Carnegie Mellon
Software Engineering Institute

State of the Practice of Computer Security Incident Response Teams (CSIRTs)

Georgia Killcrece
Klaus-Peter Kossakowski
Robin Ruefle
Mark Zajicek

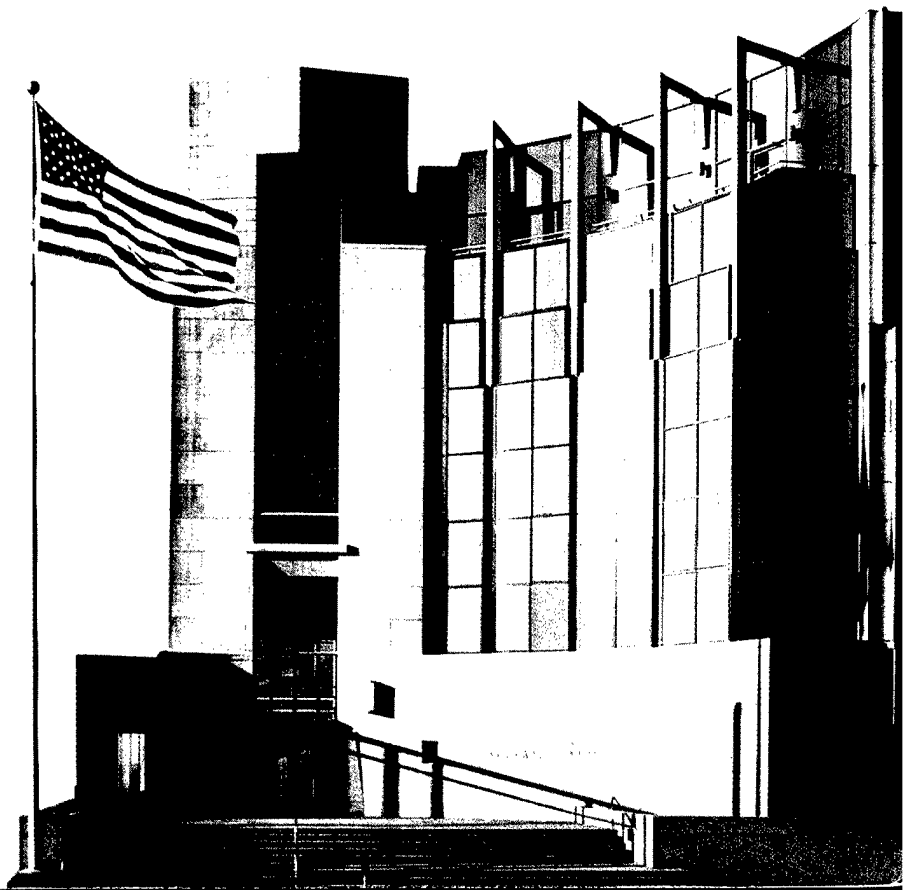
Reproduced From
Best Available Copy

October 2003

20040412 015

DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited

TECHNICAL REPORT
CMU/SEI-2003-TR-001
ESC-TR-2003-001



Carnegie Mellon
Software Engineering Institute

Pittsburgh, PA 15213-3890

State of the Practice of Computer Security Incident Response Teams (CSIRTs)

CMU/SEI-2003-TR-001
ESC-TR-2003-001

Georgia Killcrece
Klaus-Peter Kossakowski
Robin Ruefle
Mark Zajicek

October 2003

Networked Systems Survivability Program

Unlimited distribution subject to the copyright.

This report was prepared for the

SEI Joint Program Office
HQ ESC/DIB
5 Eglin Street
Hanscom AFB, MA 01731-2116

The ideas and findings in this report should not be construed as an official DoD position. It is published in the interest of scientific and technical information exchange.

FOR THE COMMANDER

Christos Scondras
Chief of Programs, XPK

This work is sponsored by the U.S. Department of Defense. The Software Engineering Institute is a federally funded research and development center sponsored by the U.S. Department of Defense.

Copyright 2003 Carnegie Mellon University.

NO WARRANTY

THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

Use of any trademarks in this report is not intended in any way to infringe on the rights of the trademark holder.

Internal use. Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and "No Warranty" statements are included with all reproductions and derivative works.

External use. Requests for permission to reproduce this document or prepare derivative works of this document for external and commercial use should be addressed to the SEI Licensing Agent.

This work was created in the performance of Federal Government Contract Number F19628-00-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.
The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

For information about purchasing paper copies of SEI reports, please visit the publications portion of our Web site (http://www.sei.cmu.edu/publications/pubweb.html).

Table of Contents

Who is the CERT CSIRT Development Team and What Do They Do? ix

Preface xi

Acknowledgements xiii

Abstract xv

1 Introduction 1
- 1.1 Purpose of the Document 3
- 1.2 Scope of the Document 3
- 1.3 Intended Audience 4
- 1.4 Use of this Document 5
- 1.5 Document Structure 6
- 1.6 About the Survey 6
- 1.7 About the Literature Search 8

2 Computer Security Incident Response Teams 11
- 2.1 What is a CSIRT? 11
- 2.2 Types of CSIRTs 14
- 2.3 History and Development of CSIRT Capabilities 17
  - 2.3.1 The Early Beginnings 17
  - 2.3.2 The Creation of FIRST 20
  - 2.3.3 Europe Becomes Involved 21
  - 2.3.4 Initiatives in the Asia Pacific Region 27
  - 2.3.5 Initiatives in Latin America 30
  - 2.3.6 Developments in Canada 32
  - 2.3.7 Developments in the United States 33
  - 2.3.8 Other Initiatives in CSIRT Development and Evolution 34
  - 2.3.9 Today's Activities 35

3 Current State of the Practice of CSIRTs 37
- 3.1 Number and Type of CSIRTs Today 37
  - 3.1.1 The Growth of FIRST Teams 38
  - 3.1.2 Growth in European CSIRTs 39

3.1.3 Total Registered CSIRTs 40
3.1.4 CSIRT Growth by General Category 42
3.1.5 Other Trends 46
3.1.6 The Spread of CSIRTs 47
3.2 CSIRT Organizational Structure 49
3.2.1 Constituency 49
3.2.2 Mission 51
3.2.3 Organizational Placement of the CSIRT 51
3.2.4 CSIRT Authority 53
3.3 Funding and Costs 54
3.3.1 Funding Strategies 55
3.3.2 Budgets 56
3.3.3 Staff Costs 57
3.3.4 The Cost of an Incident 58
3.3.5 Making a Case to Management 62
3.4 Services 65
3.5 Staffing 71
3.5.1 Staff Size 71
3.5.2 Staff Positions 72
3.5.3 Staff Skills 76
3.5.4 Staff Burnout 78
3.6 Training and Certification 79
3.7 Processes 81
3.7.1 Defining Computer Security Incidents and Other Incident Response Terminology 82
3.7.2 Having a Plan 84
3.7.3 Incident Handling Process or Methodology 87
3.7.4 Receiving Incident Data 88
3.7.5 Recording and Tracking CSIRT Data 89
3.7.6 Categorizing and Prioritizing Incident Reports 95
3.7.7 Incident Response Processes 98
3.7.8 Computer Forensics Activities 100
3.7.9 Answering the CSIRT Hotline 102
3.7.10 Hours of Operation 102
3.7.11 Types of Incidents 102
3.7.12 Number of Incidents 104
3.7.13 Secure Communications Mechanisms Used 105
3.7.14 Coordination and Information Sharing 105
3.7.15 Documenting Policies and Procedures 108
3.8 Changes in Intruder Attacks and Tools 109
3.8.1 Impact on Incident Response 112
3.9 Legal Issues and Cyber Crime Laws 114
3.9.1 International Cyber Crime Laws 115

3.9.2 United States Cyber Crime Laws 118
3.10 Current Projects 118
3.10.1 Coordination and Collaboration 119
3.10.2 Standards for Sharing or Collecting Information 122
3.10.3 Incident Data Collection 124
3.10.4 Tools 127
3.10.5 Research 128
3.11 Current Problems 128
3.12 Resources 130
3.12.1 Case Study Examples 130
3.12.2 Sample Templates, Checklists, Process Guides, Flowcharts 130

4 Summary 133

5 Future Work 137

6 Closing Remarks 139

Appendix A CSIRT Organizational Survey 141

Appendix B: Comparison of Incident Response Steps and Processes 151

Appendix C: Training Sources for CSIRTs 157

Appendix D: Cyber Crime Law Resources 165

Appendix E: Sample Incident Reporting Forms and Flowcharts 179

Bibliography 247

Index 259

List of Figures

Figure 1: Multi-Layered Infrastructure Defense 1

Figure 2: Demographics of CSIRT Survey Participants 7

Figure 3: Timeline of Internet Worm Attack and Creation of CERT/CC 19

Figure 4: Growth of FIRST Teams since 1990 39

Figure 5: Growth in Registered Teams by Geographic Distribution 41

Figure 6: Growth by Year of Total Number of Registered CSIRTs 42

Figure 7: Sector Distribution of Registered CSIRTs by Geographic Area 43

Figure 8: Differentiation of Trends in North America and Europe 45

Figure 9: Organizational Sector Representation for 2000–2002 CERT/CC CSIRT Classes 46

Figure 10: Example of Team Sponsorship and Propagation of CSIRTs 48

Figure 11: Constituencies of Survey Participants 50

Figure 12: Budget Ranges for CSIRT Organizational Survey Participants 57

Figure 13: The Incident Life Cycle 87

Figure 14: Attack Sophistication Versus Required Intruder Knowledge 110

List of Tables

Table 1: CSIRT Acronyms and Names 13

Table 2: CSIRT Organizational Models 15

Table 3: List of Founding FIRST Members 21

Table 4: Total Registered European CSIRTs 40

Table 5: Geographical Distribution of Registered CSIRTs 41

Table 6: North American and European CSIRTs by Subcategory 44

Table 7: CSIRT Funding Strategies 55

Table 8: Example of Calculating Incident Costs 60

Table 9: CSIRT Services by Category 66

Table 10: Features of a CSIRT Tracking System 91

Table 11: Sample Incident Reporting Forms and Flowcharts 92

Table 12: Methods of Categorizing and Prioritizing Incident Reports and Activity . 95

Table 13: Severity Levels of the National Hurricane Preparedness Center 97

Table 14: Challenges Faced by CSIRTs 129

Who is the CERT CSIRT Development Team and What Do They Do?

The CERT CSIRT Development Team helps organizations build their own computer security incident response teams (CSIRTs) and also helps existing teams enhance their effectiveness. The team is an outgrowth of the work and products developed in the CERT Coordination Center (CERT/CC). Our focus is to assist new and existing teams in understanding best practices and recommendations for performing incident handling and related CSIRT services. The guidance provided is based on the history and experiences of the CERT/CC, along with knowledge gained from our extensive collaborations with other teams.

To help organizations, we

- develop and teach courses related to CSIRTs
- work with teams to
  - develop strategies to plan and implement CSIRTs
  - develop best practices for operating CSIRTs
  - adopt CSIRT policies and standard operating procedures
- collaborate with teams to develop documents, templates, and checklists to assist in the incident handling process
- license courses to organizations and train their trainers to deliver the materials

For more information, please contact csirt-info@cert.org.

Preface

Since the Internet Worm incident in 1988 triggered the creation of the CERT Coordination Center (CERT/CC), we have seen continued growth in the establishment of CSIRTs. Although these types of organizations may have different names, they all have an equivalent goal: to be a focal point for preventing, receiving, and responding to computer security incidents.

As we have worked with organizations to help them create or expand their incident response capability, we have found that there are certain questions that we are repeatedly asked, including

- How many staff members do I need?
- How much will it cost?
- What services should I provide?
- Where should the CSIRT be located in our organizational structure?
- What are other organizations similar to mine doing?

Our answer to these questions is an honest but usually unsatisfactory "it depends..." It depends on the sector in which the CSIRT is located, it depends on the constituency that is being served and supported, it depends on the CSIRT's mission and scope, it depends on the expertise of the CSIRT staff, it depends on the available funding, and it depends on the measures and approaches already taken for risk and security management in the organization.

Much of the information available today relating to CSIRT structures and costs is anecdotal in nature. Few people that we know of have taken a systematic look at the structure and services of CSIRTs. We wanted to begin to gather empirical data to help us determine if there truly were any standard answers to the above questions. We knew that the answers were still going to include an "it depends..." but we also felt that by collecting this information for existing CSIRTs, we might begin to see some trends we did not expect. We were also interested in seeing if there were common answers to these questions based on the type of CSIRT an organization implemented. As a final goal, we wanted to validate what we thought were the answers to the questions being asked by comparing our findings with existing theories and assumptions. In all, the work we've done on this project will help us better understand the state of existing CSIRT practices and allow us to provide better guidance for new teams and for existing teams seeking to improve their operations.

This document provides a view of the current state of the CSIRT practice as we see it. We recognize that as teams form, mature, and expand their services and capabilities, and as the Internet and intruder threats evolve that CSIRTs practices will also evolve. However, we believe this document is a useful representation of information available at this time. We hope that this will provide guidance to those of you who are establishing CSIRTs or looking to benchmark your existing CSIRT. Certainly it will be available as a basis for any further discussion or research on these topics.

This document will also provide a general reference for teams, with links and information on CSIRT processes, articles and white papers, training materials, and legal issues. *Please note that all information mentioned here is for information purposes only. Inclusion in this report does not constitute an endorsement by the CERT/CC.*

The material in this report is based on the information we have collected through our own experiences, discussions with and observations of other CSIRTs, research and review of existing publications and literature related to CSIRTs and incident response, and the results of a pilot survey of some existing teams. We want to continue to learn, so if you have comments on this document, or if you want to share your opinions or suggest additions to this document, please contact us. We regularly attend FIRST conferences and teach CSIRT courses, and can be contacted in person or reached as a group by sending email to csirt-info@cert.org.

Acknowledgements

We would like to express our deep appreciation to our colleagues in the incident handling community who either reviewed this document or provided information for inclusion in this document.

- Andreas Bunten, DFN-CERT
- Andrew Cormack, UKERNA
- John Green, JANET-CERT
- Cristine Hoepers, NBSO/Brazilian CERT
- Yurie Ito, JPCERT Coordination Center
- Juan Carlos Guel Lopéz, UNAM-CERT
- Rob McMillan, Commonwealth Bank of Australia
- Liliana Velásquez Solha, CAIS/RNP, Brazilian Research Network
- Moira West-Brown, former team lead for the CERT/CC incident handling team and the CERT CSIRT Development Team

They gave us insight, recommendations and suggestions; provided information and resources we would not otherwise have had access to; and generally helped to make this a better document. Thank you all very, very much.

We want to thank every organization that completed our pilot survey. Without the representatives from these CSIRTs taking time to complete the survey, we would not have had the initial data presented here. For reasons of confidentiality, we cannot list their names here, but they know who they are and again, we thank you most deeply.

We would like to acknowledge and thank the following people for their contributions, support, and assistance in the production of this document.

- Barbara Laswell – who never wavered in providing her support, encouragement, and guidance as we set about our research and analysis, and who provided us the time and resources to undertake this work.
- Moira West-Brown, Don Stikvoort, and Klaus-Peter Kossakowski – for initially writing the first edition of the *Handbook for CSIRTs* [West-Brown 03], stimulating our thoughts and inspiring us to take the next steps in our CSIRT development work.

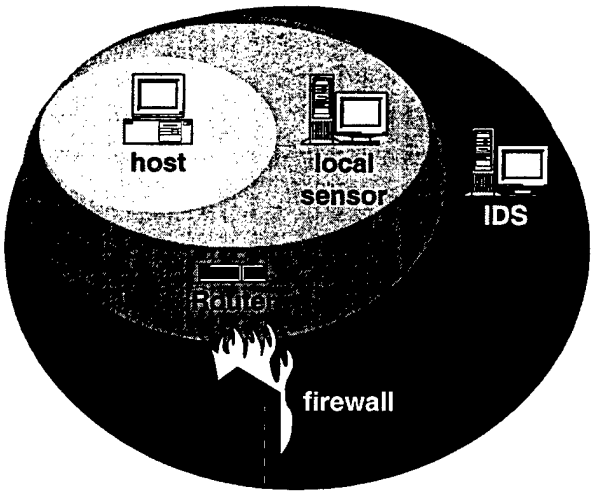
- Katherine Fithen for her continued support of our CSIRT development activities and for being an excellent resource, advisor, and friend.
- Pamela Curtis – for her dedication and perseverance in guiding us through the technical report process, editing our multitude of changes, and helping give the document one voice.
- Stephanie Rogers – for researching legal issues as they apply to incident response and providing us with links to relevant legal resources.
- Sheila Rosenthal and Terry Ireland – our library staff, for their incredible researching skills, assistance, and support.
- David Biber – our graphics artist, who helped us with the graphics in this publication and helped with the production of the example documents included in Appendix E.
- Diane Bradley and Pam Williams – who help us daily to synthesize, review, and organize information and whose support helps us to continue to be effective in the work we do.

Abstract

Keeping organizational information assets secure in today's interconnected computing environment is a challenge that becomes more difficult with each new "e" product and each new intruder tool. There is no one solution for securing information assets; instead a multi-layered security strategy is required. One of the layers that many organizations are including in their strategy today is a computer security incident response team, or CSIRT. This report provides an objective study of the state of the practice of incident response, based on information about how CSIRTs around the world are operating. It covers CSIRT services, projects, processes, structures, and literature, as well as training, legal, and operational issues. The report can serve as a resource both to new teams that are setting up their operations and to existing CSIRTs that are interested in benchmarking their operations.

1 Introduction

Keeping organizational information assets secure in today's interconnected computing environment is a true challenge that becomes more difficult with each new "e" product and each new intruder tool. Most organizations realize that there is no one solution for securing systems and data; instead a multi-layered security strategy is required.



Reproduced From
Best Available Copy

Figure 1: Multi-Layered Infrastructure Defense

One of the layers that many organizations are including in their strategy today is the creation of a computer security incident response team, or CSIRT.

Motivators driving the establishment of CSIRTs today include

- a general increase in the number and type of organizations being affected by computer security incidents
- a more focused awareness by organizations on the need for security policies and practices as part of their overall risk-management strategies
- new laws and regulations that affect how organizations are required to protect information assets
- the realization that systems and network administrators alone cannot protect organizational systems and assets

Although CSIRTs have been in existence since 1988, the development of CSIRTs and the incident response field is still in its infancy. It has not yet become a standardized field of practice but it is rapidly moving to a more standardized discipline. Many organizations are looking to formalize their incident response methodologies, processes, and organizational structures.

As organizations move to establish dedicated[1] or ad hoc[2] CSIRTs they are actively looking for guidance to see what has worked for other similar organizations. They want to know how many staff a CSIRT in a similar sector has, how they operate their incident response service, or what tools they use to record and track incident reports.

Currently there are no standard answers to these questions. CSIRTs can take many forms and have different requirements, responsibilities, functions, and structures.[3] We have seen CSIRTs whose staff only review intrusion detection logs, while other CSIRT staff recover and rebuild systems, provide security awareness training, analyze artifacts[4], publish alerts and advisories, and perform security audits and consulting.

This report is a start at collecting information about CSIRTs across a very broad canvas of activities.

