5. Determine the method of tracking and managing all manual or work-around methods until systems come back online. Determine how backlog of data will be addressed once systems come back online.
6. Obtain backup data to determine status of previous, pending, and new orders in the system. Review inventory and shipping data to determine the status of all orders.
7. For all open orders, determine priority and status of each. Develop prioritized order list to determine manufacturing, production, or operational priorities with the understanding that work will resume on a limited basis.
8. Set up and test operations on a trial basis to determine if quality, quantity, and specifications for production are acceptable. If not, take corrective action.
9. If trial run is successful, notify key customers or clients of updated status and time line for delivery.
10. If trial run is successful, begin operations on a gradually increasing basis. Create checkpoints at all critical areas to ensure production meets requirements at each step. Take corrective action as needed.
11. Identify transportation and shipping options at original or alternate site.
12. Begin shipping, receiving, and managing inventory as appropriate.
13. Develop status report for crisis management team.

RESUMING NORMAL OPERATIONS

1. Review assessment from HR regarding status of all employees.
2. Review assessments from damage assessment team, crisis management team, and other teams related to the current status of the facility.

3. Review assessments from CIRT or IT team regarding current status of IT systems.
4. Review assessments from manufacturing, warehouse, production, and operations regarding current status.
5. Review building damage assessment reports and determine feasibility and desirability of returning to original facility.
6. If returning to facility, develop project plan for repairing damage. Develop scope, budget, and time line for return.
7. If not returning to facility, determine options to locate and occupy new facility. Develop costs and alternatives.

Existing facility

1. If staying in existing facility, get bids for repairs from contractors.
2. Select contractor, initiate, and supervise repairs.
3. Obtain appropriate permits for occupancy.
4. Notify insurance company regarding facility. Update policy, as appropriate.
5. Develop list of equipment, supplies, furniture, and other resources needed for resumption of business in original facility.
6. Purchase and obtain necessary equipment, supplies, and furniture.
7. Install IT infrastructure components including LAN cables, servers, routers, firewalls, wireless infrastructure, etc.
8. Install communications equipment (phone lines, Internet access).
9. Install furniture.
10. Install and test computers, workstations, printers, faxes, copiers, and other office equipment.
11. Install and test building access and security measures.
12. Distribute necessary supplies (paper, pens, business cards, etc.).

New facility

1. If staying in alternate facility, review existing contracts for suitability and contact appropriate representatives to negotiate new contract/arrangement for long-term or permanent occupancy.
2. Contact legal representative to review any new, modified, or updated contracts.
3. Obtain appropriate permits for occupancy.
4. If locating new facility, work with real estate professional (if desired) to locate suitable facility.
5. Negotiate for facility including tenant improvements and other improvements or modifications, as needed. Sign lease or contract after appropriate legal review.
6. Notify insurance company regarding facility. Update policy, as appropriate.
7. Develop list of equipment, supplies, furniture, and other resources needed for resumption of business in facility if such resources are not already in place and available.

8. Purchase and obtain necessary equipment, supplies, and furniture.
9. Install any needed IT infrastructure components including LAN cables, servers, routers, firewalls, and needed items that are not already in place at AWS.
10. Install any additional communications equipment (phone lines, Internet access), as needed.
11. Install furniture as needed.
12. Install and test any additional computers, workstations, printers, faxes, copiers, and other office equipment, as needed.
13. Modify and test building access and security measures, as needed.
14. Distribute necessary supplies (paper, pens, business cards, etc.), as needed.

TRANSITION TO NORMALIZED ACTIVITIES

1. Determine appropriate time line to transition to normalized activities.
2. Notify all BC/DR team members of schedule and tasks for transition.
3. Notify all department heads of time line for transition.
4. Identify all operational concerns or constraints regarding transition.
5. Freeze production environment at alternate locations.
6. Perform full data backups of all critical data and vital records.
7. Ship all backups and critical records to original or new location (“location” from here on).
8. Transfer all needed personnel, equipment, machinery, equipment, and supplies to location.
9. Restore and test systems at location.
10. Verify all business systems including IT, manufacturing, production, communications, and such are installed and functional at location.
11. Redirect network traffic and communications traffic (phone lines, voice mail) to location.
12. Provide appropriate physical (building) and logical (IT, network) access to employees.
13. Resume normal activities.
14. Initiate normal data and vital record backup routines. Perform data validation and error checking.
15. Clean up and close down alternate sites according to contractual agreements.
16. Perform postdisaster review to compile and discuss lessons learned, mistakes made, and improvements found during the event.
17. Modify BC/DR plan based on outcome of postdisaster review.

This page intentionally left blank

IT Recovery Checklists

E

The tasks needed to recover IT systems are probably quite familiar to you, but they should be delineated within your BC/DR plan. Each subteam should have a clear set of guidelines and procedures for how and when they will perform their work. Be sure to note dependencies within the checklist so that teams don't work at cross-purposes. You can add items to the checklist as checkpoints for these purposes, much like milestones are used in project plans.

We've included items related to recovering office work space and business operations in this section because they are intertwined with IT recovery efforts. You can reorganize these checklists to suit your approach to BC/DR.

IT RECOVERY CHECKLIST ONE: INFRASTRUCTURE

1. Review BC/DR team member assignments and ensure all team members are present or accounted for.
2. Convene brief planning meeting to ensure all team members understand the situation, the recovery options selected, the requirements, and other constraints.
3. Provide all team members with updated contact information (if appropriate) and chain of command for problem notification and escalation.
4. Ensure all team members have inventory lists, equipment purchase order or shipment information, and that they understand recovery procedures moving forward.
5. Review equipment at alternate site (if used) or at main facility (if used). Ensure all equipment needed for selected recovery option is appropriate and meets requirements.
6. Review procedures for receiving, tracking, and testing IT equipment.
7. Receive backups from storage facility or confirm online availability of backups.
8. Inspect and test backup media, if appropriate.
9. Review or develop floor plans for replacement equipment including IT systems, communications equipment, and infrastructure components.
10. Review network diagram to verify location and connectivity of infrastructure components such as routers, switches, hubs, and gateways.
11. Review network addressing scheme, system configuration data, and security configuration data.
12. Connect all IT components to network.
13. Run procedures to configure infrastructure components.

14. Configure or restore security settings and security devices including firewalls, gateways, and routers. Test configurations, as appropriate.
15. Restore network servers and other critical equipment via backups or via alternate method of recovery (pointing systems to alternate storage locations, etc.).
16. Redirect data and voice traffic to alternate location, if appropriate. If you are restoring at the original site, ensure data and voice traffic are properly routed and working.
17. Provide network access to designated employees at alternate site.
18. Test and verify all network connectivity and security settings.
19. Document results in event log and communicate with appropriate parties.

Recovery checklist two: Applications

1. Review recovery procedures for critical applications. Verify needed servers are restored and online, as appropriate.
2. Review mission-critical data to determine which applications should be restored first.
3. Review internal and external data or application dependencies. Take action, as appropriate, to ensure all dependencies are addressed in the correct order and timing.
4. Review security settings—acquire passwords or reset passwords, as needed.
5. Restore, configure, and verify operating systems if not already performed.
6. Restore, configure, and verify applications.
7. Restore application data from backups, as appropriate. Ensure data are the most current available.
8. Verify integrity of data and functionality of applications.
9. Notify key users of application availability. Inform users of procedures to address data backlogs, if appropriate.
10. Document results in event log and communicate with appropriate parties.

RECOVERY CHECKLIST THREE: OFFICE AREA AND END-USER RECOVERY

1. Review teams and check to ensure team members are present or accounted for.
2. Review MTD and other constraints to ensure compliance with recovery requirements.
3. Verify that team members have necessary alternate work space inventory lists.
4. Review equipment at alternate location and determine if it meets recovery requirements. Note any discrepancies or gaps.
5. Review or revise material receiving, inventory management, and distribution procedures so when new equipment and supplies arrive, they can be properly managed.
6. Review floor layout for alternate work space and determine location of office furniture and equipment including copiers, file cabinets, bookcases, and printer stands.

7. Review network diagram and connectivity. Ensure office layout accommodates existing network, communication, and power connection points. Modify as needed.
8. Receive and set up office furniture per plan. Assign work areas to team members.
9. Receive and set up computers, workstations, printers, and other IT-related user equipment. Ensure wireless devices are configured to connect at current location to network and/or Internet.
10. Set up copiers, faxes, network printers, and telephones at designated locations.
11. Provide office supplies to team members as needed.
12. Provide documents, manuals, and other materials that may have been stored at and retrieved from an off-site storage facility.
13. Reroute voice and data communications to alternate work location. Notify key personnel of current location, contact information, and status.
14. Ensure connectivity to key servers, applications, and data.
15. Set up help desk or customer service function at alternate location.
16. Document results in event log and communicate with appropriate parties.

RECOVERY CHECKLIST FOUR: BUSINESS PROCESS RECOVERY

1. Verify user workstations, desktop, and laptop computers are restored and have access to necessary network resources.
2. Ensure all key personnel or designated users have usernames and passwords for alternate site access.
3. Complete workstation, desktop, or laptop restoration, as needed.
4. Retrieve critical records and forms from storage, if applicable.
5. Receive and process new transactions manually until transactions can be processed electronically.
6. Verify integrity of data on restored systems. When tests are completed satisfactorily, transition to processing transactions electronically.
7. Identify work backlog and implement processes to address backlog to enter data into systems.
8. Begin using restored systems for new transactions.
9. Begin data backup procedures to protect new data being entered into recovered systems.
10. Document results in event log and communicate with appropriate parties.

RECOVERY CHECKLIST FIVE: MANUFACTURING, PRODUCTION, AND OPERATIONS RECOVERY

1. Review maximum downtime and other constraints.
2. Assemble manufacturing, production, or operations recovery team (called “operations” from hereon).