The information for this report was gathered through

- our collective experiences in working with CSIRTs in the incident response work we have done over the years, the collaborations we have had, and the courses that we teach
- a literature search and review of related articles, books, and other documents concerning incident response, including existing or pending laws, legislation, and regulations that will have an impact on incident response work
- a pilot survey of CSIRT organizational structures. This survey was distributed to course attendees at the 14th Annual Computer Security Incident Handling Conference (FIRST) Conference in Hawaii in 2002 and to various other CSIRTs. Appendix A contains a copy of the pilot survey form.[5]

---

1 A formalized team is a capability where identified staff have been given the responsibility for both reactive and proactive CSIRT work.

2 An ad hoc team is a team called together to handle an incident as it occurs. It is more reactive in nature.

3 The different types of CSIRT organizational models are described in the SEI handbook CMU/SEI-2003-HB-001, *Organizational Models for CSIRTs*, which will be published in the fall of 2003.

4 Artifacts are basically the remnants of an intruder attack or activity. For example, malicious code or toolkits found on a compromised system would be considered artifacts.

5 If you are interesting in adding to the general knowledge of CSIRTs by filling out a survey, you can request a copy via email from csirt-info@cert.org.

- conducting follow-up discussions with CSIRTs who completed the survey and stated that they would participate in follow-up work
- collaborating with team members and other experts in the CSIRT environment to gather information on current processes, projects, and response trends
- researching and reviewing existing CSIRT-related, computer security-related, and incident response-related web sites and corresponding articles and white papers at those sites

1.1 Purpose of the Document

The purpose of this report is to provide an objective study of the state of the practice of CSIRTs and to present this information in a manner that will be beneficial for the CSIRT community. The report attempts to synthesize information about how those in the CSIRT field are operating their teams, and then provide this information as a resource to both new teams that are setting up their operations and existing CSIRTs that are interested in benchmarking their operations.

The report will also serve as a reference for CSIRTs, as it will provide a consolidated resource of information on CSIRT projects; literature; training, legal, and operational issues; and sample CSIRT processes and structures.

The information collected will also be used as the basis for identifying areas for further research and best practice development.

1.2 Scope of the Document

This document is a summary of the findings of the research done through the State of the Practice project. The State of the Practice project was conducted by the CERT CSIRT Development Team. The purpose of the State of the Practice project is to gain a better understanding of the CSIRT structures, functions, and services. Currently, much of the information available about CSIRTs is anecdotal. Our goal is to collect and analyze more empirical data to provide better insight into various CSIRT organizational structures and best practices.

This document is not an attempt to give a comprehensive review of all CSIRTs, CSIRT activities and projects, or CSIRT literature, training, or related legal issues. It is, however, an attempt to provide a general overview of these areas and issues. (In this dynamic environment, it is difficult to keep information up to date.) The findings and information presented here are

based on a sampling of CSIRTs done via survey; our own research, interviews, and observation[6]; and input and observations from others in the field.

This document provides information about CSIRTs at a particular point in time—June 2002 through August 2003. Although some of the information is time constrained, the resulting information can still provide useful insights for organizations planning to create or expand an incident response capability or formal CSIRT.

The focus of the document is the collection of data to understand how CSIRTs are structured and how they operate and to determine if there are any trends particular to a certain type of CSIRT or CSIRT sector.

This document does not try to make any recommendations for best practices or processes in day-to-day CSIRT activities. It is simply synthesizing and presenting the information gathered.

This document also does not include a review or discussion of broader security standards such as those from the International Standards Organization (ISO) or British Standards (BS).

1.3 Intended Audience

The primary audience for this document includes the general CSIRT community who may want a better understanding of the structure and functions of existing teams. It will also benefit those individuals and organizations looking to join the CSIRT community. It is specifically targeted at those managers and individuals who are involved in the process of creating and operating a CSIRT or managing incident activity. This may include

- Organizational Chief Information Officers (CIOs), Chief Security Officers (CSOs), and Information Systems Security Officers (ISSOs)
- project leaders and members charged with creating a team
- CSIRT managers
- CSIRT staff
- IT managers

As well as being a useful reference for higher management levels and all CSIRT staff, this document can also be of use to other individuals who interact with CSIRTs and would benefit from an understanding of CSIRT organizational issues. This may include members of the

[6] All contributions were provided voluntarily.

- CSIRT constituency
- law enforcement community
- systems and network administrator community
- CSIRT parent organization or other departments within the parent organization such as
  - legal
  - media or public relations
  - human resources
  - audits and risk management
  - investigations and crisis management

1.4 Use of this Document

This document was developed for use as both a stand-alone document and as a companion document to two other reports from the Software Engineering Institute:

- *Handbook for CSIRTs*, CMU/SEI-2003-HB-002 [West-Brown 03]
- *Organizational Models for CSIRTs*, CMU/SEI-2003-HB-001[7]

As a stand-alone document, this report can be used as an information reference by anyone interested in CSIRT activities. The document also provides information on

- the evolution and development of teams
- the types and numbers of teams existing today
- preliminary statistics on the types of CSIRT structures and processes gathered through the pilot survey
- current articles, publications, and training that may be of interest to anyone involved in incident response activities
- some current projects that teams may want to join or review
- resources that teams may want to use or review
- current challenges and issues that are being addressed by the CSIRT community

This document can be used in conjunction with the other two reports mentioned above to provide guidance for teams on the options for organizing and operating a CSIRT. It can be used at the early stage of CSIRT development to provide ideas for organizational structures and service offerings. It can also be used to help gather management buy-in and support and, after support has been gathered, to strategically plan and develop a team. Looking at what existing teams are doing can provide ideas for other teams and help existing teams plan their

[7] *Organizational Models for CSIRTs* will be published in the fall of 2003.

future growth. It can also be used to provide justification to management for requesting certain resources, funding, and support.

Each team will have its own circumstances, mission, and goals. These three reports provide information on alternatives and options for team operations and organization. None of the reports demand that you follow a particular course of operations.

Use the *Handbook for CSIRTs* [West-Brown 03] for specific in-depth informational guidance for issues relating to the establishment and operation of a CSIRT. Use *Organizational Models for CSIRTs* to understand the specific issues to be addressed when determining the model for your CSIRT. Use the *State of the Practice* report for examples of what other teams are doing and as an information resource and overview of CSIRT processes, structures, and resources.

1.5 Document Structure

The remainder of this document is organized as follows:

Section 2	Overview of what a CSIRT is and why it is beneficial; description of the types of CSIRTs and the history of CSIRTs
Section 3	Overview of the state of the practice of CSIRTs
Section 4	Summary of the state of the practice of CSIRTs and what is still missing; discussion of any noteworthy special topics resulting from the research
Section 5	Discussion of future work that can be done based on this report
Section 6	Where to get more help, where to read more, where to continue
Appendix A	CSIRT Organizational Survey
Appendix B	Comparison of incident response steps and processes
Appendix C	Training resources for CSIRTs
Appendix D	Cyber law resources
Appendix E	Sample incident reporting forms, templates, and flowcharts

1.6 About the Survey

The CERT CSIRT Development Team worked with other members of the CMU community to construct a pilot survey to collect information about the current organizational processes and structures of CSIRTs. The survey was distributed during June through August 2002. The

survey was an informal method of collecting information (no scientific sampling was done). The number of surveys collected did not constitute a statistical sample, so the results cannot be reviewed in such a light. However, the results did provide some interesting data that is shared in this report. The CERT CSIRT Development Team plans to continue to collect data through the use of an improved survey over the next few years.

Results from the 29 surveys collected as of the writing of the report have been incorporated into various sections of this report. The contents of the survey can be viewed in Appendix A.

The pilot survey was completed by a broad spectrum of CSIRTs across many countries and sectors. The majority of the CSIRTs participating in the survey were from the United States (38%) and Europe (34%). Other geographic areas represented were South America and the Asia Pacific region. The total number of countries that participated in the survey was 12. There were a few teams who stated that they were a global organization rather than representing one country.

Reproduced From
Best Available Copy

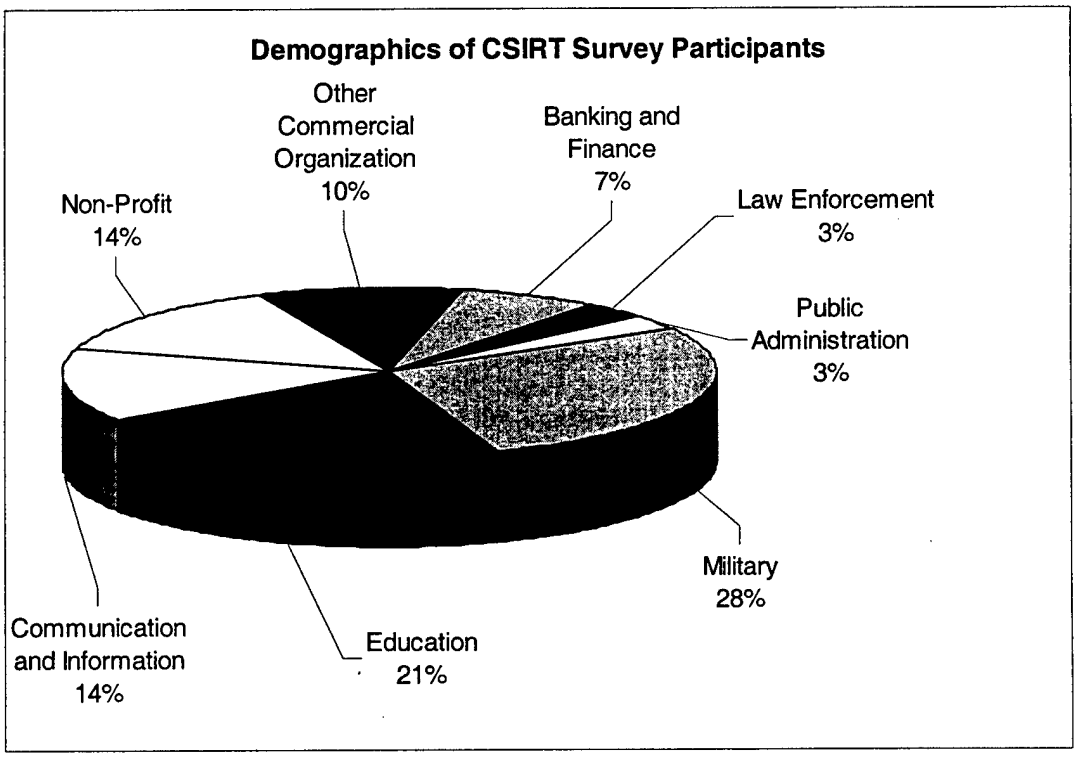


Figure 2: Demographics of CSIRT Survey Participants

The majority of the CSIRTs were from the military (28%) and education (21%) sectors. Other sectors represented were communication and information (14%), non-profit (14%), banking and finance (7%), law enforcement (3%), public administration (3%), and other commercial organizations (10%).

The participating CSIRTs also represented teams that had been in operation for over two years (62%) and those who were just starting[8] (21%). The modal[9] years of operation for the CSIRTs participating were four to six years (34%). The rest fell into the one to two year range (28%) and the seven to eight year range (17%).

Only 17% of the participating CSIRTs stated that their CSIRT was located across multiple countries. The number of countries that these CSIRTs were distributed across ranged from 2 to 103. The CSIRT located in 103 countries was in the banking and finance sector.[10]

1.7 About the Literature Search

In 1988, when the CERT Coordination Center (CERT/CC) was established, there was not much information available that described incident response or incident handling in detail. The good news today is that there is a growing body of literature that is available and that can be easily found using your favorite web search engine. (For example, at the time we were writing this document, a search on incident response provided about 15,000 links—some were duplicates, others were pointers to bookstores, sites, articles, and other references on this topic.) The more challenging task is sifting through all this data to find information that meets your specific requirements for incident handling operations and building a CSIRT capability.

In our literature review for this state of the practice, we examined books, white papers, articles, guidelines, procedures, and other similar information and research available on the web and in print.

Our examination of the literature identified a few broad-based observations that will be of interest to new or existing CSIRTs to further increase their overall knowledge and understanding of incident handling, team responsibilities, team composition, and policy and procedure issues:

- There is a growing base of anecdotal and case study information appearing in print about not only the formation and organization of CSIRTs, but also on the general types of activities these teams undertake and how they perform them.
- More information is available about the management and costs related to building and operating incident response teams.

---

8 In operation for less than one year.

9 Modal in this case means the most frequently reported.

10 In talking to other corporate CSIRTs, it was often the case that those that support multinational corporations have distributed teams in each country where their branch offices are located.

- There are some common functions suggested for incident response activities within a CSIRT—even if these functions are "grouped" somewhat differently across the literature.
- There are many similarities in CSIRT processes; however, within the day-to-day operations of a CSIRT, the way in which these processes are implemented and the depth and breadth of the services that are provided may be very different.

Many of the resources we reviewed provided various levels of detail on approaches for handling incidents. A number of them also provided information about

- defining incident response and other terminology
- developing an incident response plan
- identifying issues and steps in forming a computer security incident response team
- defining mission, goals, operations, and responsibilities
- identifying services and level of support
- determining the constituency base
- documenting policies and procedures
- tracking and tracing incidents
- performing computer forensic analysis

Many of the resources also include

- general trends in incident handling and intruder attacks
- example case studies and other CSIRT stories
- sample templates, checklists, process guides, or flowcharts related to incident handling

Where appropriate, these resources and any trends, commonalities, or processes extracted from them were included in this document.

2 Computer Security Incident Response Teams

2.1 What is a CSIRT?

Computer networks have revolutionized the way business is done, but they have also introduced substantial risk. Changes in society's use of technology have provided new opportunities for intrusions. Changes in organizational data protection requirements, local and national laws, and institutional regulations have made it imperative to address security concerns at an enterprise level. Even the best information security infrastructure cannot guarantee that intrusions or other malicious acts will not happen. When computer security incidents occur, it is critical for an organization to have an effective way to respond. The speed with which an organization can recognize, analyze, and respond to an incident will limit the damage and lower the cost of recovery.

A CSIRT is a service organization that is responsible for receiving, reviewing, and responding to computer security incident reports and activity. Its services are usually performed for a defined constituency that could be a parent entity such as a corporation, government, or educational organization; a region or country; a research network; or a paid client.

Part of a CSIRT's function can be compared in concept to a fire department. When a fire occurs, the fire department is called into action. They go to the scene, review the damage, analyze the fire pattern, and determine the course of action to take. They then contain the fire and extinguish it. This is similar to the reactive functions of a CSIRT. A CSIRT will receive requests for assistance and reports of threats, attack, scans, misuse of resources, or unauthorized access to data and information assets. They will analyze the report and determine what they think is happening and the course of action to take to mitigate the situation and resolve the problem.

Just as a fire department can be proactive by providing fire-prevention training, instructing families in the best manner to safely exit a burning building, and promoting the installation of smoke alarms and the purchase of fire escape ladders, a CSIRT may also perform a proactive

role. This may include providing security awareness training, security consulting, configuration maintenance, and producing technical documents and advisories.[11]

A majority of CSIRTs started as "response-oriented" organizations, but have since developed into organizations that work proactively to defend and protect the critical assets of organizations and the Internet community in general. This proactive work can also include influencing policy, and coordinating workshops and information exchanges. It also includes analyzing intruder trends and patterns to create a better understanding of the changing environment so that corresponding prevention, mitigation, and response strategies can be developed and disseminated.

When utilized to its fullest extent, however, a CSIRT is more than an incident response capability. The goals of a CSIRT must be based on the business goals of the constituent or parent organizations. Protecting critical assets is key to the success of both an organization and its CSIRT. The goal of a CSIRT, in this context, is to minimize and control the damage, provide effective response and recovery, and work to prevent future events from happening. In this role the CSIRT collects incident information, security weaknesses, and software and system vulnerabilities in the organizational infrastructure or within a constituency.

In a commercial, military, educational, or government setting, the CSIRT becomes a focal point for business intelligence within the organization and a primary source of authentic risk data. This information can provide an important data feed into operational risk modeling. The CSIRT can be seen as a key element in loss minimization and risk mitigation. In this same manner, the CSIRT's role as a central repository allows it to gather an enterprise-wide picture of security issues as it relates across the organization. This also allows the CSIRT to link together events that may not have been seen to be related when looked at individually.

A CSIRT can be on-site and able to conduct a rapid response to contain a computer security incident and recover from it. CSIRTs may also have familiarity with the compromised systems and therefore be more readily able to coordinate the recovery and propose mitigation and response strategies. Their relationships with other CSIRTs and security organizations can facilitate the sharing of response strategies and early alerts to potential problems.

CSIRTs can work with other areas of the organization to ensure new systems are developed and deployed with security in mind and in conformance with any site security policies. They can help identify vulnerable areas of the organization and in some cases perform vulnerability assessments and incident detection services. In their coordination function, they can be a central point that pulls together information and analysis from the physical security sector, the IT

---

[11] For a description of these various services see the *CSIRT Services* list at <http://www.cert.org/csirts/services.html>.

group, the risk and audits group, and the management group. This coordination can extend even outside the organization to include collaboration with other teams and law enforcement agencies. CSIRTs can act as a point of contact for coordinating with other legal and security agencies or for contacting victim and source sites involved in intruder activity.

CSIRTs are not all structured in the same manner; they do not all perform the same function or even have the same name. Every CSIRT is different, and these differences may include the CSIRT's

- mission, goals, and objectives
- constituency
- provided services
- definitions and terminology

Table 1 lists some of the many different types of acronyms and names for CSIRTs. Although the names are different, all teams perform incident handling. These acronyms and names are just equivalent ways of referring to an incident handling team.

Table 1: CSIRT Acronyms and Names

CSIRT	Computer Security Incident Response Team
CSIRC	Computer Security Incident Response Capability
CIRC	Computer Incident Response Capability
CIRT	Computer Incident Response Team
IHT	Incident Handling Team
IRC	Incident Response Center or Incident Response Capability
IRT	Incident Response Team
SERT	Security Emergency Response Team
SIRT	Security Incident Response Team

Although we commonly see teams referred to as "incident response teams" the term "incident response" only relates to one aspect of the work that a CSIRT does. The CERT CSIRT Development Team uses instead the term "incident handling" to describe the much broader activities that many CSIRTs perform in their day-to-day operations. Incident handling includes three functions: incident reporting, incident analysis, and incident response.

- Incident reporting involves receiving and reviewing incident reports and alerts.
- Incident analysis is the attempt to determine what has happened, what impact, threat or damage has resulted, and what recovery or mitigation steps should be followed.

- Incident response is the actions taken to resolve or mitigate an incident, coordinate and disseminate information, and implement follow-up strategies to stop the incident from happening again.

We have also begun to see others in the CSIRT community use the term "incident handling" rather than "incident response" to describe the broader realm of CSIRT activities.

It is important to realize that incident handling is not just the application of technology to resolve computer security events. It is the development of a plan of action. It is the establishment of repeatable processes and methodologies for

- notification and communication
- collaboration and coordination
- incident analysis and response

2.2 Types of CSIRTs

CSIRTs come in all shapes and sizes and serve diverse constituencies. Some CSIRTs, such as the Japan Computer Emergency Response Team Coordination Center (JPCERT/CC), support an entire country. Other CSIRTS may provide support to a particular university such as Oxford, a commercial organization such as Boeing or SUN Microsystems, or a particular domain or IP range such as the Telia CERT Coordination Centre (TeliaCERTCC). There are also corporate teams and organizations that provide CSIRT services to clients for a fee, such as IBM Managed Security Services (IBM-MSS) or the debis Computer Emergency Response Team (dCERT).

CSIRTs can be categorized in many ways. One general way is to look at the main purpose, function, or services of the CSIRT, as shown in the following examples:

- Internal CSIRTs provide incident handling services to their parent organization, which could be a bank, a university, or a federal agency.
- Coordination centers coordinate and facilitate the handling of incidents across various CSIRTs, or for a particular country, state, research network, or other such entity. Usually coordination centers will have a broad scope and a diverse constituency.
- Analysis centers focus on synthesizing data from various sources to determine trends and patterns in incident activity. This information can then be used to help predict future activity or provide early warning when current activity matches a set of previously determined characteristics.
- Vendor teams located in software or hardware companies and handle reports concerning vulnerabilities in their products. They analyze the vulnerabilities, develop patches or workarounds, and disseminate this information to their clientele or to the broader public.

They work with other CSIRTs, security experts, and researchers to track and respond to these vulnerabilities.

- Incident response providers provide incident handling services as a product to other organizations. They are sometimes referred to as managed security service providers (MSSPs).

CSIRTs can also be categorized by how they are structured. The CERT CSIRT Development Team divides these categories into the organizational models shown in Table 2.

Table 2: CSIRT Organizational Models

Model	Description
Security Team	In this model, no group or section of the organization has been given the formal responsibility for all incident handling activities per se. Available personnel at the local or division level handle security events on an ad hoc, isolated basis as part of their overall responsibilities or job assignments. Usually these personnel are in the IT department and work on general security tasks for the infrastructure of the organization.
Internal Distributed CSIRT	A distributed team is scattered across organizational and geographic locations. There is a manager who oversees and coordinates activities that affect the distributed team. Across the organization, individuals are identified as the appropriate points of contact for particular functional areas or divisions based on their experience and expertise with various operating-system platforms, technologies, and applications. A distributed team can be devoted 100% to CSIRT work or team members may only perform CSIRT work part of the time and perform other work the rest of the time.
Internal Centralized CSIRT	A centralized team is a team located in one physical or geographical location that has responsibilities for the entire organization or constituency. This is often a local or internal team at a small company or government department. In most cases, all team members are dedicated 100% to CSIRT work.
Internal Combined Distributed and Centralized CSIRT	This model represents a combination of the distributed CSIRT and the centralized CSIRT. It maximizes the use of existing staff in strategic locations throughout the organization, with the centrally located coordinating capabilities of a dedicated team, to provide a broader understanding of the security threats and activity affecting the constituency. The centralized team usually does CSIRT work 100% of the time. The distributed team could be dedicated or part time.

Model	Description
Coordinating CSIRT	Often centralized, a coordinating CSIRT is located in one physical or geographical location. In this model the CSIRT coordinates and facilitates the handling of incidents across a variety of organizations. The CSIRT can be a coordinating entity for individual subsidiaries of a corporation, multiple branches of a military organization, branch campuses in an educational organization, institutions in a research network or specific domain or for a particular country or state. Coordinating CSIRTs usually have a broader scope and a more diverse constituency.

More information about these organizational models and structures can be found in *Organizational Models for CSIRTs*.

In the pilot survey, we combined the above functional and organizational categories to create the following list:

- security team (called an ad hoc team)s
- distributed dedicated team
- distributed part-time team
- centralized team
- coordination center
- analysis center
- managed security service provider

We then asked the participating teams to identify what category best described their CSIRT structure. See Section 3.2.3, "Organizational Placement of the CSIRT," for the survey results of their responses.

CSIRTs can also be categorized by the sector in which they are located or in which their constituency is located. The sectors can be consolidated into a few general categories: government, research and education, national, commercial, and other.

The following list breaks the above categories into more detail. These were the sectors used in the CSIRT Organizational Survey. See Figure 2, "Demographics of CSIRT Survey Participants," for the results of the pilot survey.

- military
- education
- information and communication
- electric power

- oil and gas
- water supply
- government law enforcement services
- government fire and rescue services
- government and public administration
- transportation
- banking and finance
- public health services
- professional services
- other commercial organization
- other non-profit organization

2.3 History and Development of CSIRT Capabilities

Ideas about creating teams of people to handle computer security incidents and emergencies were published and discussed long before the arrival of the Internet Worm (Morris Worm) in 1988. Most ideas proposed that such teams would be used to augment existing security management groups to protect host systems and network services. Due to lack of awareness, no funding was made available to implement these types of computer emergency response teams.

2.3.1 The Early Beginnings

The major impetus for the creation of the first CSIRT was the release of the Morris Worm in November, 1988. This worm, written by a 23-year-old college student, propagated itself from computer to computer through the exploitation of various vulnerabilities. There is consensus in the historical documentation about this event that there were approximately 60,000 to 80,000 hosts on the Internet (then called the ARPANET) at the time and that approximately 10% of all hosts were infected by the Morris Worm. The main problem, however, was that many of the systems that were infected were email relays and servers that were part of the Internet backbone. Many sites also removed their systems from the network so as not to be infected. The result was that many of the Internet's communication pathways were inoperative.[12]

---

[12] For an in-depth description of the Morris Worm, see J. Reynolds , RFC 1135, *The Helminthiasis of the Internet*. Available online at <http://www.ietf.org/rfc/rfc1135.txt>.

After the worm had been successfully contained, the National Computer Security Center (part of the National Security Agency), initiated a series of meetings to discuss how to prevent and respond to such occurrences in the future. On November 8, 1988, a postmortem meeting was organized by the Defense Advanced Research Projects Agency (DARPA) to review and discuss the lessons learned from the worm activity and related response. These were some of the observations made:

- Participating staff at various major universities and computer centers were able to do a successful analysis of the worm and resulting activity while the incident was happening, even though not every detail of the worm attack and propagation was fully analyzed at that time. It was also determined that some important aspects of the worm propagation were not immediately recognized by some sites, resulting in more systems being infected. In review, it could be seen that many sites were doing duplicate work in trying to analyze the worm, and this time would have been better spent if they had collaborated. It was determined that if all involved would have been able to communicate and compare their results, the complete analysis would have been available much earlier, leading to both a quicker containment of the worm and earlier recovery or protection of systems.
- The corrective measures derived from the analysis could have prevented further infections. Because there was not a communication means available, distribution of the measures to all who needed the information was not possible and many sites did not get the information in a timely manner.
- The damage recovery was painful but straightforward, as long as the affected organization had trusted backups available. But because the complete corrective measures could not be distributed to all involved, many sites saw their recovered hosts become reinfected.

It was concluded that the most problematic part of the response effort was the missing communication mechanisms. With many sites disconnecting from the network to contain the worm activity and repair and recover their systems, and with much of the Internet mail service inoperative due to the servers and relays being infected, there was not a quick and viable way to get notification out to the Internet community on how to protect their systems from the activity or respond if they were infected. Overall, the basic problem was that there was not a formal method of coordination to handle such a computer security attack and the related analysis and response.

In recognition of this problem, DARPA announced its intention to fund the development of a coordination center for Internet security incidents. DARPA chose the Software Engineering Institute[13] as the new center's home. DARPA charged the SEI[SM] with establishing a capability

---

[13] The Software Engineering Institute (SEI) is a Federally Funded Research and Development Center. For more information see <http://www.sei.cmu.edu/about/overview/sei/sponsor.html>.

[SM] SEI is a service mark of Carnegie Mellon University.

to quickly and effectively coordinate communication among experts during security emergencies in order to prevent future incidents. The new center was also charged with building awareness of security issues across the Internet community. A pilot research program was originally funded. The center was named the Computer Emergency Response Team (CERT). Eventually CERT became a service mark for Carnegie Mellon University and the name was changed to the CERT Coordination Center (CERT/CC).

The CERT/CC opened its doors in December 1988 and began to receive phone calls starting the first day. The initial staffing was comprised of personnel from other programs within the SEI who answered the CERT/CC hotline and passed the calls to staff identified to handle incident reports. This initial transitional staff spent part of their time doing CERT/CC work until a full-time staff was in place. The initial staffing level was four technical staff with a manager.

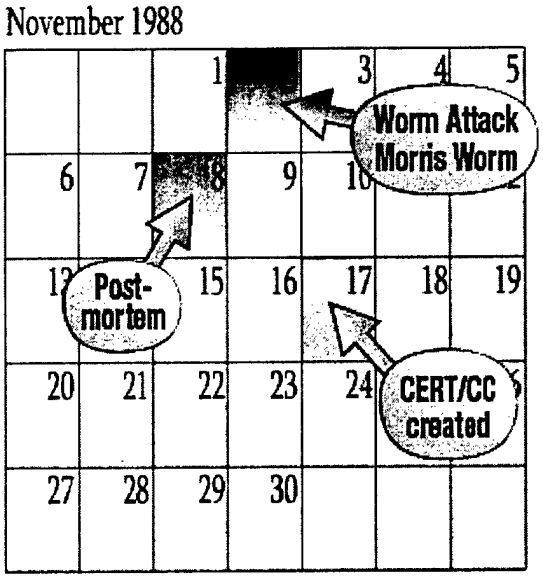


Figure 3: Timeline of Internet Worm Attack and Creation of CERT/CC

The goal and plan resulting from the DARPA postmortem and pilot project was never to have just one organization as the mechanism for the needed coordination. It was recognized that a single CSIRT would not be able to handle the differing needs of the constituencies or the resulting workload. Other agencies and constituencies were encouraged to create and sustain their own teams.

In the next year other organizations, such as the U.S. Department of Energy (DoE), the National Aeronautics and Space Administration (NASA), the U.S. National Institute of Standards and Technology (NIST), and the U.S. military, established their own teams similar to the CERT/CC but focused on their own constituencies.

2.3.2 The Creation of FIRST

In August 1989 an invitational workshop was organized by the CERT/CC to discuss not only what was learned during the first year of operation but also what the next steps were in coordinating relationships between the teams.[14] This became the first event drawing practitioners from the field and the start of the annual conferences that are now organized by the Forum of Incident Response and Security Teams.[15]

In October 1989 another worm attacked the Internet, which now consisted of approximately 170,000 hosts. This worm, called WANK, exploited vulnerabilities in systems connected to the Digital Equipment Corporation's proprietary network, DECNET. Three teams coordinated their activities to provide the response to this worm: the Department of Energy's Computer Incident Advisory Capability (CIAC), the NASA Space Physics Analysis Network, and the CERT/CC. Various warnings were released from both CIAC and CERT/CC that were helpful to the Internet community, even though many administrators did not heed the warnings and were infected by a variant of the WANK worm called OILZ released two weeks later.

After this example of successful collaboration between teams, more discussions ensued on how to set up a response team network. During a 1990 workshop by NIST and CERT/CC, a panel session presented and discussed the ideas for such a network. The session, titled "Developing the Response Team Network," included the following presentations:

- Dennis D. Steinauer (NIST, USA), "The Response Center Network : Developing It and Making It Work"
- Richard D. Pethia (CERT/CC, USA), "Developing the Response Team Network"
- Ronald H. Hysert (Canadian System Security Centre), "Developing the Computer Security Incident Response Network: A Canadian Perspective"
- Christopher C. Harvey (SPAN, France), "The Development of Response Teams in Europe"

From these and other discussions, goals for future collaboration were established. These goals were to share information among CSIRTs and, if needed, to aid one another during incidents and network-wide attacks. The CSIRT community is still pursuing these goals today. Teams working in various collaborations are looking for the most effective way to establish a coordination network.

---

14 <http://www.first.org/events/progconf/1989/progs.htm>

15 Today FIRST conferences are international forums for CSIRTs and security teams involved in incident handling. To read more about them see <http://www.first.org/conference/>.

After the workshop, further discussion brought 11 founding members (including one from France) together in November 1990 to establish a forum for CSIRTs and security teams, which is now the Forum of Incident Response and Security Teams (FIRST). At this time, the Internet had approximately 340,000 hosts.

Table 3: List of Founding FIRST Members

Air Force Computer Emergency Response Team (AFCERT)
CERT Coordination Center
Defense Communication Agency/Defense Data Network
Department of the Army Response Team
Department of Energy's Computer Incident Advisory Capability (CIAC), Lawrence Livermore National Laboratory
Goddard Space Flight Center
NASA Ames Research Center Computer Network Security Response Team (NASA ARC CNSRT)
NASA Space Physics Analysis Network (SPAN CERT)
Naval Computer Incident Response Team (NAVCIRT)
National Institute of Standards and Technology Computer Security Resource and Response Center (CSRC)
SPAN-France

FIRST is primarily a network of registered members, either CSIRTs or security teams. The members work together voluntarily and concentrate on the prevention of incidents, sharing of information, sharing of vulnerability and artifact analysis, and coordination of response activities, where appropriate, when an incident occurs.

Each year FIRST has continued to grow, and as of September 2003, 151 organizations are participating members. More information about FIRST can be found on their web site at <http://www.first.org/>.

2.3.3 Europe Becomes Involved

While the idea of CSIRTs had a growing number of supporters in the U.S in 1991 and 1992, other areas were still to a large degree without their own CSIRTs. The first European CSIRT was established in France in the Space Physics Analysis Network (SPAN). This network was traditionally part of the NASA networks and therefore the need for a team was recognized much earlier, particularly after the WANK and OILZ worm attacks.

Up until this point, only one or two European security experts had attended the annual CSIRT conference, which at that time was still being organized and hosted by the CERT/CC.[16] This began to change in 1992, particularly in the European research networks. As the number of hosts on the various European networks began to climb past 10,000, there was more need for computer and network security. As more incidents took place, those with an understanding of the CSIRT concept began to look for ways to work together. In 1992 a working group organized by the Association of European Research Networks reviewed the situation. There was agreement that CSIRT efforts in each national research network would bring a real benefit. It was expected that each European team would cooperate with the others by sharing responsibilities for communicating new vulnerabilities and security developments when they affected all teams, but that each particular team would concentrate on its own constituent community. This concept, to concentrate on one particular constituency but collaborate with other CSIRTs and security experts, is one of the key unchanged principles of the CSIRT community today.

As a result of the European working group, various national research networks started their own projects to establish CSIRTs for their organizational constituencies. As was common in this arena, teams were established along different guidelines and offered different services based on the needs of the community. Examples of two different types of teams that were established within the European research community are CERT-NL and DFN-CERT.

- The SURFnet Computer Security Incident Response Team (CERT-NL) was established by SURFnet, the Dutch research network, as a decentralized team. The team was staffed with two members of SURFnet working in cooperation with experienced specialists from other universities in the research network that could help provide broader expertise and also help provide coverage outside of their normal working hours. Since this was created as an internal project within SURFnet, there was not much of a delay in getting the team up and running. The CERT-NL team became active in 1992.[17]
- The Computer Emergency Response Team for the German Research Network DFN (DFN-CERT) was established as a centralized team. The team was located at a university that was a member of the network. Therefore, from a viewpoint of other universities, the work was handled by "external" staff (to their organization) but from another "internal" organization (of the whole network). No coverage was provided outside of normal working hours. As this was an external project, a call for tender process[18] was necessary, which resulted in a delay in establishing the team. DFN-CERT became active on the first working day of 1993.

---

16 The first five conferences were sponsored and hosted by CERT/CC. Since 1994; a different organization has sponsored and hosted the conference each year. See <http://www.first.org/events/progconf/>.

17 For more information on SURFnet see <http://www.surfnet.nl/en/>.

18 A call for tender is a call for proposals, in which people or organizations are asked to provide a bid for performing some type of work.

The early European teams followed the CERT/CC model in structure and services. They performed incident handling mainly by providing guidance; disseminating alerts, warnings, and advisories; and performing security awareness building. They did not provide on-site support.

Another idea that resulted from work by the European working group was having a centralized European team to coordinate the efforts of the other teams. To determine if this would work, a one-year research project was initiated in mid-1993 by the RARE (Réseaux Associés pour la Recherche Européene) CERT Task Force. The final report at the end of 1994 did indeed support the notion that providing incident response in Europe would best be achieved via a top-down approach. Based on the assumption that not all European research networks would have money to fund their own active teams (which was true and is still true today), the recommendation was made that a strong European team modeled after the CERT/CC should be established.

The fact that such a centralized team would require funding and would also be seen as competition to the established European teams made this recommendation unpopular, and the report had no immediate impact or influence. In looking back, it might be said that Europe was perhaps lucky to have not replaced the successful bottom-up or grass-roots approach to establishing incident response capabilities with a top-down political structure.[19] This is because any centrally established European CSIRT coordination center would be very remote to the users and sites in the various participating countries. Differences in not only the language but legal issues and cultural differences would make it difficult to have one centralized CSIRT that could adequately keep in touch with and understand the needs of the different European constituencies. To be a successful and effective team, a CSIRT must stay in contact with its constituency. This is always easier if the team is relatively near to the constituency from the start.

During this time (early to mid 1990s), there was still the question of how to structure the interrelationships between the existing European teams and also how to structure these relationships and communications with CSIRTs in other areas, such as Canada and the United States, or with teams like the newly established Australian Computer Emergency Response Team (AusCERT).[20]

Late in 1993, the first meeting of European CSIRTs was initiated by staff members of CERT-NL and DFN-CERT. The belief was that communication would ultimately lead to better cooperation. This meeting is noteworthy, as this was the first CSIRT meeting outside the U.S. In 1994 and 1995 two more meetings were held, bringing more and more teams together. A template for collecting information about CSIRTs was developed that could be shared with

---

[19] This might be a similar problem for teams that are being established in other geographic areas.

[20] AusCERT was the first CSIRT established in the Asia Pacific region. It was created in 1993.

the other teams. Again, the community of European research networks supported this idea of a centralized European CSIRT and funding was established for a task force to develop a roadmap for the future of CSIRTs in Europe.

2.3.3.1 Development of EuroCERT

The TERENA[21] task force "CERTs in Europe" final report recognized not only the need for the establishment of more local teams situated near to the constituency experiencing the attacks and incidents, but also the need for some type of coordination to improve the overall interaction between teams [Ferriera 96]. This was seen as a way to provide a higher level of support in Europe for incident handling activities than could be provided with one team acting alone. This approach led to a three-year period in which various projects were suggested, prepared, and drafted, finally culminating in a proposal for a European coordination center. This project was started later in 1997 and continued through 1999 as EuroCERT [Kossakowski 96].

There were various problems with this project, as some CSIRTs saw EuroCERT as competing with their own activities and thought that the agreements already in place between teams were efficient enough to not need facilitation or support by another organization or level of hierarchy. The failure of EuroCERT did not prove that coordination of CSIRTs could not be done; it showed rather that any coordination needed to be different from that which already existed. It needed to add value to the overall processes already in place and it needed to provide functions that were not possible under the existing individual CSIRT agreements. These problems are not inherent to European CSIRTs and organizations; similar problems have been seen in the development of CSIRT coordination efforts in various organizations, whether in an educational, governmental, or commercial setting. The resulting lesson learned is an important one that other inter-organizational CSIRT coordination efforts should keep in mind as they work to develop collaboration and coordination mechanisms in their own area or region.

Problems that still needed to be addressed regarding coordination between European CSIRTs included the following:

- The existence of so many teams made it increasingly impractical to maintain relations of the same quality with all other teams.
- It was highly unlikely that CSIRTs from one country would understand the differences between CSIRTs in another. It would be much more convenient to provide one common point of contact rather than, for example, having a French team need to decide which German team to notify or coordinate with.