3. Tour alternate operational areas to assess status or tour original operational areas to assess current damage and status. Review safety requirements against current status.
4. Review environmental conditions including heating/cooling, humidity or dust levels, air filtration status (dust, odors, airborne contaminants, etc.). Determine if current condition and status meet operating requirements.
5. Inspect any stored hazardous materials or chemicals for safety.
6. Inspect and test, as appropriate, all safety devices including fire extinguishers, smoke detectors/alarms, emergency lighting, among others.
7. Verify sufficient electrical (or other power) exists to run machinery and equipment.
8. Verify teams have alternate facility operating procedures and inventory lists.
9. Review equipment against inventory lists and operating requirements. Address any gaps or discrepancies.
10. Review and revise, as needed, equipment receiving, inventory management, and equipment distribution procedures. Ensure that equipment and inventory arriving at the alternate (or damaged original) location are tracked and monitored.
11. Receive any critical equipment, parts, supplies, or materials from off-site storage, vendor shipment, or salvage from original location.
12. Receive and inspect any salvageable or existing inventory. Assess status and dispatch inventory as appropriate (destroy, store, repackage, reuse, etc.).
13. Review floor layout for manufacturing, production, or operational activities. Ensure proper connections including power, data, or network exist in the proper locations.
14. Place equipment in locations and install, connect, and test.
15. Install and test auxiliary equipment including printers, copiers, telephones, walkie talkies, radios, and other equipment needed for operations.
16. Provide operational and configuration documentation to team leaders or equipment operators, as appropriate.
17. Install and configure any IT-related equipment including interfaces, workstations, desktops, etc.
18. Set up connectivity between operations and IT systems at alternate locations, as needed.
19. Test equipment, machinery, and configurations.
20. Test output of operations for quality, quantity, and other required attributes.
21. Test voice and data network to ensure connectivity.
22. Ensure operators have information needed to begin production including logins, passwords, keys, or other necessary tools.
23. Review and implement any manual workarounds for production or inventory management needed.
24. Review and implement any electronic production or inventory management procedures, as needed.
25. Begin manufacturing, production, or operations on limited basis.
26. Test and verify output. Expand or increase production as warranted.
27. Document results in event log and communicate with appropriate parties.

Training, Testing, and Auditing Checklists

F

Business continuity and disaster recovery training can be accomplished through testing the plan. Testing the plan results in training participants; therefore, they are referred to as one activity here.

TRAINING AND TESTING

1. Identify scope, time line, and requirements for training.
2. Determine training needs for each participant group (ERT, CMT, damage assessment, IT, etc.).
3. Develop training approach (may use testing methods for training, see item 6).
4. Develop training objectives.
5. Develop training or testing duration and cost estimates.
6. Develop training or test scenarios.
7. Develop training or testing method (paper walk-through, functional, or field exercises, full interruption).
8. Develop training or testing evaluation criteria.
9. Identify training or testing participants.
10. Identify training or testing resources needed.
11. Deliver training or conduct testing.
12. Evaluate training or testing based on evaluation criteria.
13. Collect and analyze lessons learned.
14. Revise training, testing, or BC/DR plan, as appropriate.

IT AUDITING

1. Identify IT risk mitigation strategies selected.
2. Audit IT risk mitigation strategies to ensure they have been properly implemented and configured.
3. Audit IT systems to ensure systems identified in BC/DR plan are still in place and functioning.
4. Identify new technology implementations (planned or in progress) and assess against BC/DR objectives. Recommend revisions to technology plans or BC/DR plans as appropriate.

5. Identify technology to be replaced or decommissioned (planned or in progress) to assess the impact on BC/DR plans. Recommend revisions to technology plans or BC/DR plans as appropriate.
6. Audit all processes in BC/DR plan related to IT systems to ensure steps, processes, requirements, tools, supplies, and resources identified are still accurate, current, relevant, and complete.
7. Audit IT response team to ensure team is intact, ready to respond, has clear understanding of roles/responsibilities, and has tools/resources to implement plan.
8. Audit existing systems to ensure compliance with current BC/DR plans including:
 - Operating systems
 - Networking and telecommunications equipment
 - Database and applications
 - Systems backups
 - Desktop and mobile devices
 - Security controls
 - Integration and testing
 - Other (define)

BC/DR Plain Maintenance Checklist

G

Training, testing, and auditing are three activities that generate useful information about the BC/DR plan and therefore contribute to plan maintenance. Change management and BC/DR plan audits also contribute to keeping the plan up to date. Modify the following list to meet the requirements of your organization.

CHANGE MANAGEMENT

1. Review contact list. Update and revise as needed.
2. Review vendor list. Update and revise as needed.
3. Review vendor contracts. Update, extend, and revise as needed.
4. Review team membership (ERT, CMT, CIRT, etc.). Update and revise as needed.
5. Review team membership changes. Assess training needs.
6. Develop, document, and implement formal BC/DR plan change management processes:
 - a. Monitoring changes that impact or are impacted by BC/DR plan.
 - b. Evaluating change notifications and requests.
 - c. Implementing appropriate changes to BC/DR plan.
 - d. Testing, training, and auditing revised plan.
 - e. Notifying stakeholders of changes incorporated, delayed, or denied.
 - f. Revising BC/DR plan appropriately.
 - g. Distributing updated copies of the BC/DR plan to appropriate parties.
7. Review lessons learned from training, testing, and auditing. Assess impact to BC/DR plan and revise plan as needed.
8. Review changes to IT systems and processes. Assess impact to BC/DR plan. Make changes as needed.
9. Review changes to operations, including mission-critical business processes and functions. Assess impact to BC/DR plan and revise plan as needed.
10. Review changes to corporation including mergers, acquisitions, spin-offs, downsizing, and so on. Assess impact to BC/DR plan and revise plan as needed.
11. Review and revise risk assessment. Perform subsequent planning steps (impact analysis, risk mitigation, training, testing) to update BC/DR plan.
12. Update flowcharts and checklists, as needed.

- 13.** Distribute revised plans to distribution list. Notify appropriate parties of the revised plan as well as how to obtain it and how to dispose of the outdated copies of the plan.
- 14.** Destroy or archive old copies of the plan including hard and soft copies, on- and off-site copies, and copies that may be stored with trusted vendors, partners, or at alternate work sites or facilities.
- 15.** Perform periodic audit BC/DR plan and incorporate recommendations and changes.
- 16.** Perform periodic test of BC/DR plan and incorporate recommendations and changes.
- 17.** Perform periodic training of BC/DR plan and incorporate recommendations and changes.

Glossary of Terms

Accident an unforeseen and unplanned event or circumstance, often with lack of intention or necessity

Activation (of DRP) following a set of documented procedures in a DRP once a predefined trigger (e.g., duration, severity) results in a disaster being declared

Audit an evaluation of a person, organization, system, process, enterprise, project, or product

Availability the ratio of (a) the total time a functional unit is capable of being used during a given interval, to (b) the length of the interval. For example, a unit that is capable of being used 100 hours per week (168 hours) would have an availability of 100/168 or 0.595 (59.5%). In high availability applications, a metric known as nines, corresponding to the number of nines following the decimal point, is used. For example, “five nines” equals 0.99999 (or 99.999%) availability

Backup the copying and archiving of computer data so it may be used to restore the original after a data loss event

BC/DR business continuity/disaster recovery

Biological hazard biological substances that pose a threat to the health of living organisms, primarily that of humans (also known as biohazards)

Bring your own device (BYOD) the policy of permitting employees to bring personally owned mobile devices (laptops, tablets, and smart phones) to their workplace and use those devices to access privileged company information and applications

Business case the reasoning for initiating a project or task, generally expressed in written form to include both quantifiable and unquantifiable characteristics of a proposed project

Business continuity (BC) daily activities performed by an organization to ensure that critical business functions will be available to customers, suppliers, regulators, and other entities that must have access to those functions (sometimes confused with “disaster recovery,” which is a subset of business continuity and only occurs in the event of a disaster)

Business continuity management (BCM) the set of processes that identify and evaluate potential risks to an organization and develop the organization’s resilience by ensuring critical objectives are met and the resources necessary to achieve those objectives are available; these risks, or adverse events, may include emergencies, crises, disasters, or incidents that disrupt normal business activity; in the case of an adverse event which has negative consequences, BCM ensures an effective response to minimize losses and restore regular operations

Business continuity plan (BCP) a documented set of processes and/or procedures to enable a business to continue normal operations irrespective of adverse conditions or events, including procedures for business resumption, emergency response, continuity of operations, incident management, and disaster recovery (also known as a BC/DR plan)

Business continuity planning development of the standards, program development, and supporting policies, guidelines, and procedures needed to ensure a business can continue without stoppage, irrespective of the adverse circumstances or events

Business impact analysis (BIA) a subset of business continuity planning which differentiates critical (urgent) and noncritical (nonurgent) organization functions/activities and determines recovery requirements for those functions (e.g., MTD, RTO, RPO). Critical

functions are those whose disruption is regarded as unacceptable. Perceptions of acceptability are affected by the cost of recovery solutions. A function may also be considered critical if dictated by law

Business interruption insurance contrasted with “business protection insurance” which only covers the physical damage to the business, an insurance policy which covers the loss of income that a business suffers after a disaster while its facility is either closed because of the disaster or in the process of being rebuilt after it; also known as “business income insurance”

Change advisory board (CAB) supports the Change Management team by approving requested changes and assisting in the assessment and prioritization of changes; this body is generally made up of IT and business representatives that include the change manager, user managers and groups, technical experts, possible third parties, and customers (if required)

Change management (ITSM) an IT service management (ITSM) discipline which ensures standardized methods and procedures are used for efficient and prompt handling of all changes to control IT infrastructure, in order to minimize the number and impact of any related incidents upon service

Chief information security officer (CISO) the senior-level executive within an organization responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets are adequately protected

Cold backup site an alternate site used for recovery of IT systems which does not include backed up copies of data and information from the original location of the organization nor hardware already set up; the lack of hardware contributes to the minimal start-up costs of the cold site, but requires additional time following the disaster to have the operation running at a capacity close to that prior to the disaster

Computer emergency response team (CERT) the historic designation given to the first computer security incident response team (CSIRT) at Carnegie Mellon University (CMU), established under a U.S. government contract and trademarked by CMU

Computer security incident response team (CSIRT) team within an organization which, upon notification of a potential security breach which disrupts business operations, is able to analyze the situation, determine the breadth of the compromise, and take corrective action in order to restore service as quickly as possible; part of Incident Management; also known as Computer Incident Response Team (CIRT)

Confidentiality (data) preventing the disclosure of information to unauthorized individuals or systems

Continuous data protection (CDP) backup of computer data by automatically saving a copy of every change made to that data, essentially capturing every version of the data that the user saves, allowing the user or administrator to restore data to any point in time; also known as “continuous backup” or “real-time backup”

Crisis communication plan (CCP) the preplanned documented effort taken by an organization to communicate with the public and stakeholders when an unexpected event occurs that could have a negative impact on the organization’s reputation; this can also refer to the efforts to inform employees or the public of a potential hazard which could have a catastrophic impact; the plan usually consists of three elements: (1) a holding statement (a passive prepared press statement which has been approved by the Crisis Communicators and Legal Advisors), (2) questions and answers (Q&A) with prepared and agreed answers for foreseeable questions if asked, and (3) internal communication