---

[21] TERENA is the Trans-European Research and Networking Association. More information can be found at <http://www.terena.nl/>.

These are still the same considerations behind all of today's efforts to improve the overall CSIRT infrastructure, both inside and outside of Europe.

2.3.3.2 The Development of the CSIRT Task Force

As the EuroCERT pilot was coming to an end in late 1999, TERENA, as a long-time supporter of European CSIRT activities, called for a meeting to discuss the impact this would have to the overall CSIRT activities in Europe. While all goals that EuroCERT should have achieved by its operation were revisited, all participants agreed to approach the very same goals differently.

- Instead of having a full-fledged service supported by members, useful activities were to be addressed by working groups of volunteers.
- Instead of having a central body coordinating the various teams, the ability of the individual teams should be strengthened and supported by providing mechanisms to
  - collaborate
  - integrate new teams
  - build up trust by knowing and understanding the services other teams provide
- Instead of having a central body arranging meetings among European teams, a facilitator would arrange such meetings.

The outcome of this volunteer approach was very successful. TERENA volunteered to serve as a facilitator and arrange meetings for the participating European CSIRTs three times a year. This was the start of the TF-CSIRT (CSIRT Task Force).[22] The goals of this group and its meeting minutes and project teams can be found at <http://www.terena.nl/tech/task-forces/tf-csirt/>.

Successful outcomes of this voluntary group approach to projects include

- The Incident Object Description and Exchange Format (IODEF) project. This project involved the development of a data model and specifications for exchanging incident data between CSIRTs using Extensible Markup Language (XML).[23] This project was completed and has now been transferred to the Incident Handling (INCH) Working Group of the Internet Engineering Task Force (IETF).[24]
- The Training of Network Security Incident Teams Staff (TRANSITS) project. This is a project that collected presentations and materials for CSIRT training. Various individuals from different European teams then created the final version of a set of training materials

---

22 In TERENA, a task force is the formal mechanism by which support is provided.

23 See <http://www.terena.nl/tech/task-forces/tf-csirt/iodef.html> for more information about the project.

24 See <http://www.ietf.org/html.charters/inch-charter.html> for more information about the project.

into a course for new incident handling staff. This training is supported by the European Union so that new CSIRT team members can attend the training for a nominal fee.[25]

Another benefit of this group is the opportunity for members of various teams to meet each other face-to-face at meetings throughout the year. Operational phone calls and data exchanges are easier when people get to know one another. The TF-CSIRT has been successful in providing this type of forum for many of the European CSIRTs and has offered real opportunities for collaboration and coordination, as can be seen by the projects mentioned previously. Another significant achievement of the group has been the successful expansion of its activities beyond the original research networks by attracting commercial and government teams as participants as well.

Another successful outcome of this new approach to CSIRT collaboration was the Trusted Introducer or TI. This group took over the job of maintaining a directory of European CSIRTs. Along with the directory, the TI provides an accreditation service. Directories maintained previous to the TI (1995-1997 by DFN-CERT, 1998-1999 by EuroCERT) of European CSIRTs really meant work in terms of infrastructure and maintenance. The TI was able to provide this supported infrastructure.

The first step towards the TI service was an analysis undertaken in early 2000. The analysis was commissioned by TERENA (another facilitation to get things started) and in its own words:

> *The aim of this report is to describe TI: an objective process meant to be applied to teams within the above defined scope [CSIRTs], that will enable teams new to the CSIRT community to move to a level where other teams will find it relatively easy to share information with them and work with them on incidents (in other words: to trust them) - and that will enable teams (also the already established ones) to stay on that level. To ensure the process's objectivity TI will be fully based on objective statements that can be verified* [Kossakowski 00].

A large point of discussion between teams was whether a form of certification rather than accreditation should be done as part of the TI work. Most teams felt unsure whether certification was really necessary and many thought that the issues involved were not well understood at the time. Concentrating on achievable goals, it was decided to go along with an accreditation framework.

Based on very positive feedback on the report, the teams decided to implement the TI approach. After a call for tender, the TI service started on September 1, 2000, with initial fund-

---

[25] See <http://www.ist-transits.org/> for more information about the project.

ing from TERENA, switching to funding by membership fees of accredited teams after the first year of operation.[26]

So while many people had expected much more from the EuroCERT project, the lack of a common understanding of what a "Coordination Center" would provide and how such a center would be different from any other CSIRT brought the project to an end. But the knowledge gained from this project resulted in a new concept for collaboration of CSIRTs. This concept focused on smaller and much more understandable and manageable goals and involved a format of volunteers from different teams, providing their insights, expertise, and time. In the end it enabled a much better support for European CSIRTs than was expected to be reached by the end of 1999.

2.3.3.3 Trends in European Teams Today

Many of the first European CSIRTs were developed to provide incident handling for academic research networks. Today, we see a growth in not only commercial CSIRTs in Europe but also the development of government CSIRTs such as GOVCERT.NL,[27] the national government CSIRT for the Netherlands.

2.3.4 Initiatives in the Asia Pacific Region

Although there were security teams established on an informal basis in the Asia Pacific region in the early 1990s, the first recognized CSIRT there was AusCERT. AusCERT was established in 1993 under its original name the Security Emergency Response Team (SERT). Initial funding and support was provided through a collaboration of three Australian universities: Queensland University of Technology, Griffith University, and The University of Queensland. Over time SERT evolved into AusCERT, the Australian Computer Emergency Response Team [Smith 94]. Its funding is now provided through membership subscription fees and some government funding [AusCERT 03]. In 1999 Australia was selected to host the FIRST conference to bring attention to the emerging growth of teams in the Asia Pacific region.

More CSIRTs in the Asia Pacific region were formed in 1996 and 1997. Some teams started out as voluntary organizations and then later were given government funding to be national teams. The Computer Emergency Response Team Coordination Center-Korea (CERTCC-KR), the Japan Computer Emergency Response Team Coordination Center (JPCERT/CC) and the Singapore Computer Emergency Response Team (SingCERT) are examples of teams that received government funding and were early innovators in CSIRT development in the Asia Pacific. All became FIRST members.

---

26 <http://www.ti.terena.nl/>

27 For more information see <http://www.govcert.nl/>.

These early teams have become leaders in the Asia Pacific region, helping teams within their constituency and country get started and supporting incident response efforts not only in their country but globally. They have also been highly instrumental in the creation of various working groups for Asia Pacific CSIRTs.

2.3.4.1 Creation of the Asia Pacific Security Incident Response Coordination Working Group

There was a great interest by the Asia Pacific teams in the regional meetings of the European teams, and they started similar activities to look at approaches for coordinating CSIRT collaboration and data sharing for the teams in that area. This resulted in the formation of the Asia Pacific Security Incident Response Coordination (APSIRC) Working Group in 1997. This working group was formed as an outgrowth of work by the Asia Pacific Networking Group (APNG)[28] [Ito 03].

The development of the APSIRC Working Group (APSIRC WG) was spearheaded by CERTCC-KR, SingCERT, and JPCERT/CC. The main function and services of the working group was to provide points of contact for the various member teams and to also provide resources and assistance for newly forming teams in the area [Ito 03]. Most of the initial team members were national teams such as the CSIRTs for Singapore, Malaysia, Japan, and Korea.

2.3.4.2 Creation of Asia Pacific Computer Emergency Response Team

In 2003 the APSIRC WG was transitioned into a new group, the Asia Pacific Computer Emergency Response Team (APCERT). The APCERT has both a steering committee and a secretariat to provide organizational support and direction. Its initiatives and goals involve developing a regional and operational framework for not only the sharing of information and incident data between members of APCERT but also the coordination of incident response efforts. APCERT is also looking into projects concerning accreditation of members, methods for collecting membership fees, and methods for developing and delivering training for new and existing teams [Ito 03].

APCERT full members as of August 2003 include [Ito 03]

- AusCERT - Australian Computer Emergency Response Team, Australia
- BKIS - Bach Khoa Internetwork Security Center, Vietnam
- CCERT - CERNET Computer Emergency Response Team, Republic of China
- CERTCC-KR - Computer Emergency Response Team Coordination Center-Korea, Korea
- CNCERT/CC - China Computer Emergency Response Team Coordination Center, Republic of China

[28] See <http://www.apng.org/> for more information on the Asia Pacific Networking Group.

- HKCERT/CC - Hong Kong Computer Emergency Response Team Coordination Center, Hong Kong, China
- IDCERT - Indonesia Computer Emergency Response Team, Indonesia
- JPCERT/CC - Japan Computer Emergency Response Team/Coordination Center, Japan
- MyCERT - Malaysian Computer Emergency Response Team, Malaysia
- PH-CERT - Philippine Computer Emergency Response Teams, Philippines
- SecurityMap.Net CERT - Securitymap Networks Computer Emergency Response Center, Korea
- SingCERT - Singapore Computer Emergency Response Team, Singapore
- ThaiCERT - Thai Computer Emergency Response Team), Thailand
- TWCERT - Taiwan Computer Emergency Response Team/Coordination Center, Chinese Taipei
- TW-CIRC - Taiwan Computer Incident Response Coordination Center, Chinese Taipei

Currently APCERT jointly sponsors a conference once a year with APRICOT (Asia Pacific Regional Internet Conference on Operational Technologies) and holds steering committee conference calls three times a year and face-to-face meetings twice a year [Ito 03].

2.3.4.3 Asia-Pacific Economic Cooperation (APEC) Initiatives

The Asia-Pacific Economic Cooperation (APEC[29]) is an inter-governmental organization devoted to the promotion of economic cooperation and development. APEC member organizations, called "member economies," include Australia, Brunei Darussalam, Canada, Chile, People's Republic of China, Hong Kong, China, Indonesia, Japan, Republic of Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, Philippines, Russia, Singapore, Chinese Taipei, Thailand, the United States, and Viet Nam. The majority of the work done in APEC is done through working groups [APEC 03].

One group, the APEC Telecommunications and Information (APECTEL) Working Group focuses on connectivity, telecommunication infrastructures, and other opportunities for collaboration, cooperation, and technology transfer [APECTELWG 03a]. This group has also undertaken initiatives related to e-security. One initiative is to foster the development and training of CSIRTs throughout the member economies, including the funding of a project to provide research, consulting, and training relating to the establishment and operation of CSIRTs in APEC economies. The initial developing economies scheduled to receive the training are Chile, Peru, Mexico, and the Russian Federation. The final outcome of the project will not only include a set of workshops and course materials delivered to the participants but

[29] See <http://www.apecsec.org.sg/> for more information on APEC and <http://www.apectelwg.org/apec/main.html> for more information on APEC TEL WG.

also a set of guidelines that member economies can use to help establish teams [APECTELWG 03b].

2.3.5 Initiatives in Latin America

Since the late 1990s and early 2000s, more CSIRTs have been developed in Latin America. Although many teams exist, currently only five teams are FIRST members [FIRST 03]:

- APSIRT – AT&T Latin America - Peru Security Incident Response Team.[30] According to its FIRST Team member information, APSIRT's constituency is "customers of AT&T Latin America - Peru Internet access services."
- CAIS – Brazilian Research Network CSIRT.[31] According to its FIRST Team member information, CAIS/RNP's constituency is "Brazilian academics and research institutions." It has been a FIRST member since September, 2001.
- CLCERT – Chilean Computer Emergency Response Team.[32] According to its FIRST Team member information, CLCERT's constituency is "users and organizations operating under the .cl domain and users and organizations of computer systems operating in Chile."
- NBSO – NIC BR Security Office - Brazilian Computer Emergency Response Team.[33] According to its FIRST Team member information, NBSO's constituency is "Brazil - Internet .br domain and IP addresses assigned to Brazil."
- UNAM-CERT – the CSIRT for the National Autonomous University of Mexico. UNAM-CERT has been a FIRST member since 2001.[34]

A previous CSIRT that was established in Mexico as an initiative from the Instituto Tecnológico y de Estudios Superiores (ITESM) was Mx-CERT, the Mexican Computer Emergency Response Team. This CSIRT was a member of FIRST and hosted the initial FIRST conference held in Latin America, in 1998 in Monterrey, Mexico [FIRST 03]. Mx-CERT is no longer operational.

Many more CSIRTs exist in Latin America besides those that are FIRST members. It is difficult to know the total number, as there is currently no method of identifying and verifying teams. There are various initiatives in different organizations to begin to collect security contact and CSIRT information for Latin American countries. There is no formal regional initiative in Latin America as there is in Europe or the Asia Pacific, such as the TF-CISRT, eCSIRT, and APCERT initiatives. However, in many Latin American countries, established

---

30 For more information on APSIRT, see <http://apsirt.attla.com.pe/>.
31 For more information on CAIS/RNP, see <http://www.rnp.br/cais/>.
32 For more information on CLCERT, see <http://www.clcert.cl/>.
33 For more information on NBSO, see <http://www.nbso.nic.br/>.
34 For more information on UNAM-CERT, see <http://www.unam-cert.unam.mx/>.

CSIRTs have efforts underway to help other teams get started. Other Latin American governments are also looking into creating an incident handling capacity. For example, ArCERT is the CSIRT for Argentinian government institutions.[35]

In discussions with other CSIRTs in Latin America, it was found that many of the CSIRTs already established or those being formed are mostly for government organizations, non-profit organizations, research institutes or universities, and telecommunications organizations.

2.3.5.1 Early Development of CSIRT Capabilities in Latin America

Both Mexico and Brazil seem to be the earlier leaders in CSIRT initiatives. The early development of these teams gives an indication of how teams are being created in Latin America.

CSIRT Development in Mexico

After an incident in 1993 in which a supercomputer facility in Mexico was compromised, the idea to build a small team dedicated to helping system administrators with security problems was implemented. Initially two academic institutions, ITESM and the National Autonomus University of Mexico, were working on computer security initiatives. In the later part of the 1990s the first CSIRT was developed, the previously mentioned Mx-CERT from the ITESM. In 2000 UNAM-CERT was proposed at the National Autonomus University of Mexico. It was created and became a FIRST team member in 2001. Since that time UNAM-CERT has been the point of contact with academic, government, and commercial organizations regarding incident response initiatives. UNAM-CERT also has a major initiative underway to foster and develop CSIRTs within Mexico and to help bring computer security and incident handling into the computer curriculum in Mexican universities.[36]

CSIRT Development in Brazil

The development of CSIRT Capabilities in Brazil started in August 1996, when the Brazilian Internet Steering Committee[37] released the document "Towards the Creation of a Security Coordination Center in the Brazilian Internet."[38] As a result of the discussions about this document, in June 1997[39] the NIC BR Security Office (NBSO)[40] was created to support the Internet in Brazil. It currently works as the focal point for coordinating response to incidents related to Brazilian Internet-connected networks. In August 1997[41] CAIS (the Brazilian Re-

---

35 For more information on ArCERT, see <http://www.arcert.ar/>.

36 The information on CSIRT capabilities in Mexico was contributed by UNAM-CERT.

37 <http://www.cg.org.br/sobre-cg/history.htm>

38 <http://www.cg.org.br/grupo/historico-gts.htm>, available in Portuguese

39 <http://www.cg.org.br/grupo/grupos.htm#Grupo>, available in Portuguese

40 <http://www.nbso.nic.br/>

41 <http://www.rnp.br/_arquivo/documentos/rel-rnp98.pdf>, available in Portuguese.

search Network CSIRT[42]) was created. Also in 1997 the CERT-RS was created, whose constituency is the research network at Rio Grande do Sul state. Since then several other teams have started their operations in Brazil.

Currently there are more than 20 teams established, mainly in the commercial and academic areas. Most are either security teams that perform incident response or are internal centralized CSIRTs.[43]

Another example of the growth in CSIRTS in Brazil can be seen on a web site that lists some other Brazilian CSIRTs.[44] Besides the already mentioned NBSO and CAIS/RNP CSIRTs, other teams listed include those for the Brazilian Federal Police and other CSIRTs for various universities and research institutions and telecommunication institutions. This list gives an indication of the types of non-FIRST member teams that are being created in Latin America.

2.3.6 Developments in Canada

Canada has seen an interest in and development of CSIRTs across its various sectors: commercial, military, government, and education. Currently there are four registered teams from Canada that are members of FIRST [FIRST 03]:

- BMO ISIRT – Bank of Montreal InfoSec Incident Response Team. According to its FIRST Team member information, BMO ISIRT's constituency is "The Bank of Montreal."
- CdnCIRCC – Canadian Computer Incident Response Coordination Centre.[45] According to its FIRST Team member information, CdnCIRCC's constituency includes "sectors comprising the critical infrastructure of Canada—energy and utilities, communications, services (health, financial and food), transportation (all modes), safety (nuclear safety, search and rescue, and emergency services), government (government-wide critical operations)."
- DND CIRT – Department of National Defence CIRT, whose constituency is the Department of National Defence in Canada.
- EWA-Canada/CanCERT – EWA-Canada/Canadian Computer Emergency Response Team.[46] According to its FIRST Team member information, EWA's constituency is "Canadian government, business and academic organizations."

---

42 <http://www.cais.rnp.br/>

43 The information about Brazilian CSIRTs was contributed by NBSO.

44 The list can be found at <http://www.nbso.nic.br/contact-br.html>.

45 For more information on CdnCIRCC, see <http://www.ocipep-bpiepc.gc.ca/>.

46 For more information on CanCERT, see <http://www.cancert.ca/>.

This list gives a good idea of the types of Canadian organizations that are implementing CSIRTs: financial institutions and other commercial organizations, military and police organizations, and government organizations. The 2003 FIRST conference was held in Ottawa, the Canadian capital.

Many different CSIRT initiatives at various levels of government in Canada are being implemented. Work is going on at the country, province, territory, and city level. Some provincial government CSIRTs have been operating for a few years, while others are in the process of standing up their team.

The focal point of incident handling at the country level is the Office of Critical Infrastructure Protection and Emergency Preparedness) (OCIPEP). OCIPEP is a civilian organization operating in the Canadian government's Department of National Defence. OCIPEP works under the concept of partnerships. Its web site states that "protecting critical infrastructure and responding to emergencies is a shared responsibility in Canada, requiring the full cooperation and effort of Government of Canada departments and agencies, provinces and territories, municipalities and the private sector" [OCIPEP 03].

"OCIPEP's Infrastructure Protection Coordination Centre monitors physical and cyber threats (24 hours a day/7 days per week) and serves as a central point of contact for threat and incident information. Related information is currently received from and sent to the Government of Canada, provincial and territorial governments, and the private sector" [OCIPEP 03].

2.3.7 Developments in the United States

Many different types of CSIRTs have also been developing over the years in the United States. As can be seen in the next section, there are currently over 70 U.S. teams that are FIRST members. These teams come from many sectors, including military, government, education, critical-infrastructures, financial, ISP, non-profit, and commercial organizations.

There are many, many more U.S. teams that are not FIRST members. Some of the areas where we see the biggest growth in CSIRTs have been commercial and critical infrastructure organizations. Most branches of the U.S. military have their own CSIRTs. Many federal agencies also have their own teams or are in the process of creating them.

One of the newest areas where we see interest and initiatives in creating CSIRTs is at the state government level. State governments are receiving mounting pressure to meet their compliance requirements with various laws and regulations regarding data privacy and cyber security. In 2003 a report by Zeichner Risk Analytics concluded that the majority of states have not met these requirements and regulations. The report also called for states to work together

to come up with a nationwide process for implementing and developing cyber-security laws and policies [Zeichner 03].

In September 2003, the U.S. Department of Homeland Security (DHS), in conjunction with Carnegie Mellon University, announced the formation of the United States Computer Emergency Response Team (US-CERT). The main goals of the US-CERT will be to work with public and private sectors to

- improve warning of and response to incidents
- increase coordination of response information
- reduce vulnerabilities
- enhance prevention and protection efforts [US-CERT 03]

"The US-CERT will begin as a partnership between the National Cyber Security Division (NCSD) within DHS and Carnegie Mellon's CERT/CC. The US-CERT will grow to include other partnerships with private-sector security vendors and domestic and international organizations. These groups will work together to coordinate national and international efforts to prevent cyber attacks, protect systems, and respond to the effects of cyber attacks across the Internet"[47] [SEI 03].

2.3.8 Other Initiatives in CSIRT Development and Evolution

In 1995 a working group on Guidelines and Recommendations for Incident Processing (GRIP) was formed by the Internet Engineering Task Force (IETF). Its purpose was to develop guidelines for providing consistent information about CSIRTs to those internal and external to a team's constituency.[48] The GRIP Working Group published RFC 2350, "Expectations for Computer Security Incident Response Teams as Best Current Practice" [Brownlee 98]. This Request for Comment (RFC) documented recommendations for what teams should publish about themselves and explained why this information would be useful for users of a CSIRT.

As intruders make more use of home users' computer systems, CSIRTs today are struggling to figure out ways to interact with this type of constituency. Some interesting public outreach projects and services are currently offered by the CERTCC-KR.[49] The initiatives include

- providing free anti-virus software and vaccine programs to elementary and secondary education organizations

---

47 For more information on US-CERT, see <http://www.us-cert.gov/>.

48 The GRIP Working Group was disbanded when its work was completed. Its initial charter can be read at <http://www.ietf.cnri.reston.va.us/proceedings/96mar/charters/grip-charter.html>.

49 For more information on CERTCC-KR, see <http://www.certcc.or.kr/>.

- operating a 24x7 phone number for anyone to call and report computer security incidents and receive assistance in resolving them. This initiative is known as the Cyber 118 Operation.
- providing a test lab for information security products. This lab is available for free to industry.

These initiatives show the diversity of CSIRT services.

2.3.9 Today's Activities

Today there are many more CSIRTs in operation and many different projects underway to facilitate coordination and information sharing between teams and to standardize terminology and processes in CSIRT operations. Some of the issues being discussed at the time of the publishing of this report in 2003 still reflect the original goals and objectives of early discussions, namely, to create an effective way to coordinate information sharing, analysis, and response between teams. Teams today are still investigating the tools required for this type of coordination and also what organizational structures will work best. Many areas are talking about creating regional coordination mechanisms to focus on particular geographic areas. How these regional mechanisms will then coordinate has yet to be determined. Other areas of discussion and activity include finding ways to standardize work and information exchange between CSIRTs, the impact of changing laws and regulations on CSIRT activities and organizational protection strategies, and the difficulty in finding, training, and retaining qualified incident handling staff. These activities, as well as information about how CSIRTs are currently operating, are discussed in the next section, "Current State of the Practice of CSIRTs."

3 Current State of the Practice of CSIRTs

This section takes a look at the information gathered through our research efforts. It pulls together information from our survey, literature search, interviews, and research. The main focus is to provide a picture of the current CSIRT community and how teams go about their work. We will discuss the organizational structure and processes of teams, the problems in determining the actual number of teams, the types of services being offered by teams, the type of training available for teams, the types of projects being implemented by teams, and the major impacts on teams, such as changes in intruder trends and laws.

Topics include the following:

- the number and types of CSIRTs today, including some background on the change in number and type of CSIRT in the past few years
- the organizational structures of CSIRTs, including constituency and mission, location, hours of operation, authority, and reporting structures
- types of CSIRT funding and the costs of operating a CSIRT
- the types of services offered by different types of teams
- the skill sets and staff positions needed on a team, along with a review of available training
- how CSIRTs receive, record, track, categorize, and prioritize incident data
- with whom CSIRTs coordinate response activities and share data
- current influences on CSIRT operations that can potentially affect the creation and operation of CSIRTs
- changes in the nature and type of intruder threat and the impact this has had on the day-to-day operations of CSIRTs
- an overview of some of the recent projects undertaken by or beneficial to the CSIRT community

3.1 Number and Type of CSIRTs Today

It is difficult to determine exactly how many CSIRTs are in existence today. Some of the reasons for this difficulty are as follows:

- There is not one entity for registering the existence of a CSIRT, so one must look at various lists or registrations to try to pull this information together.
- There is not one clearinghouse or other place to validate the existence of a team.
- Not all teams are publicized, since many internal teams do not want to tell anyone of their existence.
- Not all teams are formalized entities (ad hoc teams, for example, aren't called CSIRTs even though they perform CSIRT work), so it is difficult to determine how to include them in a list of CSIRTs.
- There is no mechanism to reach all CSIRTs and gather input.
- There are no standard requirements to determine if a group is a CSIRT or not.

Because of these issues we do not have a comprehensive list of CSIRTs and can only estimate the total number of teams. We will take a look at existing lists or registrations of CSIRTs that are available and will review the change in number and types of CSIRTs on them. Based on those changes, we can make some predictions concerning general changes in the CSIRT community. The main lists we have access to are

- First Team Members List
  <http://www.first.org/team-info/>
- Directory of European CSIRTS
  <http://www.ti.terena.nl/teams/>
- Asia Pacific Computer Emergency Response Team members list
  <http://www.apcert.org/member.html>

Teams belonging to these lists have gone through some review or accreditation process before being accepted into the related organization. Because of this, we will refer to the teams on these lists as "registered" teams, as they are recognized as established teams.

3.1.1 The Growth of FIRST Teams

Since 1991, through a steady influx of new teams, FIRST has grown today to include 151 members. Figure 4 shows this increase, as well as the geographical breakdown of FIRST teams between Asia and the Pacific, Europe, North America (Canada and the United States), and Latin America.[50] As of August 2003 there were no FIRST members from Africa.[51]

---

50 Please note that FIRST team data is only through August 2003.

51 We only consider the teams that are still active as of August 2003. As previously stated, in 1990 eleven teams started the international network, but only five of them are still active.

Reproduced From
Best Available Copy

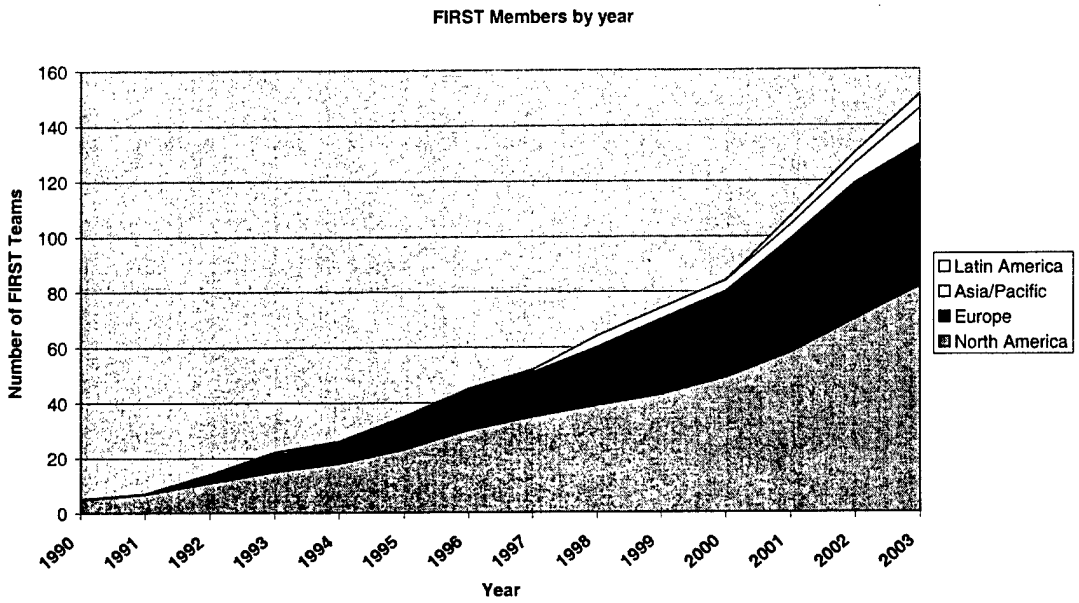


Figure 4: Growth of FIRST Teams since 1990

As of August 2003, the actual number of FIRST teams, broken down by region, was

- Asia/Pacific: 13
- Latin America (South America, Central America, and Mexico): 5
- Europe: 51
- North America (Canada and the United States): 82

As can be seen in the chart above, North America has had a continuing increase in the number of teams over the years. Beginning in 2000, there was a sharper increase in the number of European teams. Most Asia/Pacific teams joined FIRST in or after 1997-1998.The majority of the Latin American teams joined FIRST beginning in 2001.

3.1.2 Growth in European CSIRTs

Another set of teams for which we have good statistical data is the European teams. This is because the Trusted Introducer has created a directory of all known European teams,[52] whether they are FIRST members, Trusted Introducer members, or not in either group. This does not mean that every team in Europe has been identified; there are probably many local teams that have not publicly announced themselves.

[52] <http://www.ti.terena.nl/teams/>

Table 4 combines the total number of European teams who are FIRST members with non-FIRST members identified in the European CSIRT directory. This information is collected through August of 2003.

Table 4: Total Registered European CSIRTs

Year	European FIRST Members	European Non-FIRST Members	Total for Europe
2000	31	22	**53**
2001	41	28	**69**
2002	48	28	**76**
2003	51	33	**84**

Looking at the numbers, it is clear that the number of non-FIRST teams in Europe is still considerable, approximately one third of the total registered European teams. It also seems a fairly stable number over the past few years. The larger growth in European FIRST teams indicates that it is attractive to become a FIRST member once a team is established.

3.1.3 Total Registered CSIRTs

As previously discussed, registered CSIRTs are considered those who have gone through some accreditation process and registered with FIRST, APCERT, or the Trusted Introducer.

Table 5 and Figure 5, which list the total registered teams broken down by geographic region from 1990 through August 2003, show that the biggest growth in CSIRT development and team establishment has been in Europe and North America (Canada and the United States). This is not surprising, as the initial CSIRTs were all in the U.S., with Europe being the next area to establish teams.

Table 5: Geographical Distribution of Registered CSIRTs

Year	North America	Europe	Asia/ Pacific	Latin America	Total
1990	5	0	0	0	5
1991	7	0	0	0	7
1992	11	3	0	0	14
1993	15	6	1	0	22
1994	18	9	1	0	28
1995	23	14	1	0	38
1996	30	17	1	0	48
1997	35	19	1	0	55
1998	39	24	4	0	67
1999	43	30	6	0	79
2000	49	53	7	0	109
2001	58	70	9	3	140
2002	66	76	12	4	158
2003	82	84	17	5	188

Reproduced From
Best Available Copy

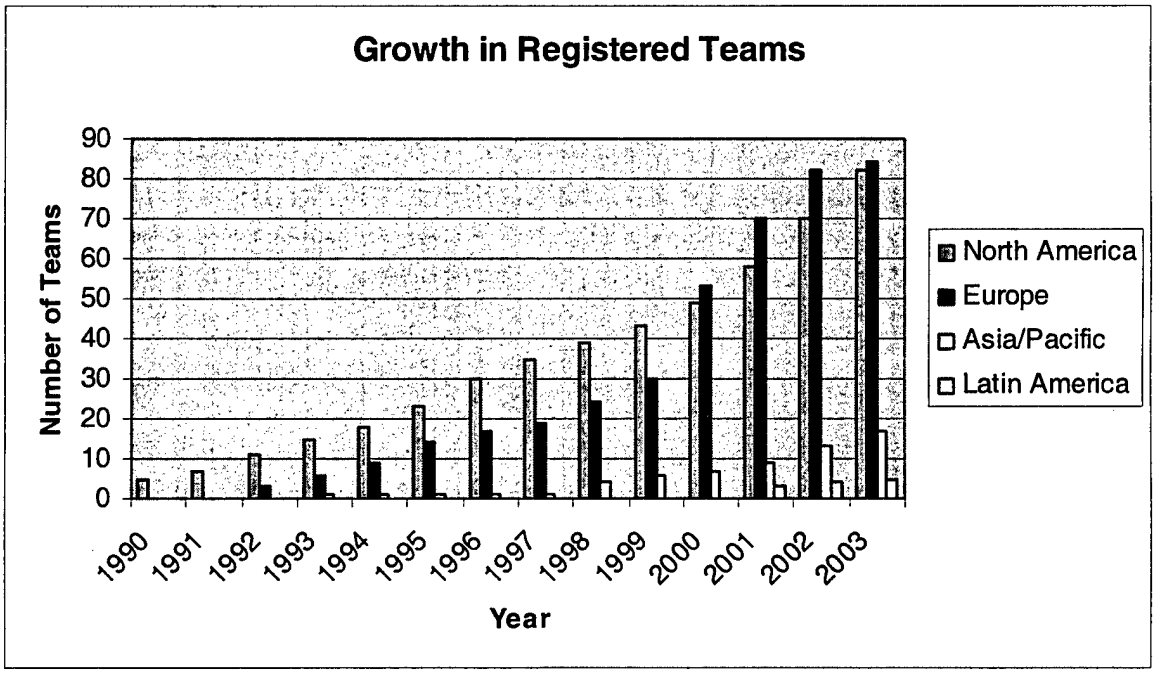


Figure 5: Growth in Registered Teams by Geographic Distribution

In looking at the growth of teams each year, it can also be seen that the most significant growth has occurred in the last four years, as the total number of registered teams doubled from 79 in 1999 to 158 in 2002.

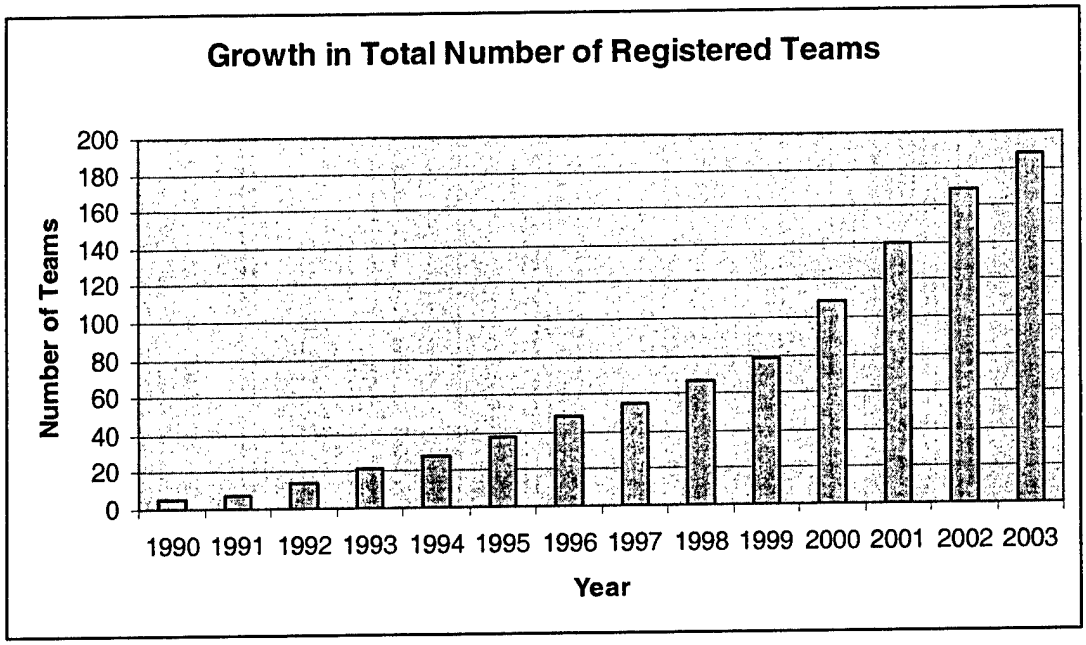


Figure 6: Growth by Year of Total Number of Registered CSIRTs

Reproduced From
Best Available Copy

3.1.4 CSIRT Growth by General Category

Figure 7 lists the regional distribution of the registered teams and shows their growth in five general sectors. The five general sector categories are government, research, commercial, national, and other. A "national" team claims a whole nation or country as its constituency and has sufficient proof to show that the team is indeed regarded by that country as a CSIRT for that constituency. Some national teams are government funded. Others are an outgrowth of a research network that has expanded from handling incidents for just that network to handling them for a whole country.[53]

[53] We applied these categories to the teams ourselves and therefore might have made a mistake in assignment, but the trend information is still correct. This analysis was done to look only at general trends.

Reproduced From
Best Available Copy

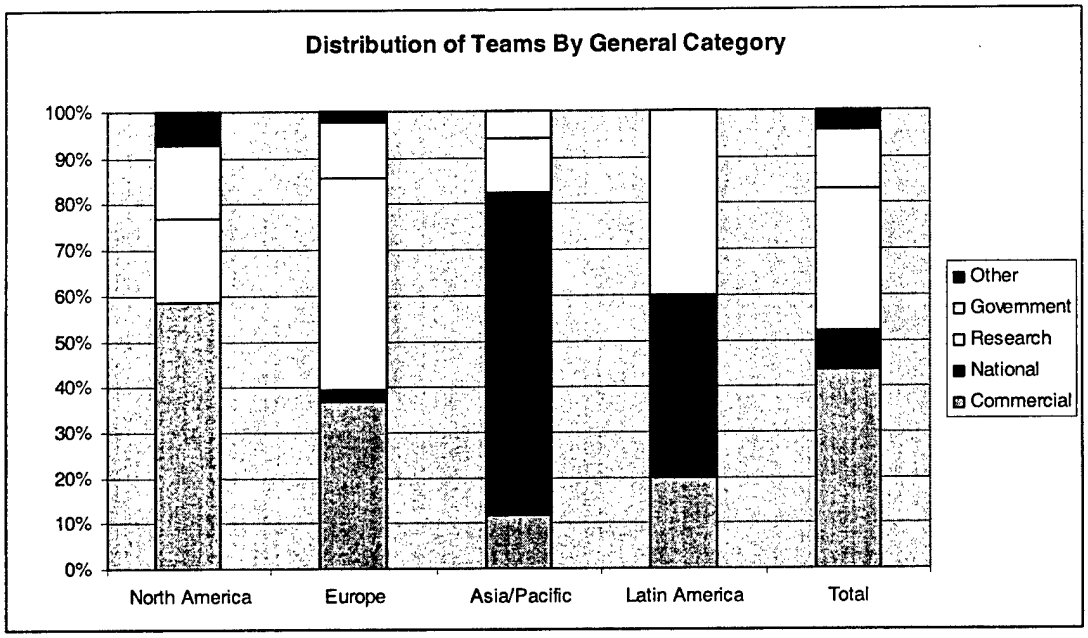


Figure 7: Sector Distribution of Registered CSIRTs by Geographic Area

Figure 7 shows some interesting but not unexpected trends:

- In North America (Canada and the United States) we see a majority of commercial teams and a lower number of research-oriented teams.
- In Europe, the relationship between commercial and research teams is just the opposite. This is a historic trend, as nearly all European countries have national research networks and these organizations have been the early adopters since 1992. Over the years these research-oriented CSIRTs were responsible for raising the awareness of ISPs and other commercial organizations, which then established their own teams.
- In the Asia Pacific region, the majority of the "registered" teams are national teams, most or all of them funded by the corresponding national government.
- In Latin America the low number of teams precludes identifying any clear emerging trends, although we see evidence of research, commercial, and national teams in existence. We expect that this diversity will continue.