- Crisis management** process by which an organization deals with a major event that threatens to harm the organization, its stakeholders, or the general public; in contrast to risk management, which involves assessing potential threats and finding the best ways to avoid those threats, crisis management involves dealing with threats before, during, and after they have occurred
- Crisis management team (CMT)** a designated team within an organization responsible for crisis management, which directs the actions of subteams during a crisis, such as an emergency response team (ERT) and one or more disaster recovery (DR) teams
- Critical path method (CPM)** calculates the longest path of planned activities to the end of a project (i.e., critical path), and the earliest and latest that each activity can start and finish without making the project longer
- Critical records** data sets or information, physical or electronic, which are critical to normal business operations
- Critical success factor (CSF)** the term for an element that is necessary for an organization or project to achieve its mission; e.g., a CSF for a successful IT project is user involvement
- Criticality** when used to determine business continuity requirements, the importance of a particular business function or process, and underlying system(s) or discrete set(s) of data, required to operate the business normally
- Cyber** used in names coined for “electronic” or computer-related counterparts of a preexisting product or service, e.g., the Internet referred to as cyberspace, or a computer system (discrete set of hardware and software) referred to as a cyber asset (CA)
- Cyber crime** any crime that involves a computer and a network, regardless if the computer is the target of the crime or if it is used in the commission of a crime; also known as “computer crime”
- Cyber incident response plan (CIRP)** documented processes and procedures for handling a security incident, including team member roles and responsibilities, and lines of authority, definition of a security incident, definition of a reportable incident, training, detection, classification, escalation, containment, eradication, and documentation; also known as “incident response plan”
- Cyber threat** a possible danger, intentional or accidental, that might exploit a computer or network vulnerability to breach security and thus cause possible harm; also known as “computer threat”
- Damage assessment team** team responsible for initial damage assessment, typically part of an emergency response team (ERT) set up to coordinate activities during the immediate aftermath of a disaster
- Data conservator** the designated “owner” of a discrete set of information within an organization responsible for authorizing access and defining business requirements for such information
- Data encryption** the process of encoding information (“in transit”—such as when travelling across a network—or “at rest”—such as when written to permanent storage media) in such a way that eavesdroppers or hackers cannot read it, but that authorized parties can
- Data privacy** the relationship between collection and dissemination of data, technology, the public expectation of privacy, and the legal and political issues surrounding them; privacy concerns exist wherever personally identifiable information is collected and stored—in digital form or otherwise
- Data recovery** the process of salvaging data from damaged, failed, corrupted, or inaccessible secondary (or backup) storage media, such as internal or external hard disk drives, solid-

state drives (SSD), USB flash drives, storage tapes, CDs, DVDs, RAID, and other electronics, when it cannot be accessed normally

Data replication maintaining a copy of data in its original form at an alternate location

Data security “information security”

Data sensitivity the control of access to information or knowledge that might result in loss of an advantage or level of security if disclosed to others; loss, misuse, modification, or unauthorized access to sensitive information can adversely affect the privacy or welfare of an individual, trade secrets of a business or even the security, internal and foreign affairs of a nation depending on the level of sensitivity and nature of the information; also known as “information sensitivity”

Data transmission encryption same as “data encryption in transit”; “data encryption”

Defense in depth the use of administrative, logical, and physical security controls to protect information (data) while at rest or in transit; in the “onion” analogy, with data at the core of the onion, the combination of administrative, logical, and/or physical controls employed at separate application, host/operating system, and network layers (outward, respectively) to protect the data based on its classification

Desktop exercise when used in reference to DRP testing, training, or auditing, refers to a method of testing the DRP whereby the testing participants work through disaster recovery procedures on paper in a simulated disaster environment

Disaster a natural or man-made (or technological) hazard resulting in an event of substantial extent causing significant physical damage or destruction, loss of life, or drastic change to the environment

Disaster recovery a subset of business continuity that deals with technology recovery as opposed the recovery of business operations

Disaster recovery plan (DRP) a documented process or set of procedures to recover and protect a business’ IT infrastructure in the event of a disaster

Downstream loss loss of data transmission or interconnection from current system to other system, rendering other system partially or wholly nonfunctional

Emergency preparedness preparing equipment and procedures for use when an emergency or disaster occurs, i.e., planning; preparedness measures can take many forms including the construction of shelters, implementation of an emergency communication system, installation of warning devices, creation of backup environmental services (e.g., power, water, sewage), and rehearsing evacuation plans; also known as “disaster preparedness”

Emergency response protocol or set of actions to perform to mitigate the negative effects of an emergency, including actions required for medical assistance/first aid, building evacuation, fire prevention, hazardous materials spills, hostage situations, information systems attacks, or disaster relief

Emergency response team (ERT) a group of people who prepare for and respond to any emergency incident, such as a natural disaster or an interruption of business operations; in business continuity planning, the ERT is typically a subteam of the crisis management team (CMT) and includes roles such as internal disaster assessment teams, building evacuation coordinators, first responders, and the like

Escalation procedure in relation to business continuity planning, the specific conditions and events that trigger the activation of an emergency response plan

Event log a file which is appended with events reported by an application, database, operating system, or other IT infrastructure component, used to monitor for incidents and maintain an audit trail

Fault tolerance the property that enables a computer system to continue operating properly in the event of the failure of (or a fault within) some of its components

Federal Emergency Management Agency (FEMA) an agency of the U.S. Department of Homeland Security, initially created by Presidential Reorganization Plan No. 3 of 1978 and implemented by two Executive Orders on April 1, 1979, whose primary purpose is to coordinate the response to a disaster that has occurred in the United States and that overwhelms the resources of local and state authorities

Federal Trade Commission (FTC) an independent agency of the U.S. government, established in 1914 by the Federal Trade Commission Act, whose principal mission is the promotion of consumer protection and the elimination and prevention of anticompetitive business practices, such as coercive monopoly; Section 5 of the FTC Act gives the FTC broad authority to investigate “unfair and deceptive acts and practices in or affecting commerce”; the FTC has increasingly used this broad authority aggressively in the privacy and data security contexts, initiating investigations pertaining to a wide variety of “unfair” or “deceptive” practices; in particular, the FTC has brought a number of cases alleging that Web site operators engaged in deceptive acts in failing to adhere to their stated policies and practices

Fraud wrongful or criminal deception intended to result in financial or personal gain

Gramm-Leach-Bliley Act (GLBA) also known as the Financial Services Modernization Act of 1999 and enacted November 12, 1999, GLBA implemented The Safeguards Rule among other changes required of commercial banks, investment banks, securities firms, and insurance companies operating in the United States. The Safeguards Rule requires financial institutions to develop a written information security plan (WISP) that describes how the company is prepared for, and plans to continue to protect clients’ nonpublic personal information; the Safeguards Rule applies to information of any consumers past or present of the financial institution’s products or services; the WISP must include (1) denoting at least one employee to manage the safeguards, (2) constructing a thorough risk analysis on each department handling the nonpublic information, (3) developing, monitoring, and testing a program to secure the information, and (4) changing the safeguards as needed with the changes in how information is collected, stored, and used

Hardening (computer) the process of securing an IT system by reducing its surface of vulnerability; a system has a larger vulnerability surface the more that it does; in principle, a single-function system is more secure than a multipurpose one; reducing available vectors of attack typically includes the removal of unnecessary software, unnecessary usernames or logins, the disabling or removal of unnecessary services, patching the operating system kernel, closing open network ports, and setting up intrusion-detection systems, firewalls, and intrusion-prevention systems

Hazard an unavoidable danger or risk, even though often foreseeable

Health Insurance Portability and Accountability Act (HIPAA) enacted August 21, 1996, this federal law implements, among other requirements, the Security Rule for healthcare providers, health insurance companies, and their business associates, which requires all covered entities to protect Electronic Protected Health Information (EPCI) by implementing administrative, physical, and technical security safeguards, including having a contingency plan for responding to emergencies (documenting data priority and failure analysis, testing activities, and change control procedures), backing up their data, having disaster recovery procedures in place, encryption of EPCI in transit over open networks, ensuring that the data within its systems have not been changed or erased in an unauthorized

manner, data corroboration, including the use of check sum, double-keying, message authentication, and digital signature, and authentication controls such as password systems, two- or three-way handshakes, telephone callback, and token systems

Hot backup site a duplicate of the original site of the organization, with full computer systems as well as near-complete backups of user data; real-time synchronization between the two sites may be used to completely mirror the data environment of the original site using wide area network links and specialized software

Human resources (HR) the personnel of a business or organization who are part of the triad of people, processes, and technology used to implement business continuity planning

Human threat possible disruption in normal operations caused by a human, whether intentional (e.g., terrorism, sabotage) or unintentional (e.g., inadvertent data entry, tripping over power cord)

Human-caused hazard see “[human threat](#)”

Hypervisor software, firmware, or hardware which allows multiple virtual machines, or guest operating systems, to run using the same host machine hardware

Impact assessment same as business impact analysis (BIA)

Impact criticality see “[criticality](#)”

Incident management the activities of an organization to identify, analyze, and correct hazards in order to prevent a future reoccurrence; as defined by ITIL, an unplanned interruption to an IT service, reduction in the quality of an IT service, or failure of a configuration item (CI) that has not yet impacted service

Information assurance act of ensuring that data are not lost when critical issues arise, including natural disasters, computer/server malfunction, physical theft, or any other instance where data have the potential of being irrevocably lost

Information security (InfoSec) defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording, or destruction; attributes include confidentiality, integrity, and availability (commonly referred to as CIA—the triad of information security)

Integrity (data) maintaining and assuring the accuracy and consistency of data over its entire life cycle

International Organization for Standardization (ISO) founded on February 23, 1947, and headquartered in Geneva, Switzerland, an international standard-setting body composed of representatives from various national standards organization whose mission is to promote worldwide proprietary, industrial, and commercial standards; ISO 22301 deals specifically with business continuity standards

IT governance a subset discipline of corporate governance focused on information technology (IT) systems and their performance and risk management; an IT governance framework is used by an organization to establish transparent accountability of individual decisions and ensure the traceability of decisions to assigned responsibilities

IT Information Library (ITIL) trademarked by the British Government and currently a Crown Copyright, a set of practices for IT service management (ITSM) that focuses on aligning IT services with the needs of business, published in a series of five core publications, each of which covers an ITSM life cycle stage (ITIL 2011 edition); ITIL underpins (but is different from) ISO/IEC 20000, the International Service Management Standard for IT service management