In Table 6 we categorize the large number of teams in North America and Europe by more detailed sectors.

Table 6: North American and European CSIRTs by Subcategory

Subcategory	North America	Europe
Banking and Finance	8	4
Managed Security Service Provider[54]	15	8
Commercial	12	5
Vendor	10	1
ISP	3	13
National	0	2
Research Network	1	28
Research Organization	2	2
University	12	9
Military	5	2
Government	8	8
Health	2	1
Individuals	4	1
Total	**82**	**84**

The following observations can be made about this data:

- Not surprisingly, most vendor teams are located in the U.S., or at least that is where their development group and product security teams are located.
- While many more managed security service providers and commercial companies have a team in North America, most of the ISP teams are in Europe.
- As previously stated, Europe is characterized by the many national research network teams, but it is interesting that a similar number of universities in North America and Europe have their own teams established.

[54] These are sometimes called "managed service providers."

Reproduced From
Best Available Copy

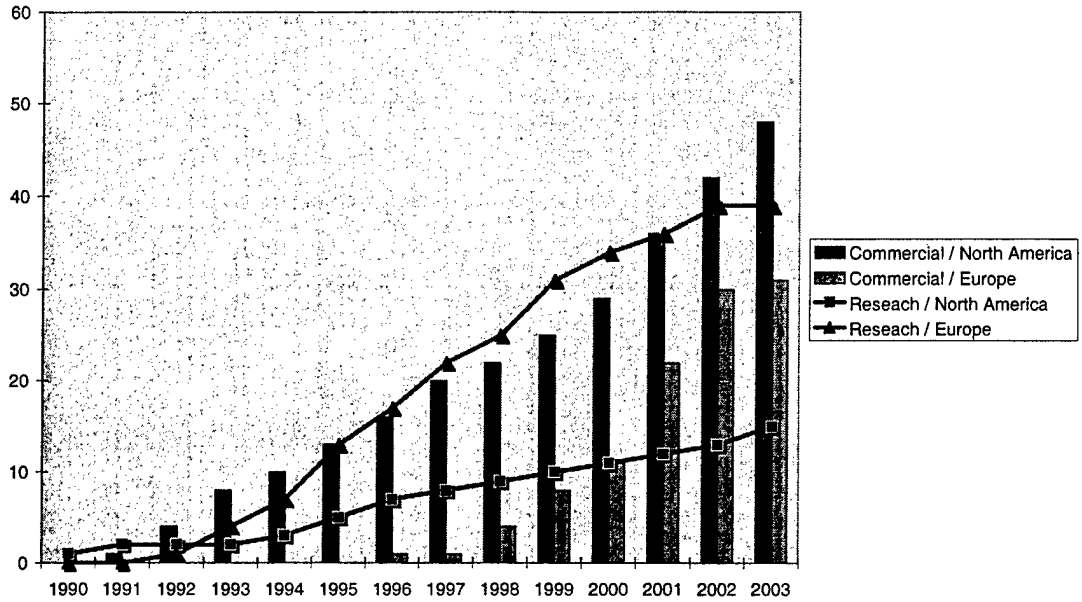


Figure 8: Differentiation of Trends in North America and Europe

Figure 8 shows the following trends:[55]

- The growth rate of research-oriented teams in Europe is decreasing. This is because many of the research networks and large universities already have their own teams and the smaller universities do not seem to have the need to create such a team. The growth that did occur was due to the remaining larger universities establishing teams when they realized the need.
- The growth rate of commercial teams in Europe has begun to exceed that of research teams in Europe, while the number of research teams and commercial teams has steadily increased in North America. The number of commercial teams in North America is still four times that of the number of research teams.
- It appears from the data available for registered teams that the increase in the number of teams in North America is primarily due to the growth of commercial teams, while the increase in the number of teams in Europe was initially due to the establishment of research network teams and is now primarily due to the growth of commercial teams.

[55] Keep in mind that the numbers for North America are based on the registered teams and that the real numbers might be higher by 40 to 50 percent. Since we assume that the increase would be equally proportional for each category and subcategory, our further conclusion seems to be in keeping with these trends, but should be taken with some caution.

3.1.5 Other Trends

Other trends we have observed include the growth of teams in particular sectors. The CERT/CC has seen over the past few years a marked increase in the number of teams from banking and finance, insurance, law enforcement, and critical infrastructures such as power and energy, transportation, and information and communications. There has also been an increased interest in creating CSIRTs for federal government agencies, U.S. state governments, and national teams for countries in all areas of the world. Figure 9 shows the breakdown by sector of organizations that have attended CERT/CC CSIRT courses from 2000-2002.

In the past seven years we have seen another trend as incident response services have become offered, along with a range of security services, by consulting or managed security service providers (MSSP). As more and more organizations require such support, they now have a choice of creating their own team or hiring a team with the skills and experience to do the job. Table 6 shows that as of August 2002, there were approximately 23 MSSP CSIRTs that were either members of FIRST or the European CSIRTs Directory. The first registered MSSP CSIRTs were in 1996. Since that time one or two have been added every year, with a large increase in 2001.

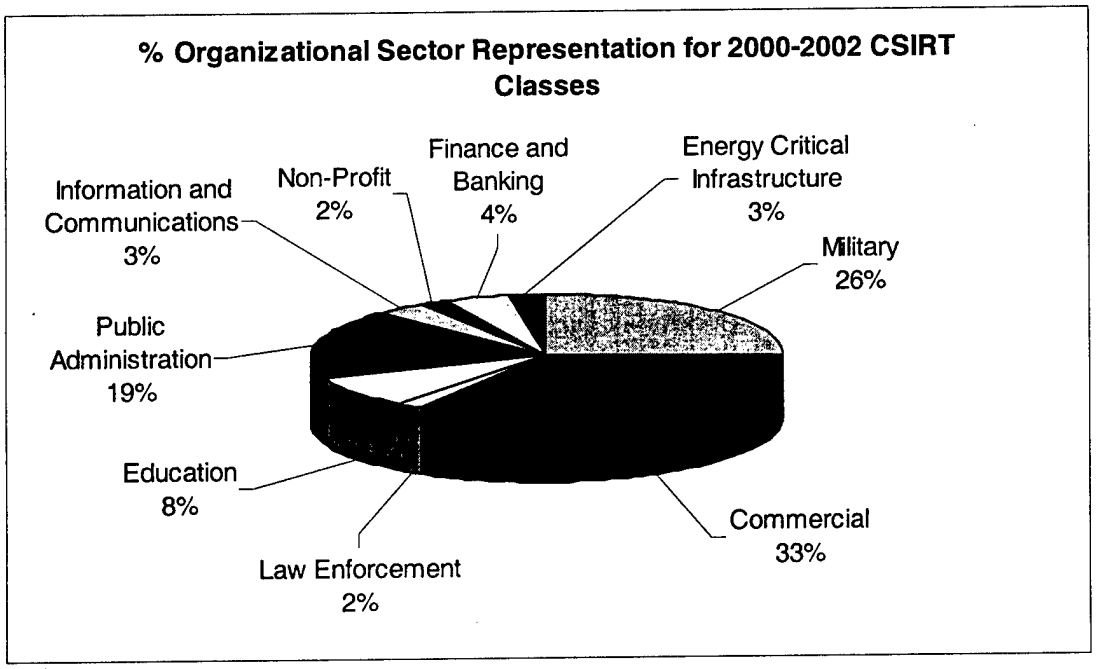


Figure 9: Organizational Sector Representation for 2000–2002 CERT/CC CSIRT Classes

Another good example of the large number of teams that exist but are not registered comes from work that is done by CERTCC-KR. This team works with a group of 200+ established CSIRTs in Korea through an initiative called "CONCERT." These teams come from universi-

Reproduced From Best Available Copy

ties, ISPs, security companies, and other public and private organizations. These types of public-private coordination efforts are becoming popular in various countries around the globe.

3.1.6 The Spread of CSIRTs

Most descriptions about how CSIRTs are formed come from anecdotal information based on our experience and the experiences of other teams. Here are some observations concerning how new teams are supported and the changes we have seen in how this support has been provided.

3.1.6.1 Support from Existing Teams

The history of CSIRTs, while only covering 15 years, has shown that existing teams provide a tremendous amount of support to new teams as they are being established. This support involves sharing of policies and procedures, provision of training, and sponsorship for membership in organizations such as FIRST. An example of this support and how it has helped promote the establishment of more teams can be seen in Figure 10. This figure shows the interactions between various types of teams that sponsored another team, and how this trend carries on as those teams in turn sponsor other teams. Although team names are not mentioned, the figure is based on actual data, and is an illustration of how FIRST sponsorship has worked.

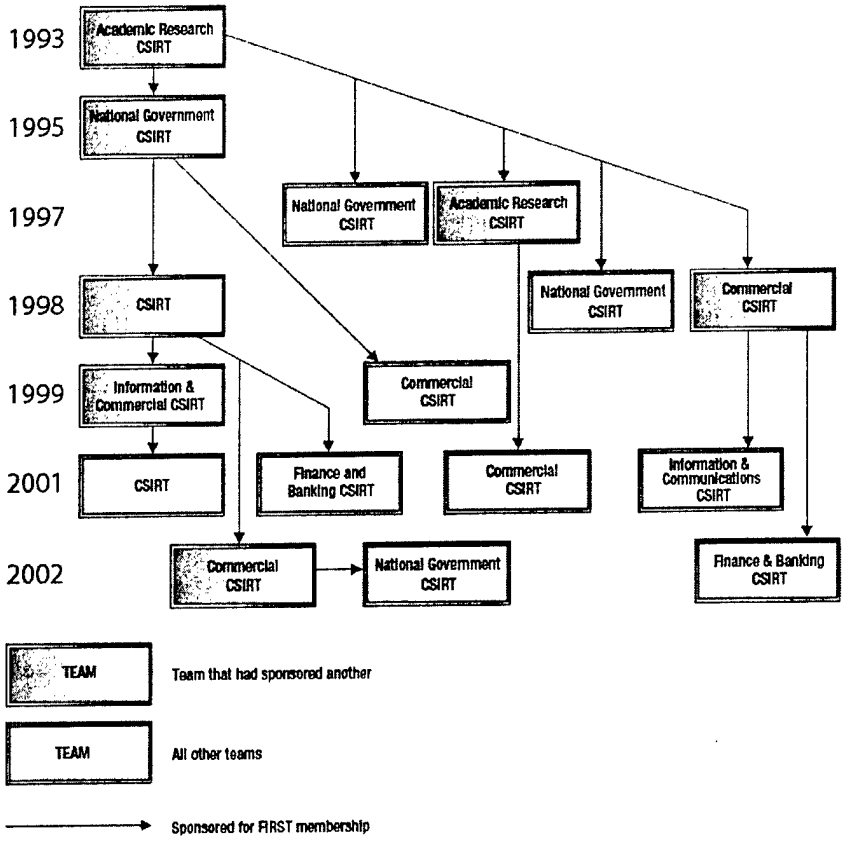


Figure 10: Example of Team Sponsorship and Propagation of CSIRTs

Newly forming teams have benefited from site visits to established team sites; reviewing other teams' web sites, incident reporting forms, and guidelines; and networking at conferences such as the annual FIRST conference or meetings such as those regularly held by the TF-CSIRT. Many teams are quite willing to receive visitors and share their experiences in establishing their own team. They are also generally very supportive. In addition, many existing teams still consider it important for their day-to-day function to meet other teams, as any interaction with those teams will be easier once they have established contact. Such meetings help teams gain a better understanding of each other and establish a means of communication.

As mentioned in Section 1.7, "About the Literature Search," many teams have also made articles and publications available about their process for establishing their team. These documents help new teams have an idea of a process to follow and also help teams avoid pitfalls and be aware of issues that will need to be addressed. Prior to 1998—the year the first edition of the CERT/CC *Handbook for CSIRTs* [West-Brown 03] was published—no comprehensive document was available for interested organizations to learn about the challenges and tasks

associated with establishing a CSIRT.[56] Today there are many articles and books available to help teams get established and sustain and improve their operations.

3.1.6.2 Movement of Personnel

Over the years we have seen a growing demand for personnel with skills in establishing and managing a CSIRT. We have also seen a shift of personnel as those with that experience move on to new teams or to consulting services that specialize in CSIRT setup. Movement of personnel between teams is another way to spread incident handling knowledge. In addition, experienced teams and key personnel have started to deliver training and tutorials on establishing and managing a team and on incident handling and forensic analysis.[57]

As the need for more staff trained in security issues and incident response has become apparent, more post-secondary education institutions have established programs in information assurance and computer security. This has provided a needed supply of people who are trained to understand and handle incidents. This is discussed in more depth in Section 3.6, "Training and Certification."

3.2 CSIRT Organizational Structure

Organizational structure refers to how a CSIRT is set up or organized to do business. This includes who the CSIRT is providing service for, along with what goals, objectives, and functions the CSIRT has. It also includes the CSIRT's place in the organization, which includes who the CSIRT reports to in the management hierarchy and what department or group the CSIRT is located in. It can also include what authority the CSIRT has. To gather information on the state of the practice of CSIRTs concerning these organizational issues, we asked various CSIRTs to tell us this information by participating in the pilot CSIRT Organizational Survey, which is discussed in Section 1.6, "About the Survey."

3.2.1 Constituency

Within the incident response community, the *constituency* generally refers to the individuals or organizations that are served by the CSIRT. These constituent members share some type of specific characteristics (network, sector, location, agency, etc.) and are identified as employees, customers, subscribers, clients, or even information consumers. The constituency itself can be a number of different entities, such as single departments within an organization, a university, a company, government or military agency, national or international corporations,

---

56 Certainly there were already papers that highlighted specific issues, but there was no single document that covered the whole breadth of information related to creating and operating a new team.

57 Available training is described in Section 3.6 and in Appendix C.

service providers, or nation states [West-Brown 03]. Whomever it serves, the CSIRT must clearly identify the constituency to ensure that they are providing services to appropriate individuals.

The majority (86%) of the CSIRTs participating in the CSIRT Organizational Survey stated that they did have an identified constituency. Some of the new and developing teams stated that they were still in the process of identifying their constituency.

The types of constituencies identified by the survey participants are shown in Figure 11.

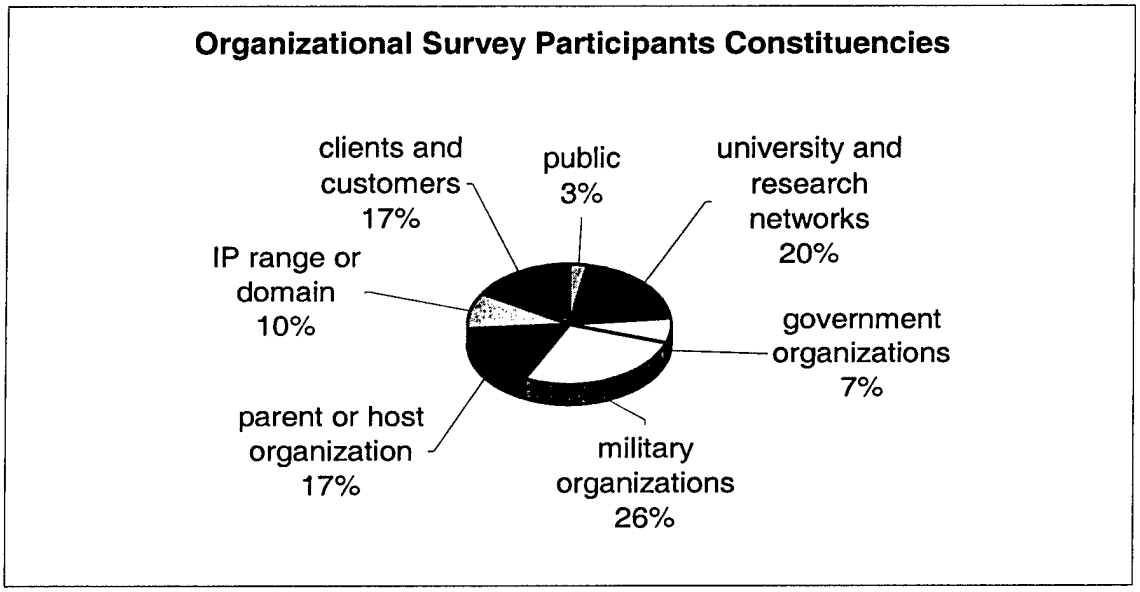


Figure 11: Constituencies of Survey Participants

As would be expected, the educational sector CSIRTs identified their parent research network or university as their constituency. The military CSIRTs identified other areas of the military or specific military departments, and the information and communication CSIRTs identified their customers or supported IP ranges and domains as their constituency. The non-profit CSIRTs identified the public or their host organization as their constituency.

It should be pointed out that a CSIRT does not just interact with its constituency. A CSIRT may also communicate with other CSIRT teams and security experts, individuals outside of the CSIRT who are reporting problems, representatives from law enforcement, or vendors. Many CSIRTs, if time permits and if their policies allow, will try to help those outside of their constituency when reporting problems. But the constituency is the formal group that the CSIRT provides service for according to its mission.

3.2.2 Mission

Because of the wide variety of CSIRTs and the diverse constituencies they serve, there is no one standard mission that all teams proclaim. The majority of the CSIRTs participating in our survey stated that they have an identified mission statement and included that statement or an approximation. Most mission statements included references to

- protecting and maintaining the security of constituent systems
- managing and coordinating incident response activities
- minimizing damage in the event of a security incident
- educating the constituency on security issues and best practices

Many teams define their mission on their main web page and in literature describing their services. Mission statements can easily be found for a large number of national and coordinating CSIRTs. It is more difficult to find mission statements for MSSP CSIRTs, as their web pages are devoted to the types of services that clients can purchase.

An example of a national CSIRT mission can be seen on SingCERT's "About SingCERT" page [SingCERT 03]:

> "Mission
>
> One Point of Trusted Contact
>
> Facilitate Security Threats Resolution
>
> Increase National Competency in IT Security"

The roles and responsibilities of the team, the mission and goals that it has, and how the team will operate must be identified and refined as the CSIRT is being planned and developed. One thing we have also learned is that teams evolve over time. Effective CSIRTs must be able to adapt to changes in funding, mission, constituency, management, or staffing. This has happened to a number of teams, including the CERT/CC, AusCERT, and DFN-CERT, to mention a few.

3.2.3 Organizational Placement of the CSIRT

There is no clear standard or consistent placement or location of a CSIRT within the organizational reporting structure of a host or parent organization. Current teams are positioned across a wide range of departments, including the information technology (IT) department, security department, and even the audit or compliance department. A CSIRT can also be its own department not located within any other area. It is difficult to determine where a team is located in the organization without looking at an organization chart or asking the team. For MSSP CSIRTs, you may be able to find the division the service is located in by looking at

their web pages. This may also be true for university or research networks. But for local and commercial teams, that information is not usually available.

There is also no standard manager to which a CSIRT reports. The title of the manager often relates to the department in which the CSIRT is located and the title that department's manager has been given, such as "Head of Network Services" or "Director of Telecommunications." Depending on who you talk to in the CSIRT community, you will get a variety of answers to the question "To whom should a CSIRT report?" Some will say they should report to the CIO, others to the CSO, and others to the head of audit or the compliance divisions.

To find out more information, we asked in our survey where CSIRTs were organizationally located and to whom they reported. Participants in the CSIRT Organizational Survey cited the IT department 41% of the time as their location in the hierarchical structure of their parent or host organization.[58] The next most frequently cited location (24%) was for CSIRTs that are separate groups outside of any existing department.

Looking at the survey data for the sector in which a CSIRT is located and its organizational placement, the following trends can be observed:[59]

- The majority of the military CSIRTs were located within the IT department.
- Almost all participating educational sector CSIRTs were located in the IT department of the parent university or research network.

There were no other correlations based on sector.

3.2.3.1 To Whom the CSIRT Reports

The survey data also showed no clear or consistent reporting structure for CSIRTs.

- 38% of the participating CSIRTs stated that they report to someone other than the CIO, IT manager, CSIRT manager, or security manager. Most of the teams identified an organizational department or manager to whom the team reports.
- 31% stated that they report to the CIO.
- The only correlation between the sector and the reporting structure was in the banking and finance sector, where all participating teams reported to the CIO. Across the other sectors, the teams reported to various other managers.

---

58 In an informal survey of 14 CSIRTs done by the CERT CSIRT Development Team in 2000, the majority of the teams also identified this location as the department in which the CSIRT was positioned.

59 See page 16 for a list of all sectors used in the survey.

3.2.3.2 Organizational Model

The various organizational models for CSIRTs are described in Section 2.2, "Types of CSIRTs." The last part of that section details the categories used in the survey.

The largest number of participating CSIRTS (34%) identified the centralized CSIRT model as their current organizational model.[60] This type of team is situated in one location and usually performs CSIRT work 100% of the time. The rest of the teams were fairly evenly distributed across the following categories: ad hoc team (13%), coordination center (13%), combined team (17%) and distributed part-time team (21%).

The only correlation between sector and team model in the survey data was in the information and communication sector, where most participating CSIRTs identified themselves as having some type of distributed team, whether it was ad hoc, dedicated distributed, or combined. There was no other correlation in the data collected between what sector the CSIRT was located in and what type of CSIRT model the team had.

3.2.4 CSIRT Authority

"Authority" describes the control that the CSIRT has over its own actions and the actions of its constituents related to computer security and incident response. Authority is the basic relationship the CSIRT has to the organization it serves.

According to the *Handbook for CSIRTs*, there are three levels of authority or relationships that a CSIRT can have with its constituency [West-Brown 03]:

- Full authority: The CSIRT can make decisions, without management approval, to direct response and recovery actions. For example, a CSIRT with full authority would be able to tell a system administrator to disconnect a system from the network during an intruder attack.
- Shared authority: The CSIRT participates in the decision process regarding what actions to take during a computer security incident, but can only influence, not make, the decision.
- No authority: The CSIRT cannot make any decisions or take any actions on its own. The CSIRT can only act as an advisor to an organization, providing suggestions, mitigation strategies, or recommendations. The CSIRT cannot enforce any actions. For example, the CERT/CC is a CSIRT that has no authority over its constituency, which is the Internet community.

---

[60] See Table 2 for descriptions of team models.

A CSIRT, due to its position, may also be able to exert pressure on the constituent to take a specific action. An ISP, for example, may be able to force its constituents to take a specific action or face discontinuation of Internet services [West-Brown 03].

When CSIRT organizations first began to form, most of them had "no authority." These were mostly national CSIRTs, university or research CSIRTs, and coordinating CSIRTs. Over time as more commercial and local teams were established, these types of teams required more authority to perform their work. We see today that many commercial, educational, and military teams have full or shared authority over their constituency systems.

The most frequent type of authority cited by the CSIRTs participating in the survey was full authority (34%); this crossed the various sectors and categories of CSIRTs. Others identified that they had no authority (24%) or shared authority (24%).

The only correlation with sector and CSIRT authority was that all participating non-profit CSIRTs stated that they had no authority. No correlations were identified between the CSIRT model and the assigned CSIRT authority.

3.3 Funding and Costs

One question we have been asked quite frequently is "How much does it cost to start and operate a CSIRT?" Unfortunately, the answer is not easy; there is no one figure that can be given for what a CSIRT will cost to set up and operate. There is also not much literature on this topic, and what is available is generally anecdotal rather than quantitative in nature.

The costs for setting up a team depend on the circumstances and environment in which the team is established. An internal team that is distributed may not need additional salary or equipment costs while a new team being set up in its own department will incur many more costs. CSIRT costs will include not only start-up costs (software, computing equipment, capital furniture expenditures, supplies, Internet domain registration fees, facilities costs, phones, fax machines) but also personnel costs (salaries and benefits). Once the CSIRT is operational, there will be continuing sustainment costs, both for operational expenditures (ongoing facilities maintenance, support of equipment, upgrades, supplies, travel) and personnel costs (raises, professional development and training).

In this section we look at the ways CSIRTs are funded today and the types of budgets they have, and then discuss issues in determining the cost of incidents.

3.3.1 Funding Strategies

Several strategies exist for funding a CSIRT. They are listed in Table 7.

Table 7: CSIRT Funding Strategies

Strategy	Description	Example
Membership subscriptions	time-based subscription fees for delivery of a range of services	AusCERT has a membership subscription [AusCERT 03]
contract services or fee-based services	payment for services as delivered	CanCERT provides for-fee services, MyCERT, at one time had for-fee services [CanCERT 03, MyCERT 03]
government sponsorship	a government department funds the CSIRT	FedCIRC is sponsored by the U.S. government
academic or research sponsorship	a university or research network funds the CSIRT	CERT-NL is sponsored by the SURFnet research networks [CERT-NL 03]
parent organization funding	a parent organization establishes and funds the CSIRT	local teams such as those created by Siemens or MCI WorldCom [FIRST 03]
consortium sponsorship	group of organizations, government entities, universities, etc. pool funding	
a combination of the above	for example, funding is provided through government funding and private contract	CERT/CC is funded by government and private sponsorship

CSIRTs are most often funded by a parent organization, whether it is a university, commercial organization, military organization, or government entity.

This was supported from the data collected in the CSIRT Organizational Survey, where 55% of the participating teams identified their funding as coming from their parent organization and 45% said their funding came from the government. Only a few of the CSIRTs' funding came from more than one category. Only a small number of CSIRTs indicated that they charged fees for their services (10%). We of course would expect that MSSP CSIRTs would be one type of team that charged fees for their services. However, there are other teams that also charge. Some teams provide a set of public services and then a higher level of service can be acquired through some form of contracted services. CanCERT, for example, is an MSSP that has a set of public services and has additional services that can be purchased. The public services include international coordination and limited incident response [CanCERT 03]. The client services include alerts and advisories, help desk, and informational resources.

Malaysia Computer Emergency Response Team (MyCERT) is not an MSSP but at one time it offered some services for free and additional or special services for a fee[61] [MyCERT 03].

One of the biggest problems faced by CSIRTs is the ability to obtain and maintain funding. In the book *Incident Response*, Kenneth van Wyk and Richard Forno point out that it can be very difficult to get sufficient funding for the team because "information security, in general, plays a supporting role...security functions are not revenue-generators, they are revenue consumers." As a result, many organizations are challenged to find ways to make a business case for funding. The authors also suggests being "aggressive, assertive, and confident" in presenting a funding case to management. CSIRTs might also consider diverse mechanisms to obtain funding—levying a tax on business units or charging a fee for services [van Wyk 01]. Another idea to save costs is to start with an ad hoc team, one that is pulled together to handle an incident. The composition of the ad hoc team comes from other parts of the organization. Staff that perform job functions related to IT maintenance and security are also assigned incident response tasks. For such a model to work successfully, however, just making staff assignments isn't enough to have a good response capability; staff, management, and the constituency need to understand that incident response takes priority over other tasks. If this is not handled correctly it will cost the organization more by having an inadequate and possibly incomplete response.

3.3.2 Budgets

CSIRT budgets are as diverse as the types of teams. Factors influencing budget costs include the type of industry sector the CSIRT is in (which can influence salary costs), the number of services to be offered, and the assistance provided by other areas of the organization (which could cut down on the amount of staff and resources needed).

Survey participants were asked to identify what budget range most closely fit their CSIRT budget (including salary costs). The categories used were as follows:

- Under $50,000 USD
- Between $50,000 and $100,000 USD
- Between $100,000 and $500,000 USD
- Between $500,000 and $1,000,000 USD
- Between $1,000,000 and $2,500,000 USD
- Between $2,500,000 and $5,000,000 USD
- Above $5,000,000 USD

---

[61] According to their current web site, MyCERT no longer offers these special services. This information came from their web site in 2002.

Reproduced From
Best Available Copy

Figure 12 shows the breakdown of budgets indicated by the survey participants.

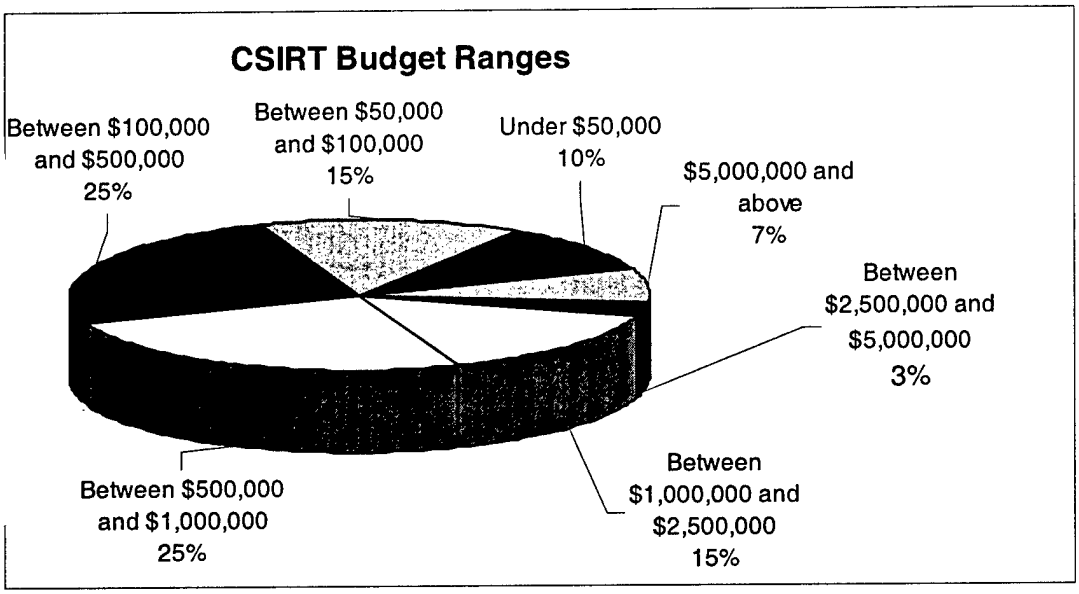


Figure 12: Budget Ranges for CSIRT Organizational Survey Participants

The 7% that said their budgets were above $5,000,000 were all military CSIRTs. The majority of the remaining CSIRTs identified their budgets as ranging between $500,000 and $1,000,000 (25%) and between $100,000 and $500,000 (25%). Therefore, 50% of the participating CSIRTs indicated that their budgets were between $100,000 and $1,000,000. Educational and non-profit CSIRTs, as expected, had the lowest budgets. No other trends by sector were seen.

3.3.3 Staff Costs

In the Internet Security Systems (ISS) white paper "Computer Security Incident Response Planning," the amount quoted for security administrators and consultant salary costs (obtained from a January 2001 SysAdmin, Audit, Network, Security [SANS] Security Alert) ranged from approximately $60,000–$80,000 per year [ISS 01]. This figure applies to those who perform system and network administration. The ISS report also quoted a Gartner estimate that a dedicated two-person incident response team will cost $251,000 in the first year for capital expenditures, with $324,000 per year for salaries, benefits, and training. Additionally, Gartner's numbers for external investigation and other forensics services were in the $100,000 range, for providing specialized skills in the collection and analysis of incident information [ISS 01]. External staff undertaking this type of work will generally need more specialized training in data collection, the use of analysis tools and techniques, and knowledge in handling such information to ensure that any potential evidence will be admissible in a court of law. ISS also mentions that it may be difficult (and costly) to hire and retain a cadre

of such expert staff even for larger companies; while for smaller organizations the costs would be prohibitive.

3.3.4 The Cost of an Incident

In trying to determine the cost of a team, many organizations try to first determine how much an incident or threat will cost to compare this with the cost of mitigating the incident. To do this, organizations must find a way to quantify the cost of an incident.

3.3.4.1 Incident Cost Analysis and Modeling Project (ICAMP)

Two studies that were done to determine a process for quantifying the costs of incidents are the "Incident Cost Analysis and Modeling Project (ICAMP) I" [Rezmierski 98] and "Incident Cost Analysis and Modeling Project (ICAMP) II" [Rezmierski 00], which sought to provide a way to measure loss to universities from incidents in computing environments. The 1998 study calculated costs for 30 incidents at a little over $1 million and provided an estimate of the actual costs for particular IT incidents. It includes sample incident types and templates that can be used by others to calculate incident costs.

The ICAMP II study was designed to provide more information about incident data. This second study gathered information related to incidents and their costs and chose to divide the incidents into two broad types of activities. The first was categorized as "Service Interruptions" and included incidents separated into the following:

- compromised access
- hacker attacks
- insertion of harmful code
- denial of service

The second type of activity included in the data collection was "copyright violations" and they included distribution of illegal software (e.g., MP3 and "warez"). Based on these categories (service interrupts and copyright violations), the study revealed that the average cost for 15 incidents included in the study was just over $59,000.

A further breakdown resulted in the following costs based on type of incident:

- a compromise: $1,800
- harmful code: $980
- denial of service: $22,350
- hacker attacks: $2,100
- copyright violations: $340

The authors point out in the second study that the focus was on specific types of incidents that participating schools believed were on the rise. They also stated that they used the "most conservative figures for calculating costs in all cases" [Rezmierski 00].

Another result of the ICAMP studies confirms an observation that the CERT CSIRT Development Team has made: there is a lack of robust database tools to collect, track, and assess the amount of time spent handling and resolving incidents. The ICAMP studies also pointed out that in the university environment there is insufficient staffing to be able to identify the types of incidents that are occurring.

In 1998, David Dittrich used the ICAMP I incident cost model to calculate the costs associated with a large-scale incident affecting multiple hosts at the University of Washington. In a *SecurityFocus* article, Dittrich says "fair and accurate damage estimates can be produced, and with very little work, provided that those doing the work are disciplined and diligent in keeping track of time, at the time of incident response. Unfortunately, this is where the system often breaks down...The need for diligence in collecting time data for every security incident response calls for policies and procedures to be set at the institutional level, and enforced as a regular part of incident handling, in order to have meaningful figures on institutional losses due to security incidents" [Dittrich 02].

He went on to provide information about tracking and calculating these costs:

> *The fact is, it is rather simple to estimate damage due to security incidents if you know a few simple facts about the personnel who are responding to, or are affected by, the incident. Such information can be ascertained by answering the following questions:*
>
> - *Who worked on responding to or investigating the incident?*
> - *How many hours did each of them spend?*
> - *How many people were prevented from working because of the incident?*
> - *How much productive time did each of them lose?*
> - *How much do you pay each of those people to work for you?*
> - *How much overhead do you pay (insurance, sick leave, etc.) for your employees?*
>
> *Once you know these facts (and they are all pretty easy to determine), it takes simple mathematics to come up with a pretty accurate damage estimate* [Dittrich 98].

Dittrich goes on to say that a big challenge is getting people to keep track of the time they spend on handling incidents (whether that is writing detailed notes in a log book, using time

management tools, or other approaches for capturing effort). Dittrich provided an example of how the ICAMP model could be used for tracking a set of incidents.

Table 8: Example of Calculating Incident Costs

Title	Hrs	Cost/Hr ($)	Total ($)	-15% ($)	+15% ($)
Investigator	37	33.65	1,245.05	1,058.29	1,431.81
Administrator*	3	33.65	100.95	85.81	116.09
Benefits at 28% of salary[62]			348.61	296.32	400.91
Total			1694.61	1440.42	1948.81

*Expected time for system reinstallation

It should be pointed out that the examples above focus on direct costs, but in calculating the total cost of an incident there are many intangible and indirect costs that can be included in the calculation of the cost of an incident. Some of these intangible and indirect costs include loss of reputation; loss of productivity; increase in insurance premiums; and cost of new security measures, software, and configurations. Putting a dollar figure on some of these costs may be difficult, but should be achievable with input from financial and auditing staff.

3.3.4.2 Other Incident Cost Examples

The JANET-CERT team has set up a web page called "Case Studies: The Costs of Incidents." One example they list is a web defacement incident that cost an estimated 6000 pounds sterling. The case study breaks the costs down into staff costs and overall business costs. These costs given did not include any impact on the site's reputation that resulted from the incident. The defacement occurred at a university that taught computer security, but the site said they did not have any way to calculate these types of costs or to determine if this affected any student's decision to attend the school [JANET-CERT 03].

The 2003 Computer Security Institute/Federal Bureau of Investigation (CSI/FBI) Computer Crime and Security Survey indicated that 75% of the survey respondents said they suffered financial losses as a result of computer crimes; however, less than half (47%) were able to quantify the losses. Respondents who did quantify the losses reported a total of $202M, down 56% from the $455M reported in the 2002 survey. The 2003 CSI/FBI survey reported the

---

62 When calculating the costs of salary or personnel in the U.S., institutions that pay some form of benefits for their employees will add that benefit cost into their total calculation. So in this example whatever salary cost of a person was attributed to the incident, added to it was a benefit cost that was calculated by taking the amount of the salary dedicated to the time spent handling the incident and then multiplying that by .28 (28%).

highest amount of (dollar) losses were caused by theft of proprietary information and denial-of-service attacks (total annual losses were about $70.2B and $65.6B, respectively). Virus reports amounted to approximately $27.4B [Richardson 03].

Another survey, the Information Security Breaches Survey 2002 from the United Kingdom's Department of Trade and Industry (DTI), was conducted between November 2001 and mid-January 2002. This survey reported that the costs associated with resolving computer security incidents, as reported from participants in the survey, ranged from a lower limit of less than £10,000 (66% reporting) to an upper limit amounting to more than £500,000 (4% reporting). The average (mean) cost of a serious incident was reported as approximately £30,000 [Potter 02].

The 2002 Australian/Deloitte Touche Tohmatsu/NSW survey was based on 95 responses from public and private sector organizations (from a total of about 500). Their survey sought responses on the following categories of incident activity:

- theft/breach of proprietary or confidential information
- unauthorized privileged access
- financial fraud
- telecommunications fraud
- sabotage of data or networks
- denial-of-service attacks
- degradation of network performance associated with heavy scanning[63]
- wiretapping
- telecom eavesdropping
- virus/worm/Trojan horse infection
- laptop theft
- system penetration by outsider
- unauthorized access to information by insider
- insider abuse of internet access or email
- insider abuse of internal computer resources [Australia 02]

---

[63] Although not explicitly identified, the scanning referenced in this survey seems to indicate external scanning against a respondent's system(s) based on statements in the survey suggesting that even if organizations have no vulnerabilities to exploit remotely, they still "experienced financial losses due to network degradation associated with hacker scanning tools" [Australia 02].