IT risk management considered a component of a wider enterprise risk management program, the application of risk management to information technology assets in order to

- manage IT risk (i.e., the business risk associated with the use, ownership, operation, involvement, influence, and adoption of IT within an enterprise)
- IT service level** as defined by ITIL, a level of IT service specified in a service-level agreement (SLA) and measured as a service-level objective (SLO), which can be quantified in terms such as time/duration for response, availability, quality, and/or scope of service
- IT service management (ITSM)** implementation and management of quality IT services that meet the needs of the business; to structure IT-related activities and the interactions of IT technical personnel with internal business customers and users
- Key man insurance** an important form of business insurance used for business succession or business protection purposes; an insurance policy taken out by a business to compensate that business for financial losses that would arise from the death or extended incapacity of an important member of the business; also known as “key person insurance” or “keyman insurance”
- Likelihood** used to quantify risk, likelihood is a numerical level of certainty assigned to the occurrence of a particular threat or hazard based on the level of vulnerability present; risk can be quantified as likelihood multiplied by impact
- Maximum tolerable downtime (MTD)** also known as maximum tolerable period of disruption (MTPOD), a quantifiable business continuity requirement which specifies the maximum amount of time that an enterprise’s key products or services can be unavailable or undeliverable after an event that causes disruption to operations before its stakeholders perceive unacceptable consequences; MTD is equal to the sum of the recovery time objective (RTO) for a particular IT service and the work recovery time (WRT) for normal or workaround business process to resume after recovery of the applicable IT systems and data
- Media relations** contrasted with “public relations” which describes managing a company’s relationship with the public at large, management of a company’s relationship with journalists; used in crisis communications to describe how a company communicates with the media during a disaster, strike, or other business disruption which impacts its shareholders and/or the public at large
- Mission-critical** any factor of a system (equipment, process, procedure, software, etc.) whose failure will result in the failure of business operations, i.e., critical to the organization’s “mission”; as a rule in crisis management, if a triage-type decision is made in which certain components must be eliminated or delayed, e.g., because of resource or personnel constraints, the mission critical ones must not be among them
- Mobile site** for disaster recovery planning purposes, a mobile site refers to an alternate DR facility which can be relocated to a different geographic area and used for limited or temporary recovery operations; a mobile site typically houses required workspace, power, network, data center, and/or end user systems and can be used to temporarily resume business critical operations until the damaged or inaccessible facility is restored
- National Flood Insurance Program (NFIP)** established through the National Flood Insurance Act of 1968, the program enables property owners in participating communities to purchase insurance protection from the government against losses from flooding; NFIP insurance is designed to provide an insurance alternative to disaster assistance to meet the escalating costs of repairing damage to buildings and their contents caused by floods
- National Institute of Standards and Technology (NIST)** a nonregulatory federal agency within the U.S. Department of Commerce whose Computer Security Division develops

standards, metrics, tests, and validation programs as well as publishes standards and guidelines to increase secure IT planning, implementation, management, and operation

Natural disaster a major adverse event resulting from natural processes of the Earth; examples include floods, volcanic eruptions, earthquakes, tsunamis, and other geologic processes; a natural disaster can cause loss of life or property damage to vulnerable populations, and typically leaves some economic damage in its wake, the severity of which depends on the affected population's resilience, or ability to recover

Network-attached storage (NAS) file-level computer data storage connected to a computer network providing data access to a heterogeneous group of clients, removing the responsibility of file serving from other servers on the network; often manufactured as a computer appliance—a specialized computer built from the ground up for storing and serving files—rather than simply a general purpose computer being used for the role

Pandemic an epidemic of infectious or contagious disease that has spread through human populations across a large region, crossing international boundaries, and usually affecting a large number of people

Parametric estimate an estimate of the values of parameters based on measured/empirical data that have a random component; for example, to estimate the proportion of a population of voters who will vote for a particular candidate, the proportion is the parameter sought and the estimate is based on a small random sample of voters

Payment card industry data security standard (PCI DSS or PCI) defined by the Payment Card Industry Security Standards Council, a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards; created to increase controls around cardholder data to reduce credit card fraud via its exposure

Personally identifiable information (PII) as used in information security and solely a legal concept, any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information; also known as "personal data"

Plan maintenance act or method of updating a written plan to maintain its currency and relevancy as organizational or operational changes occur, such as change in business processes, data growth, corporate acquisitions, new product launch, system development milestone, etc.

Procedure the specific instructions necessary to perform a task or part of a process

Process related activities that produce a specific service or product (for example, Procurement to Payment), the majority of which typically cross departments or functional areas

Process map a diagram showing the relationship of the procedures in a process, including who is responsible to perform the procedure (e.g., team, department, or division), what major functions are performed, and when the function is triggered; also called a "swim lane diagram"

Project a temporary endeavor with a defined beginning and end, usually time-constrained and often constrained by funding or deliverables, undertaken to meet unique goals and objectives, typically to bring about beneficial change or added value; stands in contrast to "business as usual," or the repetitive, permanent (or semi-permanent) nature of existing business operations

- Project management** the discipline of planning, organizing, motivating, and controlling resources to achieve specific goals
- Project management methodology** the approach, or sequence of steps, taken to manage project activities; examples include lean, agile, iterative, incremental, and phased
- Project team** a team whose members usually belong to different groups, functions, and are assigned to activities for the same project
- Protected Health Information** confidential health information, including name, medical record number, diagnoses, treatments, medications and more, which can be identified as belonging to a specific individual
- Public relations** the practice of managing the spread of information between an individual or an organization and the public, in order to persuade the public, investors, partners, employees, and other stakeholders to maintain a certain point of view about it, its leadership, products, or of political decisions
- Qualitative threat assessment** a three-to-five-step evaluation of probability times impact (e.g., Very High to Low) performed when the organization requires a risk assessment be performed in a relatively short time or to meet a small budget, or when a significant quantity of relevant data is not available, or when the persons performing the assessment don't have the sophisticated mathematical, financial, and risk assessment expertise required; typically performed through interviews of a sample of personnel from all relevant groups within an organization charged with the security of the asset being assessed; may be followed by a quantitative evaluation of the highest risks to be compared to the costs of security measures
- Quantitative threat assessment** how much an organization could estimate to lose from an asset based on the risks, threats, and vulnerabilities; typically expressed as a calculation of the Annualized Loss Expectancy (ALE), equal to the single loss expectancy (SLE) of an asset (defined as the loss of value to asset based on a single security incident) times the Annualized Rate of Occurrence (ARO) (an estimate based on the data of how often a threat would be successful in exploiting a vulnerability), i.e., $ALE = SLE \times ARO$; the values of assets to be considered are those of all involved assets, not only the value of the directly affected resource, e.g., if you consider the risk scenario of a laptop theft threat, you should consider the value of the data (a related asset) contained in the computer and the reputation and liability of the company (other assets) deriving from the loss of availability and confidentiality of the data that could be involved, keeping in mind intangible assets (data, reputation, liability) can be worth much more than physical resources at risk (the laptop hardware itself)
- Reasonable security** used in information security practice, this legal definition requires both (1) implementation of an ongoing process and (2) addressing certain categories of security measures, including physical facility and device security controls, physical access controls, technical access controls, intrusion-detection procedures, employee procedures, system modification procedures, data integrity, confidentiality and storage, data destruction and hardware and media disposal, audit controls, contingency plan (data backup, disaster recovery, emergency-mode operation), and incident response plan (to specifically address security breach requirements)
- Recovery point objective (RPO)** the maximum tolerable period, derived during a Business Impact Analysis (BIA), in which data might be lost from an IT service due to a major incident
- Recovery time objective (RTO)** the duration of time and a service level, derived during a Business Impact Analysis (BIA), within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a

break in business continuity; duration of time can include the time for trying to fix the problem without a recovery, the recovery itself, testing, and the communication to the users

Redundant array of inexpensive disks (RAID) a data storage technology that combines multiple disk drive components into a logical unit, where data are distributed across the drives in one of several ways called “RAID levels,” depending on the level of redundancy and performance required; also known as “redundant array of independent disks”

Regulatory compliance the goal that corporations or public agencies aspire to achieve in their efforts to ensure that personnel are aware of and take steps to comply with relevant laws and regulations; due to the increasing number of regulations and need for operational transparency, organizations are increasingly adopting the use of consolidated and harmonized sets of compliance controls; this approach is used to ensure that all necessary governance requirements can be met without the unnecessary duplication of effort and activity from resources

Reliability the ability of a system or component to perform its required functions under stated conditions for a specified period of time; as reliability of a system increases, so does availability

Relocation team the members (or subteam) of the disaster recovery team responsible for coordinating the process of moving from the hot site to a new location or to the restored original location

Remote journaling capturing information about an electronic message or database transaction while it is in transit and storing that information outside of the production system or off site; typically used for audit purposes; journaling is different from archiving in that the journaled message is captured while in transit (as opposed to after it has been written), should be encrypted and users should not have access to their own journaled message store

Resource and logistics team used in BC/DR planning, the team responsible for re-establishing the flow of equipment and supplies after a localized or widespread disaster, including how items will be purchased, tracked, and managed; may be a subteam of crisis management team (CMT)

Return on investment (ROI) metric is to measure, per period, rates of return on money invested in an economic entity in order to decide whether or not to undertake an investment

Risk the potential that a chosen action or activity (including the choice of inaction) will lead to a loss or other undesirable outcome

Risk acceptance taking no additional action to avoid a risk because the risk involved is not adequate enough to warrant the added cost it will take to avoid that risk

Risk assessment the determination of quantitative or qualitative value of risk related to a concrete situation and a recognized threat (or hazard)

Risk avoidance any action where ways of conducting business are changed to avoid any risk occurrence, e.g., the choice of not storing sensitive information about customers can be an avoidance for the risk that customer data can be stolen

Risk management the identification, assessment, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities

Risk mitigation prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process, with the goal of using the least-cost

approach and implementing the most appropriate controls to decrease mission risk to an acceptable level, with minimal adverse impact on the organization's resources and mission

Risk mitigation strategy decision to accept, reduce, avoid, or transfer risk in order to minimize effect of risk

Risk transference purchasing insurance or outsourcing the risk to a third party when the risk has a very high impact but is not easy (or too costly) to significantly reduce the likelihood by means of internal controls

Sabotage a deliberate action aimed at weakening another entity through subversion, obstruction, disruption, or destruction

Sarbanes-Oxley Act (SOX) also known as the "Public Company Accounting Reform and Investor Protection Act" (in the Senate) and "Corporate and Auditing Accountability and Responsibility Act" (in the House); a U.S. federal law created in 2002 that set new or enhanced standards for all U.S. public company boards, management, and public accounting firms; as a result of SOX, top company management must now individually certify the accuracy of financial information, penalties for fraudulent financial activity were significantly increased, the independence of the outside auditors who review the accuracy of corporate financial statements was increased, and the oversight role of boards of directors increased; SOX requires covered entities to establish controls to protect financial data, including during disaster recovery operations

Security breach an act from outside an organization or entity that bypasses or contravenes internal security policies, practices, or procedures; also known as data breach; a similar internal act is called a "security violation"

Security breach notification the legal requirement in most states in the United States where companies must immediately disclose any security breach to customers, usually in writing

Single point of failure a part of a system that, if it fails, will stop the entire system from working; generally undesirable in any system with a goal of high availability or reliability, be it a business practice, software application, or other industrial system

Social engineering in the context of information security, any number of methods used to manipulate people into performing actions or divulging confidential information for the purpose of information gathering, fraud, or gaining computer system access; examples include phishing, baiting, tailgating, and *quid pro quo*

Storage area network (SAN) a dedicated network that provides access to consolidated, block level data storage, primarily used to make storage devices, such as disk arrays, tape libraries, and optical jukeboxes, accessible to servers so that the devices appear like locally attached devices to the operating system

Subject-matter expert (SME) a person who is an expert in a particular area or topic; also known as "domain expert"

Succession planning a process for identifying and developing internal people with the potential to fill key business leadership positions in the company, with the purpose of increasing the availability of experienced and capable employees that are prepared to assume these roles as they become available

System development lifecycle model (SDLC) a process of creating or altering information systems, and the models and methodologies that people use to develop these systems, involving stages such as preliminary analysis, requirements definition, design, development, integration and testing, acceptance, installation, deployment, and maintenance

Terrorism the systematic use of terror, often violent, especially as a means of coercion

- Theft (data)** the intentional or unintentional copying of secure information to an untrusted environment
- Threat (computer)** any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service; also, the potential for a threat-source to successfully exploit a particular information system vulnerability
- Training** used in BC/DR planning, the systematic participation of employees and other BC/DR plan resources in regular “dry run” exercises designed to convey necessary information required during an actual emergency or disaster
- Trigger** in BC/DR planning, the criteria or threshold, which if met, requires activation of the plan; e.g., in an unplanned outage, the expectation of maximum tolerable downtime (MTD) being exceeded for a critical business process can trigger activation of a BC/DR plan; widespread disasters are also common triggers for plan activation
- U.S. Centers for Disease Control and Prevention (CDC)** a U.S. federal agency under the Department of Health and Human Services, headquartered in Atlanta, Georgia, whose main goal is to protect public health and safety through the control and prevention of disease, injury, and disability
- Uninterruptible power supply (UPS)** an electrical apparatus that provides emergency power to a load when the input power source, typically the main power grid, fails; differs from an auxiliary or emergency power system or standby generator in that it will provide near-instantaneous protection from input power interruptions, by supplying energy stored in batteries or a flywheel
- Upstream loss** loss of data transmission or interconnection from other system to current system, rendering current system partially or wholly nonfunctional
- Value-added reseller (VAR)** a company that adds features or services to an existing product, then resells it to end users as an integrated product or complete “turn-key” solution; the added value can come from professional services such as integrating, customizing, consulting, training, and implementation
- Vital** in BC/DR planning, necessary to the existence or continuance of a business’ operation
- Vulnerability** the susceptibility of an organization or community to a hazard and the prevailing condition, including physical, socioeconomic, and political factors that adversely affect its ability to respond to hazards or disaster events
- Vulnerability (computing)** a weakness which allows an attacker to reduce a system’s information assurance, comprised of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw
- Vulnerability assessment** the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system; in BC/DR planning, assessing the threats from potential hazards to a company’s employees and infrastructure
- Warm backup site** a compromise between a hot and a cold backup site, where hardware and connectivity are already established, though on a smaller scale than the original production site or even a hot site; warm sites will have backups on hand, but they may not be complete and may be between several days and a week old (e.g., backup tapes sent to the warm site by courier)
- Work breakdown structure (WBS)** a deliverable-oriented decomposition of a project into smaller components (product, data, service, or any combination), which defines and groups a project’s discrete work elements in a way that helps organize and define the total

work scope of the project, and also provides the necessary framework for detailed cost estimating, schedule development, and control

Work recovery time (WRT) after recovery of a system, the time required to recover lost data, re-establish upstream or downstream integration points or dependencies, input work backlog and test system/data before normal operations resume; WRT + RTO = MTD (maximum tolerable downtime)

Workplace violence violence, usually in the form of physical abuse or threat, that creates a risk to the health and safety of an employee or multiple employees

Written information security program (WISP) a legal term referring to a written document which describes how an organization implements measures that are reasonable and designed to achieve the desired security objectives as written in laws and regulations, and how you employ an ongoing, repetitive process which identifies new developments and threats, assesses risk, identifies and implements appropriate security measures, and verifies implementation

This page intentionally left blank

Index

Note: Page numbers followed by *f* indicate figures and *t* indicate tables.

A

ABC Energy Corporation. *See* Business continuity and disaster recovery (BC/DR)
Accountable care organizations (ACOs), 284–285
ACOs. *See* Accountable care organizations (ACOs)
Activation phase, BC/DR plans
 creation and maintenance, 378
 developing triggers, 379–380
 intermediate disaster/disruption, 377–378
 major disaster/disruption, 378
 minor disaster/disruption, 376–377
 to recovery, 380–381
 response and notification, 376
 size and nature, company, 378–379
Application Recovery Statement (ARS)
 checklists, 127
 instructions, 127
 parts, 126–127
ARS. *See* Application Recovery Statement (ARS)
Audits, BC/DR plan
 checklist, 514
 definition, 499
 description, 519
 IT systems and security, 499–501
 and standard project, 513–514
 training and testing, 513

B

BC. *See* Business continuity (BC)
BC/DR. *See* Business continuity and disaster recovery (BC/DR)
BC/DR plans
 activation phase (*see* Activation phase, BC/DR plans)
 additional resources, 407
 administrative support team, 386
 analysis and planning activities, 370
 appendices, 406–407
 audits (*see* Audits, BC/DR)
 change control, 404–405
 CMT, 384–385
 communications plans (*see* Communications plans)
 contact information, 390–392
 damage assessment team, 385
 definition, 369–370

development, 114, 371, 371*f*
distribution, 405–406
emergency preparations, 114
equipment and supplies, 388–389
event logs, 403–404
fire/flood, 382–383
HR team, 387
impact analysis, 113
implement risk mitigation strategies, 371–375
ISO/COBIT, 369–370
IT team, 386
legal affairs team, 387–388
maintenance/review phase, 115, 383
management, 385
media relations team, 387
network configuration, 382–383
operations assessment team, 385–386
phases, 375–383, 409
physical/personnel security team, 388
plan maintenance (*see* Plan change maintenance)
progress, 52, 52*f*, 113*f*
project close out
 business operations, 516
 description, 519
 steps, 515–516
 workable roadmap, 515
project definition, risk assessment, 113, 118–119
recovery to continuity, 381–382
risk mitigation strategies, 114
tasks and resources
 acquisition and testing, 394–395
 cloud services, 395–396
 comparison process, 394
 contractual terms, 394
 description, 410
 functional and technical requirements
 development, 397
 requirements identification, 398–399
 selection criteria, 393–394
 service levels, 397–398
 vendor options identification, 399
 vendor proposal/response to requirements, 398
team guidelines, 389–390
training, testing and auditing, 114–115
transportation and relocation team, 386–387
undamaged equipment, 382
WBS, 112–113, 370

- BCP. *See* Business continuity planning (BCP)
- BIA. *See* Business impact analysis (BIA)
- BIA report preparation
- criticality, data, 269–270
 - risk assessment, 269
 - risk mitigation strategies, 269–270
- Bring-your-own-device (BYOD) legal issues, 40
- Business continuity (BC), 444–446
- Business continuity and disaster recovery (BC/DR)
- availability solutions, 20–21
 - BCP, 2
 - business impact analysis, 22
 - components, 26
 - cost, planning vs. failure, 11–17
 - data availability requirements, 354
 - definition, 25–26
 - disaster types
 - accidents and technological, 18
 - human-caused, 18
 - natural, 18
 - disastrous events, 24
 - emergency preparedness training, 7
 - financial industries (*see* Financial services)
 - hardware or system failures, 6–7
 - human-caused disasters, 6–7
 - implementation stage, 7
 - information resources, 20–21
 - maintenance strategy, 22–23, 337, 338f
 - multiple layers, systems, 6–7
 - plan development, 23
 - plan maintenance, 23–24
 - planning and implementation, 6
 - planning efforts, 150
 - planning projects, 2–3
 - PM tools, 25
 - process, 8–9
 - project initiation, 21–22
 - recovery cycle, 4, 5f
 - redundant system, 3–4
 - reliable system design, 19–20
 - requirements, IT governance
 - application recovery procedures, 126–127
 - definition, 124–125
 - IT service level definition, 125–126
 - risk assessment, 22
 - risk avoidance, 340–341
 - and risk mitigation strategies (*see* Risk mitigation process)
 - steps, 20–21, 21f
 - subject matter, 19, 20f
 - technology, 10–11
 - testing
- recovery, actual incidents, 143–144
- scheduled BC/DR tests (*see* Scheduled BC/DR tests)
- training, testing and auditing, 23
- types, companies, 25
- Business continuity planning (BCP)
- business disruption, 3–4
 - continuous availability, 3–4
 - disaster recovery, 4
 - redundant systems, 3–4
- Business impact analysis (BIA)
- BC/DR plan, 226–227
 - business function and criticality matrix, 255–256, 256t
 - data gathering, 249–254
 - data points, 256, 257t
 - definition, 192, 272
 - disruption, 254–255
- human impact
- DBA, 231
 - financial losses, 230
 - human needs, 231–232
 - succession planning, companies, 230
 - identification, business functions, 241–248
 - impact criticality, 232–241
 - inputs, 219
 - mission-critical business processes, 226
 - mission-critical functions, 270
 - MTO, 227
 - nonmonetary effect, 227–229
 - optimal point, planning, 270–271
 - phase, 225, 226f
 - preparation, report, 268–270
 - risk assessment phase, 225, 226f
 - risk mitigation strategies, 256–260
 - RTOs, 270
 - type, data points, 256
 - upstream and downstream losses, 229–230
- Business requirements, 107–109
- BYOD legal issues. *See* Bring-your-own-device (BYOD) legal issues

C

- CAB. *See* Change Approval Board (CAB)
- Cardiovascular imaging systems (CVIS), 285
- CDC. *See* Centers for Disease Control (CDC)
- Center for Information Technology Leadership (CITL), 276
- Centers for Disease Control (CDC), 183–184
- Centers for Medicare and Medicaid Services (CMS), 289–290
- Change Approval Board (CAB), 130

- CIA. *See* Confidentiality, integrity and availability (CIA)
- CIRP. *See* Cyber incident response plan (CIRP)
- CIRT. *See* Computer incident response team (CIRT)
- CITL. *See* Center for Information Technology Leadership (CITL)
- Cloud DR
- applications and managed DR, 464
 - back up and restore, 464, 465
 - bandwidth requirements, 461
 - DR options, 462–465
 - IT decision-makers/influencers, 461–462
 - PaaS, 460
 - products and services, 460
 - ROBOs, 465–468
 - RPOs, 465
 - shortcomings and challenges, 461
 - SMB case studies
 - Amazon Web Services, 469–470
 - BUMI, 471–472
 - cloud backup, 473–474
 - DR service provider, 472
 - Psomas, 471
 - snapshot-based cloud backup, LAUSD, 470–471
 - snowmageddon and snowpocalypse, 469
 - SMB cloud adoption, 461–462
 - and storage hardware, 460
- CMS. *See* Centers for Medicare and Medicaid Services (CMS)
- CMT. *See* Crisis management team (CMT)
- Co-location Data Center
- cost, 458
 - description, 476
 - internal capability and cost, 459–460
 - selection, provider, 457–458
 - value, 457
- Common security framework (CSF)
- HITRUST, 324–325
 - ISO/IEC 27000 series, 324
 - ITIL, 325
 - National Institute of Standards and Technology, 324
- Communications plans
- community and public, 401–402
 - customers and vendors, 401
 - description, 410–411
 - employee, 400–401
 - internal, 400
 - shareholders, 401
- Components, project planning
- estimates, 69–70
- formation, project team, 71–74, 117
- negotiation, BC/DR Budget, 64
- objectives, 63–64
- potential solutions, 66
- problem and mission statement, 65
- project proposal, 68
- requirements and constraints, 66–67
- sponsor, 70–71
- success criteria, 67–68
- WBS, 64
- Computer incident response team (CIRT)
- alert and mobilize, 442–443
 - assess and stabilize, 443
 - attack/incident, 441
 - day-to-day responsibilities, 444
 - IT departments, 441
 - monitor, 442
 - network permissions, 441–442
 - resolve, 443
 - review, 443–444
 - terms and acronyms, 444
 - training, 441
- Confidentiality, integrity and availability (CIA)
- blocks, information security, 191
 - protection, 161–162
- Confidentiality, integrity, and availability (CIA), 278–279
- Continuity of operations plan, 75
- Cost, planning *vs.* failure
- BC/DR plan, 11–12
 - disasters plan, 13
 - emergencies and disasters, 14
 - evolution, IT architecture, 14
 - minor disaster recovery procedures, 12–13
 - non-IT elements, 12–13
 - people, 15–16
 - process, 16–17
 - technology, 17
 - time and resources, 14–15
 - top and bottom-line growth, 11
- Crisis communication plan, 75–76
- Crisis management team (CMT)
- communications, 433–435
 - emergency response and disaster recovery, 433
 - finance, 436
 - human resources, 435
 - insurance, 436
 - legal, 436
 - review and management, 433
- CRM. *See* Customer relationship management (CRM)

- Customer relationship management (CRM), 88, 89, 102–103
- CVIS.* *See* Cardiovascular imaging systems (CVIS)
- Cyber assets
- annual review recovery plan, 148
 - and CIP, 148–149
 - definition, 148
 - NERC CIP Reliability Standards, 134
- Cyber incident response plan (CIRP), 76
- Cyber threats
- availability, 191
 - BIA, 192
 - CIA, 191
 - confidentiality, 191
 - customer impersonation, 422
 - cyber crime
 - categorization, 194
 - security resources, 193
 - financial services industry, 422
 - “hacktivist” groups, 422
 - information security, 423–424
 - integrity, 191
 - IT system failure-theft, sabotage and vandalism, 195
 - loss of records/data-theft, sabotage and vandalism, 194–195
 - MIT technology review, 423
 - phishing and pharming, 423
 - PWC report, 423
- D**
- Database administrator (DBA), 231
- Data gathering
- definition, 272
 - enthusiastic response, 249
 - interviews, 252–253
 - qualitative and quantitative cost descriptions, 249
 - questionnaires, 251–252
 - workshops, 253–254
- Data security legal obligations
- contributor profile, 43
 - hacking, 44
 - Sony playstation network, 44
 - State laws, 45–47
- DBA.* *See* Database administrator (DBA)
- Disaster recovery (DR). *See also* Business continuity and disaster recovery (BC/DR)
- activation and emergency response checklists, 437
 - description, plan, 75
 - IT tasks (*see* IT recovery tasks)
 - recovery checklists, 437–438
 - SMBs (*see* Small- to medium-sized businesses (SMBs))
- Disparate systems interoperability
- billing and payment systems, 317
 - definition, 330
 - diagnostic imaging, 316
 - EMR, 315–316
 - environmental services, 316–317
 - food services applications, 316
 - HR, 318
 - medical equipment, 316
 - payroll systems, 317
- DRaaS.* *See* DR-as-a-Service (DRaaS)
- DR-as-a-Service (DRaaS)
- and RaaS, 463
 - subscription, 452
 - telecommunications and hosting companies, 472
- E**
- Earthquakes
- likelihood *vs.* impact, 179–180
 - map, U.S. Geological Survey, 178–179, 178*f*
 - preparedness plans, 179–180
- EHRs. *See* Electronic Health Records (EHRs)
- Electrical storms, 175–176
- Electronic Health Records (EHRs), 281
- Elements, project success
- executive support
 - budgets and capabilities, 55–56
 - business terminology, 55–56
 - gain, 54
 - management, 117
 - objectives, 57–58
 - planning phases, 60
 - PM process, 61–63
 - requirements, 58–59
 - scope, 59–60
 - shorter schedule and multiple milestones, 61
 - user involvement, 56
 - experienced project manager, 56–57
- Emergency response and recovery
- business continuity, 444–446
 - CMT (*see* Crisis management team (CMT))
 - DR activities, 427
 - ERT, 430–432
 - local emergency responders, 427
 - management, 428
 - plans, 428–430
- Emergency response teams (ERT)
- BC/DR activation, 431
 - communication equipment, 431
 - definition, 430
 - roles and responsibilities, 432
 - safety and effectiveness, 431

- skills, 432
 team hierarchy, 430, 431f
 training, 431–432
- Enterprise resource planning (ERP)
 application, 89
 availability, 67–68
- ERP. *See* Enterprise resource planning (ERP)
- ERT. *See* Emergency response teams (ERT)
- F**
- Fair Credit Reporting Act (FCRA), 29, 34
 FCRA. *See* Fair Credit Reporting Act (FCRA)
- FDA. *See* Food and Drug Administration (FDA)
- Federal laws, data security
 infrastructure cyber security, 49
 U.S. House, representatives proposed bill, 48
 U.S. senate response, 49
- Federal Trade Commission (FTC), 33, 34, 40
- Financial services
 business continuity, 416
 cost and administration, 424
 cost-effective DR solutions, 424
 cyber threats, 422–424
 desktop virtualization, 424
 EU regulation, 415
 Hurricane Sandy, 420–422
 industry impact (*see* September 11 attacks)
 IT departments, 424–425
 regional and worldwide financial activities, 415
 regulatory bodies, 413
 September 11 attacks (*see* September 11 attacks)
 United States regulation, 414–415
- Fire
 causes, 169–170, 171
 chemical suppression systems, 171
 human-caused, 185
 insurance, 170
 prevention and protection measures, 170
- FM-200 dry fire suppression, 135
- Food and Drug Administration (FDA)
 computer technology, 290
 disaster plan, 292
 medical devices, 290
 medical equipment vendors, 290
 patient monitoring system, 291
 recovery solutions, 292
 server hardware, 292
 server software, 290
 vendor hardware architecture, 291
 Windows mobile OS, 291
- FTC. *See* Federal Trade Commission (FTC)
- Functional requirements
 billing system, 110
 definition, 109
 ranking systems, 110–111, 110t
- G**
- Gravest short-term threat, 196–197
- H**
- Health Information and Management Systems Society (HIMSS), 300
- Health information management (HIM)
 medical records, 313
 operational business process scoring matrix, 312, 312t
- Health information exchanges (HIEs)
 and ACOs, 284–285
 BC/DR discovery, 284
- Health information technology (HIT)
 admitting, 310–311
 ambulatory clinics, 279
 applications and business entities, 280
 architecture, 299–310
 behavioral health facility, 280
 CITL, 276
 clinical care
 nursing, 314
 physician, 313–314
 support services, 314–315
 clinical outcome, 276
 communication and integration, 277
 communications systems, 322–323
 consumer-driven healthcare, 286–287
 data storage and replication, 318–319
 definition, 328
 economic downturn, 276
 EMR, 275
 governmental incentives and penalties, 281–283
 HIEs, 283–285
 hospitals, 278
 insurance verification and billing services, 310–311
 interoperability, disparate systems, 315–318
 legal and risk management, 276–277
 and medical equipment, integration, 285–286
 mitigation strategies, 288
 mobile devices, 319–320
 nursing and clinical leadership, 276–277
 organizations, 280
 patient care, 326–328

- Health information technology (HIT) (*Continued*)
- patient monitoring data, 288
 - pharmacies, 279
 - physician offices, 278–279
 - real-time data, 287–288
 - regulatory environment, 289–296
 - rising cost, 280–281
 - risk management
 - facilities management systems, 299
 - organizational solvency, 298–299
 - patient care, 298
 - patient safety, 297–298
 - security frameworks, 323–325
 - SNFs, 278
 - type, solution, 277
 - virtual desktop infrastructure, 320
 - virtualization and cloud computing, 320–322
- Health Information Technology for Economic and Clinical Health (HITECH), 294–295
- Health Insurance Portability and Accountability Act (HIPAA)
- electronic data, 293–294
 - elements, 292–293
 - health information, 293
 - PHI, 293
 - reality, information security, 294
 - security rule, 293
- HIEs. *See* Health information exchanges (HIEs)
- HIMSS. *See* Health Information and Management Systems Society (HIMSS)
- HIPAA. *See* Health Insurance Portability and Accountability Act (HIPAA)
- HIT. *See* Health information technology (HIT)
- HITECH. *See* Health Information Technology for Economic and Clinical Health (HITECH)
- Human resources (HR) systems, 99, 318
- Hurricane Sandy
- BC/DR efforts, financial industry, 421–422
 - DR sites, 421
 - and earthquakes, 421
 - financial companies, 420
 - IT technologies, 420
 - and NYSE, 421
 - staff lacked power, 421
 - super storms, 420
 - surveyed metrics, 420–421
- Hurricanes/typhoons/cyclones
- definition, 180–182
 - storm, 181
 - Superstorm Sandy, 181
- I
- ICS. *See* Industrial control system (ICS)
- Identification, business functions
- facilities and security, 242–243
 - finance, 243–244
 - human resources, 244–245
 - IT, 245
 - legal/compliance, 245–246
 - manufacturing (assembly), 246
 - marketing and sales, 246–247
 - operations, 247
 - research and development, 247
 - warehouse, 248
- Impact criticality, BIA
- business functions and processes, 234
 - critical functions, 233
 - desirable functions, minor, 234–235
 - essential functions, vital, 233–234
 - recovery time requirements
 - BC/DR planning process, 241
 - data collection processes, 237
 - disruption and recovery, 238
 - disruption and recovery relationship, 239–240, 239f
 - end-to-end business impact analysis, 240, 240f
 - hardware cluster, 238
 - mission-critical business systems, 237–238
 - mission-critical systems, 238
 - MTD, 235
 - optimal recovery point, 238
 - RPO, 236
 - RTO, 236
 - WRT, 236
- Industrial control system (ICS)
- description, 140
 - EMS SCADA and generation DCS systems, 141
 - government regulation, 141
 - low-cost Internet Protocol devices, 140
 - reliability, 141
 - risk management and contingency planning, 142
- Information gathering methods, 168–169
- Information security management
- responsibility, 37–38
 - WISP (*see* Written information security program (WISP))
- Information technology (IT)
- ability, communication, 97
 - ability to work well, people, 97–98
 - business functions, 261
 - and critical business experience, 98
 - critical business functions and processes, 268
 - critical business processes, 268

- developing data and business function map, 260
- example, business process, 263, 263t
- experience working, cross-departmental team, 97
- MTD, 268–269
- operational impact-warehouse fire, 265, 266t
- optimal mitigation strategies, 268
- project communication, 98
- recovery objectives, 268
- risk scenarios, 268
 - small business financial impact, 264, 265t
- Information Technology Information Library (ITIL), 325
- Information Technology Laboratory, 283–284
- Information Technology Service Management (ITSM), 325
- Infrastructure threats
 - building-specific failures, 195–196
 - causes, 220
 - definition, 195
 - disruption, oil/petroleum supplies, 197
 - food/water contamination, 197–198
 - loss, utilities, 196–197
 - organizational disaster preparedness, 199
 - public transportation disruption, 196
 - regulatory/legal changes, 198–199
- IT. *See* Information technology (IT)
- IT architecture
 - business systems
 - administrative and financial systems, 301
 - automated building controls, 302
 - financial systems, 302
 - healthcare-related business system, 302
 - supply chain management systems, 302
 - clinical systems
 - clinical applications, 300–301
 - definition, 300
 - healthcare organization, 301
 - lab system, 300
 - quality systems, 301
 - data protection, 299–300
 - datatype
 - semi-structured, 303–304
 - structured, 303
 - unstructured, 303
 - definition, 329–330
 - electronic data, 299–300
 - HIMSS, 300
 - planning stages, acquisition, 299–300
 - storage demand, 299
 - types, systems and storage
 - assessment and recovery tasks, 305
 - clinical systems, 304
- configuration files, 305
- data center, 304
- end user devices, 309–310
- life support equipment, 304
- medical identity theft, 309
- medical network, 306
- network connectivity, guests, 306–307
- network core, 305–306
- RFID, 307–308
- RTLS, 307–308
- security infrastructure, 308–309
- technical support and sales, 304
- wireless network, 307
- IT backup and recovery strategies
 - business processes, 358–359
 - description, 367
 - documentation, risk mitigation, 364–365
 - recovery systems
 - cold site, 361
 - desktop solutions, 362–363
 - fully mirrored site, 359–360
 - hot site, 360
 - malware, 364
 - mobile site, 360–361
 - reciprocal site, 361
 - software and licensing, 363
 - storage and disk systems, 361–362
 - warm sites, 360
 - web sites, 363–364
- IT Governance
 - application recovery procedures
 - ARS, 126–127
 - documented dependencies, 126–127
 - BC/DR plans, 123
 - BC/DR requirements
 - documents, 124–125
 - face-to-face discussions, 125
 - IT Operations and Security groups, 125
 - Payroll Department, 125
 - Requirements document, 124, 125
 - discretionary funding, 123
 - service level definition, 125–126
- IT recovery tasks
 - BC/DR plan, 438
 - CIRT (*see* Computer incident response team (CIRT))
 - CMT, 439–440
 - infrastructure checklist, 438–439
 - IT DR team, 440
 - IT-related dependencies, 440
 - network and systems infrastructure, 438–439
 - RTO, 439–440

- IT risk mitigation
 data and records, 356
 description, 367
 systems and infrastructure, 356–358
- IT-specific risk management
 definition, 161–162
 medium-to-large organizations, 162
 NIST, 162
 objectives, 162–163
 PCI, 162
SDLC (see System development lifecycle (SDLC) model)
- L**
- Legal and regulatory obligations, data and information security
 BYOD, 40
 direct financial losses, 30–31
 FCRA, 29
 FTC, 34, 40
 HIPAA regulations, 32
 identity theft, 33
 loss/disclosure, sensitive personal information, 31
 management (*see* Information security management)
 PRC, 33
 protections, 33–34, 41
 “reasonable security”, 35–36
 requirements, 30
 security breach notification, 36–37
 security laws, regulations and guidelines directory, 35
- M**
- Maximum tolerable downtime (MTD), 235
 Maximum tolerable outage (MTO), 227
 Medical equipment, integration
 information systems, 286
 life support, 286
 medical laboratory, 286
 monitoring, 285–286
 therapeutic, 285
 MIA. *See* Missing in action (MIA)
 Missing in action (MIA), 71
 MTD. *See* Maximum tolerable downtime (MTD)
 MTO. *See* Maximum tolerable outage (MTO)
- N**
- National Institute of Standards and Technology (NIST)
 definition, 162
 likelihood matrix, 208, 208*f*
 publications, 163
- Natural and environmental threats
 Avian Flu/pandemics
 CDC, 183–184
 definition, 183
 drought, 177
 earthquakes, 178–180, 178*f*
 electrical storms, 175–176
 fire, 169–171
 floods
 buildings, 172
 causes, 171–172
 emergency lighting systems, 173
 federal and state governments, 172
 hurricanes/typhoons/cyclones, 180–182
 severe winter storms
 cold temperature, 174
 disruption, business, 174
 heavy snow and ice, 174
 weather warnings, 175
 tornados, 180
 tsunamis, 182
 volcanoes, 182–183
- NERC CIP. *See* North American Electric Reliability Corporation’s Critical Infrastructure Protection (NERC CIP)
 NERC CIP-009 recovery testing, 148–149
 NIST. *See* National Institute of Standards and Technology (NIST)
 North American Electric Reliability Corporation’s Critical Infrastructure Protection (NERC CIP), 134, 141–142, 143, 148
- O**
- Occupant emergency plan, 76–77
 On-premise DR
 description, 475
 IT system, 454–455
 operating expenses, 453–454
 preventative measures, 454
 recovery strategy, 455
 scenarios, 454
 SMB case studies
 affigent LLC, 456
 24 Seven Talent company, 455–456
 Open System SnapVault (OSSV), 137–138
 Oracle Sun Sparc servers, 136
 OSSV. *See* Open System SnapVault (OSSV)
 Outage Management System (OMS)
 application server, 139
 back-end Oracle database, 139
 description, 139
 IT support staff, 139, 140

P

PaaS. *See* Platform-as-a-Service (PaaS)

PACSs. *See* Picture archiving and communication systems (PACSs)

Parametric estimation, 69–70

Payment Card Industry (PCI), 162

Payment Card Industry Digital Security Standards (PCI DSS)

- AuthorizeNet, 295–296
- cardholder data, 295
- data security methods, 295
- information security policy, 296
- network resources, 296
- revenue sources, 296
- vulnerability management program, 296

PCI. *See* Payment Card Industry (PCI)

PCI DSS. *See* Payment Card Industry Digital Security Standards (PCI DSS)

Personal health information (PHI), 319

Phased approach, 61, 101–102

PHI. *See* Personal health information (PHI)

Picture archiving and communication systems (PACSs), 285

Plan change maintenance

- activities, 514–515, 519
- changes, IT, 507–508, 511–512
- corporate changes, 509
- description, 518
- evaluate and incorporate change, 512–513
- iterative process, 506–507
- legal, regulatory/compliance changes, 510
- monitor change

 - people, 511
 - process, 511
 - technology, 511–512

- operations changes, 508–509
- steps, 506, 506*f*
- strategies, management, 510
- training, testing, and auditing, 507

Platform-as-a-Service (PaaS)

- DRaaS and RaaS, 463
- DR scenario, 463
- and IaaS, 463

PM. *See* Project management (PM)

Population management, 281

PR. *See* Public relations (PR)

PRC. *See* Privacy Rights Clearinghouse (PRC)

Privacy Rights Clearinghouse (PRC), 33, 41

Processes, project

- change control, 88–89
- escalation, 87
- progress, 88

quality control, 89

repeatable, 86

reporting, 86–87

team meetings, 86

Project communications plan, 89–90

Project initiation

- BC/DR plans (*see* BC/DR plans)
- business requirements, 107–109
- definition, 51–52, 106–107
- elements, project success, 52–63
- facilities/security, 99–100
- factors, 116
- finance/legal, 100–101
- functional requirements, 109–111, 110*t*
- HR, 99
- information technology, 96–99
- management

 - change, 94
 - progress, 93

- marketing and sales, 102–103
- operations, 105–106
- organization (*see* Project organization)
- PR, 103–105
- project close out, 95–96
- purchasing/logistics, 102
- technical requirements, 111–112, 111*f*
- tracking, 94–95
- warehouse/inventory/manufacturing/research, 101–102

Project management (PM)

- BC/DR planning process, 21
- certified, 52
- IT methodologies, 23
- process

 - Lean, Agile and BC/DR, 62
 - small companies, plans, 62–63
 - solution determination, company's needs, 62–63

- tools, 25
- training and skills, 25

Project organization

- budget reduction, project plan, 81, 81*f*
- communications plan, 89–90
- designation, parameter, 84
- document concerns, 83
- infrastructure, 84–85
- least flexible parameter, 83
- most flexible parameter, 83
- objectives

 - business continuity plan, 74
 - CIRP, 76
 - continuity, operations plan, 75

- Project organization (*Continued*)
 crisis communication plan, 75–76
 disaster recovery plan, 75
 occupant emergency plan, 76–77
 processes (*see* Processes, project)
 quality, 82
 reduction, schedule, 81–82, 82*f*
 requirements, 78–80
 scope, budget, schedule and quality, 81, 81*f*
 stakeholders, 77–78
- Project schedule, 92
- Project sponsor
 BC/DR project, 70–71
 definition, 70
 MIA, 71
- Project team formation
 logistical components, 73
 organizational chart, 72
 political aspect, crisis management, 73–74
 technical specialties, 72–73
- Project tracking, 94–95
- Public relations (PR), 103–105
- Q**
- Qualitative threat assessment
 customized scale, 207, 207*t*
 five-element, single-rating system, 210, 210*f*
 likelihood, adverse impact, 211, 212*t*
 likelihood, event, 211, 212*t*
 NIST likelihood matrix, 207, 208, 208*t*
 power outage, 208, 208*f*
 refined scale, 210, 210*f*
 scales, overall likelihood, 211, 212*t*
 total risk value, power outage, 209, 209*f*
 triage, 207
- Quantitative threat assessment
 benefits, 221
 creation, 204
 definition, 203
 risk assessment methodology, 204, 204*f*
 small business, 205
 total risk cost, power outage, 205, 206*f*
 triage, 207
- R**
- Radiology information systems (RIS), 285
- Recovery checklists, 437–438
- Recovery point objectives (RPOs)
 application awareness, 465
 requirements, 452
- Recovery time objective (RTO), 236, 439–440
- Regional health information organizations (RHIO), 283–285
- Regulatory environment
 CMS, 289–290
 FDA, 290–292
 healthcare organizations, 289
 HIPAA, 292–294
 HITECH, 294–295
 PCI, 295–296
 state and local requirements, 296
 types, requirements, 289
- Reliable system design, 19–20
- Remote and branch offices (ROBOs)
 deploy application acceleration and WAN optimization, 468
 description, 465
 virtualize and consolidate servers, 466
 virtualize and streamline data storage and backup, 466–467
 virtualize applications and desktops, 467–468
- RHIO. *See* Regional health information organizations (RHIO)
- RIS. *See* Radiology information systems (RIS)
- Risk assessment
 activities, 151
 BC/DR progress, 151–152, 152*f*
 human threats
 chemical/biological hazards, 189–190
 cyber threats, 190–195
 fire, 185–186
 labor disputes, 187
 terrorism, 185, 188–189
 theft, sabotage and vandalism, 186–187
 war, 190
 workplace violence, 187–188
 information gathering methods, 168–169
 management (*see* Risk management)
 natural and environmental threats (*see* Natural and environmental threats)
 power outage, 166–167
 reduction, 152
 threats
 assessment subprocess, 167, 168*f*
 checklist, 199, 200*r*
 infrastructure, 195–199
 IT-specific, 199, 201*t*
 methodology (*see* Threat assessment methodology)
 organize, data, 199, 201*t*
 output, 199, 201*f*
 sources, 167
 vulnerability (*see* Vulnerability assessment)

Risk management
 vs. assessment boundaries, 154, 154f, 155
 certification, 155
 cost and benefit, 156
 definition, 153
 framework, SDLC model, 221
 impact assessment, 158
 infrastructure, 161
 IT (*see* IT-specific risk management)
 magnitude and frequency, 156
 mitigation strategy development, 158–159
 opportunity costs, 155–156
 people, 159–160
 process, 160
 technology, 160–161
 threat assessment, 156–157
 vulnerability assessment, 157–158

Risk mitigation process
 acceptance, 340
 access, documentation
 backup procedures, 128–129
 central location, documentation, 128–129
 IT projects, 130
 tapes, off-site copy, 129–130
 avoidance
 limitation, 341
 transference, 341–342
 backup and recovery considerations, 358–365
 BC/DR, 337, 338f
 and BIA data, 337
 BIA phases, 337–339
 business function, 353
 CAB, 130–131
 compute and data
 database recoverability, 138
 NetApp storage systems, 138
 Novell's PlateSpin tool, 136
 Oracle Sun Solaris, 137–138
 production systems, 136
 server virtualization and shared network-
 attached storage, 137
 shared enterprise storage, 138
 virtualization technologies, 135–136
 virtual server instances, 136–137
 VMotion and HA, 137
 data center and network, 134–135
 description, 366–367
 development phase, 337
 disaster recovery, 128
 disk mirroring, 353
 ICS, 140–142
 IT, 355–358

mitigation phase details, 337, 338f
 people, buildings and infrastructure, 354–355
 recovery options
 comparison, approaches, 343–344
 cost vs. capability, 347
 data and requirements, 343–344
 as needed, 345
 prearranged options, 345
 preestablished, 345–346
 recovery time of options, 346
 review existing controls, 349–350
 SLAs, 347–349
 recovery requirements, 343
 relationship, time and cost, 339, 339f
 security control baselines and change detection
 network vulnerabilities, 134
 Tripwire, 134
 security control testing
 cost vs. benefit, 131–132
 Tripwire, 131–132
 self-service application failover and failback,
 139–140
 separation of duties, 132
 types, 365–366
 vulnerability assessment
 centralized security, 132–133
 IT network, 133

Risk mitigation strategies implementation
 antivirus and antimalware software, 371
 available resources, 371–373
 earthquake/flood, 374–375
 likelihood, occurrence, 374–375
 operational elements, 375
 tasks and DR, 374, 374f
 vulnerability, 373–374

ROBOs. *See* Remote and branch offices (ROBOs)

RPOs. *See* Recovery point objectives (RPOs)

RTO. *See* Recovery time objective (RTO)

S

Sarbanes-Oxley (SOx) 404 application recovery
 testing, 147–148

Scheduled BC/DR tests
 corporate data center redundancy testing
 network part, test, 146
 storage part, test, 146
 test plan, 145

EMS SCADA EOC testing, 146–147

enterprise business continuity testing, 149

NERC CIP-009 recovery testing, 148–149

SOx 404 application recovery testing, 147–148

- SDLC model. *See* System development lifecycle (SDLC) model
- Security breach laws
- definition, personal information, 45
 - federal laws, 47–49
 - notification procedure, 46
 - penalties, 46
 - safeguarding personal data, 47
- September 11 attacks
- backup data center, 418, 419
 - BC/DR plan, 418
 - electronic records, 419
 - Federal Reserve Board, 417–418
 - global financial community, 419–420
 - untested organizations, 419
 - World Trade Center towers, 417
- Service level agreements (SLAs)
- cost and capabilities, 365
 - elements, 347–349
 - risk mitigation strategies, 349
- Skilled nursing facilities (SNFs), 278
- SLAs. *See* Service level agreements (SLAs)
- Small- to medium-sized businesses (SMBs)
- cloud, DR, 460–474
 - co-location data center, DR, 456–460
 - disaster preparedness, 453
 - DR (*see* Disaster recovery (DR))
 - on-premise DR, 453–456
- SMBs. *See* Small- to medium-sized businesses (SMBs)
- SMEs. *See* Subject matter experts (SMEs)
- SNFs. *See* Skilled nursing facilities (SNFs)
- Solaris' ZFS file system, 136, 137–138
- Subject matter experts (SMEs), 234
- System development lifecycle (SDLC) model
- vs.* Agile methodologies, 163
 - identification, risk, 165–166
 - phases, 163, 164*t*
 - resources, 165
 - web sites, 165
- T**
- Technical requirements, 111–112, 111*f*
- Testing, BC/DR
- cost and feasibility, 496–498
 - gaps/weaknesses identification, 496
 - information flow, 495–496
 - recommendations, 499
 - resources, 495
 - steps, 495
 - task integration, 495
 - test evaluation criteria, 498–499
- and training
- annual walk-through, plan, 490–491
 - checklists usage, 490
 - communication, 487
 - copies, plan, 489
 - definition, 485–486
 - disruption and accuracy, 487, 488*f*
 - ERT/CMT, 486
 - evaluation criteria, 488–489
 - field exercises, 492
 - follow-up meeting, 490
 - functional exercises, 491–492
 - identify training, 490
 - interruption test, 492–493
 - notes, 490
 - participants dividing, 490
 - realistic scenarios development, 488
 - roles and responsibilities, 486
 - team leaders, 485
 - training plan implementers, 493
- understanding of processes, 494–495
- Threat assessment methodology
- qualitative, 207–211
 - quantitative, 203–207
 - types, tools, 222
- Training, BC/DR
- description, 503
 - development, 483–484
 - emergency response, 480–481
 - monitoring and measuring, 484
 - recovery and failure, 481
 - scheduling and delivering, 484
 - scope, objectives, timelines and requirements, 481–482
 - and testing, 485–493
 - training needs assessment, 482–483
- V**
- Value-added reseller (VAR), 310
- VAR. *See* Value-added reseller (VAR)
- Virtualization and cloud computing, HIT
- clinical applications, 321
 - cloud-based storage, 322
 - upstream and downstream systems, 320–321
- Vulnerability assessment
- corporate assets and operations, 223
 - definition, 211–213, 216–217
 - deliverable, 218–219, 219*f*
 - infrastructure, 216
 - people, 214–215
 - phases, SDLC, 217
 - process, 215

risk assessment, 213, 213*f*

risk equation, 218

sample statements, 217–218, 218*t*

technology, 216

W

WBS. *See* Work breakdown structure (WBS)

WISP. *See* Written information security program (WISP)

Work breakdown structure (WBS)

BC/DR plan, 112–113

definition, 91

development, 83

Work recovery time (WRT), 236

Written information security program (WISP)

categorization, 39

education, 39

measures, 39

negligence law and security regulations, 38

requirements, 38–39, 41

third-party service provider arrangements, 39

WRT. *See* Work recovery time (WRT)