The Australian Computer Crime & Security Survey for 2003 asked for feedback on these same categories of attacks. The 2003 survey was submitted to 350 public companies in Australia, with responses from 214. The survey results for the annual cost of computer crime for 2003 totaled more than $11.8 million,[64] double the $5.7 million reported in the previous year's survey [Australia 03]. The 2002 survey pointed out that some of the respondents' costs reflected only the cost of investigation and recovery. Other losses, such as lost business opportunities, degradation of network performance, and cost of misuse, to mention a few, were difficult to quantify.

Simone Kaplan, in a *CSO Online* article "Criteria for Determining the Cost of a Breach," provides a list that can be used to identify costs associated with a computer security incident [Kaplan 02]:

- system downtime
- people downtime
- hardware and software costs
- consulting fees
- money (salaries/benefits)
- cost of information
- cost of lost business
- incidentals
- legal costs
- cost to company reputation

The Center for Education and Research in Information Assurance and Security (CERIAS) Incident Response Database is an example of an incident tracking system designed to help capture the costs of incidents. It is a web-based system that can be downloaded for free from <https://cirdb.cerias.purdue.edu/website/> [CERIAS 03].

3.3.5 Making a Case to Management

Whatever the form of the CSIRT capability, much of the literature (see, for example, Mandia, West-Brown, and SANS) makes the point that, to be successful, the team must have senior management support (sometimes called "buy-in"), as illustrated by the quotations included below:

[64] Note that the total responding for 2002 was 75 (80%), whereas for 2003 it was 126 (58%).

"Our experience shows that, without management approval and support, creating an effective incident response capability can be extremely difficult and problematic."

-- *CERT CSIRT Development Team, 2002*

"Management and user buy-in are critical to the success [of the team]"

-- *Schultz and Shumway* [Schultz 02]

"Until you have management buy-in, you'll find it hard to get time, money, and political support for your incident handling activities."

--*SANS Computer Security Incident Handling Step-by-Step* [SANS 03]

"Any policies, procedures, or incident response teams existing without top-level support usually fail."

– *Mandia and Prosise* [Mandia 01]

"Without proper support from management...an effective CSIRC is not possible."

-- *Wack* [Wack 91]

What was true 10 years ago still applies today in the incident response area. There have been a number of situations where a response team was set up as a direct result of activity that occurred. The CERT/CC, for example, was established in November of 1988 as a direct result of the Morris Worm.[65] In 1992, a surge in the number of reported incidents that were being launched from Australia (to overseas sites) resulted in a combined effort from the Queensland University of Technology, Griffith University, and The University of Queensland to seek federal funding to establish an Australian response team. "Although the proposal was rejected by the government, the organizations had such strong convictions that this was needed that they decided to build the capability anyway and looked for ways to fund the activity from their own budgets" [Smith 94, p. 44]. In building their plan, AusCERT (then called SERT) sought guidance and assistance from existing response teams to help them understand what was needed and how to coordinate efforts with other response teams [Smith 94].

Making the case to management to gather support for building a CSIRT will involve several steps. The need to identify and collect data for both the direct and indirect cost of incidents will be helpful in this regard. Such costs will include, as mentioned before, staff time spent on recovery and on implementing any lessons learned, system downtime, loss of productivity,

---

[65] <http://www.cert.org/meet_cert/meetcertcc.html>

loss of critical service, any loss of revenue from services and operations that are unavailable, repair costs, value of compromised information, loss of reputation, or an increase in insurance premiums. Other data to gather will include the risks to the organization's information security assets.

Matched against these costs and risks will be the benefits that the CSIRT can provide, including reduction in recovery costs due to more streamlined response processes and better communication channels; the ability to gather and evaluate new threats to the organization's operation; and the ability to provide an enterprise-wide view of not only the security weaknesses but the related response efforts and their implementation. The CSIRT, in essence, becomes one of the providers of business intelligence to the organization.

The CSIRT will also show that it will be able to reduce incident activity and the damage resulting from those incidents that do occur. The CSIRT will need to put a cost on the "loss" avoided and the risk minimized by the work a CSIRT performs. It's generally accepted that a CSIRT will show a business benefit in the long term, when successfully implemented, whether in business efficiency, reduced customer complaints, or enhanced reputation of the parent organization. These types of issues and success stories are needed as part of the overall business case to management. The organization's business continuity plans and risk models, if in place, should be able to be used to support the case for a CSIRT.

In the article by Sarah Scalet entitled "Risk: A Whole New Game," she mentions the increased interest in insurance companies who are offering cyber insurance and the move towards creating actuarial models that map security practices to financial losses (versus guesses at loss figures). Scalet mentions that courts are beginning to apply dollar figures to losses from security breaches as well and that this could have an impact on companies being asked to meet a certain standard of due care [Scalet 02].

The emergence of such legal precedents and standards will be another impetus to organizations to develop incident handling capabilities. These capabilities are beginning to become requirements in various laws and regulations. For example, in the U.S., the Gramm-Leach-Bliley Act of 1999 (GLBA, also known as the Financial Services Modernization Act of 1999) requires financial institutions to not only have customer privacy policies and an information security program, but also a response capability. The European Data Protection regulations require all data controllers to have appropriate technical and procedural means to protect the data they hold. The establishment of a CSIRT or a response capability can be seen as one indicator of a company actively engaging in due care or providing the required procedural response.

One methodology for understanding the information and security needs of an organization is the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)[SM] process. OCTAVE is a risk-based strategic assessment and planning technique for security. OCTAVE is self-directed, meaning that people from an organization assume responsibility for setting the organization's security strategy. Risks to critical assets are used to prioritize areas of improvement and set the security strategy for the organization. The results of such a process can be used to help make a case to management concerning security and response requirements [Alberts 02].[66]

Most in the CSIRT community will agree that to make a case to management you must put issues in terms of management's concerns and language. Risk and damage must be translated into dollars and cents for the organization. This means showing how the CSIRT will help increase productivity, increase cost savings, comply with regulations protect the company's reputation, decrease the threats against company assets, or even enable departments to score well on an audit.

3.4 Services

Each CSIRT is different and provides services based on the mission, purpose, and constituency of the team. Some of the services offered relate directly to incident handling, a core service of a CSIRT. Other services, such as security training or audits, only relate indirectly to incident handling, while serving broader organizational security needs. Some services may be provided by other parts of the organization, such as an IT, training, or audit department, instead of the CSIRT, or may even be outsourced. The actual assignment of tasks and responsibilities depends on the structure of the CSIRT's parent or host organization.

These services and a variety of others have been defined in the *List of CSIRT Services* jointly published by the CERT/CC and the TI service and included in *Organizational Models for CSIRTs*. That report and the corresponding list groups CSIRT services into three categories:

- **Reactive services**. These services are triggered by an event or request, such as a report of a compromised host, wide-spreading malicious code, or something that was identified by an intrusion detection or network logging system. Reactive services are the core component of incident handling work.
- **Proactive services**. These services provide assistance and information to help prepare, protect, and secure constituent systems in anticipation of future attacks, problems, or events. Performance of these services will directly reduce the number of incidents in the future. These services are ongoing, rather than being triggered by a direct event or request.

[SM] OCTAVE is a service mark of Carnegie Mellon University.

[66] For information on OCTAVE publications, see <http://www.cert.org/octave/pubs.html>.

- **Security quality management services**. These services augment existing and already well-established services that are independent of incident handling and traditionally have been performed by other areas of an organization such as the IT, audit, or training department. If the CSIRT performs or assists with these services, the CSIRT's point of view and expertise can provide insight to help improve the overall security of the organization and identify risks, threats, and system weaknesses. These services are generally proactive in nature but contribute indirectly, rather than directly, to a reduction in the number of incidents.

Table 9 provides a high level overview of the various CSIRT services within each of the above categories as outlined in *Organizational Models for CSIRTs* and the corresponding CSIRT Services List. The services listed in Table 9 are defined and explained in detail in the CSIRT Services list available at <http://www.cert.org/csirts/services.html>.

Table 9: CSIRT Services by Category

Reactive Services	Proactive Services	Security Quality Management Services
+ Alerts and Warnings	O Announcements	✓ Risk Analysis
+ Incident Handling –Incident analysis –Incident response on site –Incident response support –Incident response coordination	O Technology Watch O Security Audit or Assessments O Configuration & Maintenance of Security Tools, Applications, & Infrastructures	✓ Business Continuity & Disaster Recovery Planning ✓ Security Consulting ✓ Awareness Building ✓ Education/Training
+ Vulnerability Handling –Vulnerability analysis –Vulnerability response –Vulnerability response coordination	O Development of Security Tools O Intrusion Detection Services	✓ Product Evaluation or Certification
+ Artifact Handling –Artifact analysis –Artifact response –Artifact response coordination	O Security-Related Information Dissemination	

As illustrated in Table 9, there are many different types of services that a CSIRT can provide. In reviewing the service offerings from different CSIRTs, it can be seen that there is not one set combination of functions or services that a CSIRT provides. However, to be considered a CSIRT, a team must provide some form of incident handling service.

Incident handling includes three functions: receiving incident reports, performing incident analysis, and performing incident response. These translate into four basic services: incident analysis, incident response on-site, incident response support, and incident response coordination. The various types of "incident response" services indicate the wide variety of "re-

Reproduced From Best Available Copy

sponses" different types of CSIRTs choose to provide. Some teams actually perform repair and recovery operations (incident response on-site). Others provide technical advice and recommendations through phone, email, and documentation (incident response support). And others facilitate the exchange of incident data, response and mitigation strategies (incident response coordination). Incident Analysis is not only the technical analysis of the incident report but also includes sub-services such as forensics evidence gathering and tracking and tracing intruders. These two functions are sub-services because not all CSIRTs perform these types of analysis.

In talking with and observing various teams, it can be seen that most teams perform incident handling in some form. What that incident response work is varies from team to team. Some teams spend their day reviewing intrusion detection system (IDS) logs. When they see an alert or abnormal network traffic their response is to pass that alert on to another part of the organization to handle. Other teams may spend their day watching IDS logs but when an alert goes off, they send someone to analyze and investigate and determine the response. Still other teams may do no IDS monitoring and instead staff a help desk to receive and handle security incident reports. When they receive reports they may go to the affected machine to perform diagnostic procedures and forensic analysis to determine what is wrong and capture any necessary evidence. Other teams that coordinate incident response activities may rarely analyze a system, but instead make sure information about ongoing threats and attacks are published to the constituency, so the constituency can take the appropriate steps to protect themselves.

As we reviewed the literature, we found that the descriptions and identification of the range of services a CSIRT can provide is very similar, although these are discussed at various levels depending on the focus of the publication (e.g., management perspective versus technical). It should also be noted that often different authors refer to these services with slightly different names.

To find out what types of services current teams are offering, we asked participants in the CSIRT Organizational Survey[67] to indicate which services they currently provide. The most frequently reported service was, of course, incident handling (97%). Those who said they did not perform incident handling were military coordination centers. The next most frequently offered services were

- publish advisories or alerts (72%)[68]
- perform security policy development (72%)

---

[67] As the new CSIRT Services document was not complete when the survey was created, the list of services on the survey was only a subset of the new services list.

[68] In creating the pilot survey we did not distinguish between writing advisories or forwarding advisories written by others. We included both in this service. In any future surveys we may choose to make a distinction.

- perform artifact analysis (66%)
- perform virus handling (66%)
- provide and answer a hotline (62%)
- monitor IDS (62%)
- produce technical documents (62%)
- do training or security awareness (59%)
- perform some type of technology watch or monitoring service (55%)
- perform forensic evidence collection (55%)
- track and trace intruders (52%)
- pursue legal investigations (44%)

The least offered services were

- penetration testing (17%)
- security configuration administration (24%)

The other least offered services were

- vulnerability handling (41%)
- vulnerability assessments (28%)
- vulnerability scanning (31%)
- doing security product development (34%)
- monitoring network and system logs (38%)

Profiling of the teams by organizational location and services provided the following results:[69]

- When the CSIRT is its own department, only 14% perform penetration testing or vulnerability assessments. Less than half perform forensic evidence collection, tracking and tracing intruders, and legal investigations.
- When the CSIRT is located within the IT department, 100% perform incident handling and IDS monitoring. 92% produced advisories and 83% perform artifact analysis, virus handling, and security policy development.
- When the CSIRT is located within the security team, 75% perform forensic evidence collection, pursue legal investigations, and provide a hotline service and a technical watch service. 25% perform penetration testing, vulnerability scanning, vulnerability assess-

[69] Any services not mentioned were only listed by a small number of the teams.

ments, or training. None perform security configuration administration, IDS monitoring, or system and network monitoring.

Profiling of the teams by sector and services provided the following results:

- Banking and finance: CSIRTs: 100% perform incident handling, artifact analysis, virus handling, IDS monitoring, technical document development, security policy development, forensic evidence collection, tracking and tracing of intruders, and legal investigations.
- Education: CSIRTs: 100% perform incident handling and IDS monitoring; 83% perform artifact analysis, virus handling, advisory production, security policy development, training, and forensic evidence collection.
- Information and communication: CSIRTs: 100% perform incident handling and forensics analysis; 75% perform a technology watch service, produce advisories, perform security policy development, track and trace intruders, and pursue legal investigations.
- Military CSIRTs: 88% perform incident handling, 75% produce advisories and perform virus handling, and 63% provide a hotline service. None of the military teams participating in the survey provide penetration testing and only 22% perform vulnerability scanning, assessments, or forensic evidence collection.
- Other commercial CSIRTs: 100% perform incident handling, virus handling, network and system monitoring, technology watch, security policy development, and security product development and produce advisories.
- Non-profit CSIRTs: 66% provide training, technical document development, advisory publication, and a hotline service. None perform penetration testing, vulnerability scanning, security configuration administration, or legal investigations.

Profiling of the teams by CSIRT model and services produced the following results:

- Ad hoc teams: 100% perform incident handling; 75% perform virus handling. None perform penetration testing, vulnerability scanning, vulnerability assessments, or security configuration administration. Only 25% perform a technology watch service or monitor IDS. This seems fitting with the nature of such teams not to be involved in proactive or security quality management services.
- Coordination centers: 100% perform incident handling, technology watch services, advisory production, technical document production, security policy development, and tracking and tracing intruders. This seems to fit with the focus on coordination and being proactive.
- Centralized CSIRTs: 90% perform incident handling; 80% perform advisory production and virus handling. Only 10% perform penetration testing.
- Combined teams: 100% perform incident handling and artifact analysis; 80% perform security policy development.

- Distributed dedicated CSIRTs: 100% perform incident handling, security policy development, and forensic evidence collection; 66% provide a hotline service and an advisory publication service, produce technical documents, provide training, track and trace intruders, and perform vulnerability assessments. None perform penetration testing and security configuration administration.
- Distributed part-time CSIRTs: 100% provide incident handling, IDS monitoring, and security policy development; 75% monitor systems and networks, produce advisories, and publish technical documents.

Other general trends:

- All (100%) of those who stated that they perform penetration testing also stated that they perform vulnerability scanning services.[70]
- 80% of the teams performing penetration testing identified themselves as a centralized, dedicated, or combined team.
- No military, banking and finance, or non-profit CSIRT participating in the survey performs penetration testing.[71]
- Of those teams performing legal investigations, 92% also perform forensic evidence collection and 85% also perform both tracking and tracing and artifact analysis.
- All of those teams who stated that they provide a vulnerability assessment service also perform forensic evidence collection and security policy development.
- 86% of those who provide vulnerability assessments also produce advisories.
- The largest number of those doing artifact analysis work are located in a centralized or combined team (32%).
- 94% of the teams performing tracking and tracing also perform artifact analysis.
- 90% of the teams performing security product development services also provide training, publish advisories, and perform security policy development. The majority of those who performed security product development services were centralized teams, combined teams, or centralized coordination centers. Only 25% of the ad hoc teams perform security product development services.
- Of the teams performing security configurations, all were either located in the IT department or the CSIRT was its own department. 86% of those performing this service were a combined or centralized team. 86% of those performing this service also monitored IDS. None of the ad hoc teams perform security configurations or IDS monitoring.

---

70 It should be pointed out that this was the trend we saw in the responses to the CSIRT survey. In talking with other teams who did not complete the survey, we have seen teams who performed scanning but not penetration testing.

71 This could mean that a different part of their organization performs this type of activity.

3.5 Staffing

The majority of documents we reviewed stress the importance of identifying staff (or a team) that is responsible for handling computer security incidents. This staff may be full time and devoted to incident handling tasks, or it may be ad hoc and pulled together only when an incident occurs.

3.5.1 Staff Size

A question we frequently hear is "How big should my team be?" This is not an easy question to answer, because it depends on a lot of factors. Most people involved in incident handling agree that one person is not enough, but there is no standard number concerning how many staff members are needed. This depends on the expertise of the staff, the incident workload, and the type of services offered. It also depends on what work related to incident handling and computer security is provided by other parts of the parent or host organization.

Depending on the level of service provided, the size of the team may need to have a minimum number of staff. For example, for a 24x7 service like the hotline, you can begin to estimate how many staff you might need to provide this service. If you have three shifts, you will need at least four to six people to provide a basic hotline service: three to cover the shifts and a backup for each to cover sick time and vacations. Depending on the number of calls that come in, one person for each shift may not be enough. So you may need another three staff members. However, if the hotline staff also performs other tasks, such as technical monitoring, triage, or incident analysis, then even that number of staff may not be enough.

There was one European CSIRT that was staffed with just one person who spent just 20% of his time handling incident reports—for a whole country. While by today's standards this would seem an unlikely model, at that time this "team of one" provided a valuable service to other CSIRTs in the community by acting as a facilitator to distribute incident reports to the appropriate entities.

In looking at the data gathered in the CSIRT Organizational Survey and through our literature review, no specific staffing trends or best practice staffing levels were seen. The survey data showed that

- 31% of participating CSIRTs stated that they had 1–5 full-time staff.
- 31% stated that they had 6–10 dedicated full-time CSIRT staff.
- 21% stated that they had over 10 staff.
- Only one stated that they had over 100 staff and that was a combined military team.
- Even some ad hoc and distributed part-time teams stated that they had some staff devoted to incident handling on a full-time basis.

Not surprisingly, in the majority of cases the teams with the larger staffs had a larger budget. An important question we did not ask in the survey was the size of the constituency and networks supported by each team. This may have provided more useful information to gauge the team size effectiveness. In any future surveys we will ask that question.

Across the board, most CSIRT sectors and models had both full-time and part-time staff.

- 38% of the participating CSIRTs stated that they had 1 to 5 part-time staff working on the team.
- 17% said they had 6 to 11 part-time staff working on the team.
- One team said that they had 100 part-time staff distributed across various sites.
- As would be expected, almost all distributed teams, ad hoc teams, and combined teams had part-time staff. However, a few combined teams had only full-time staff. And the majority of the ad hoc and distributed part-time teams had only part-time staff.
- 48% of those with part-time staff said that the staff involved provided the equivalent of work done by 1 to 3 full-time staff.

Smith, in his article "Forming an Incident Response Team," says that the AusCERT team recognized early that the size of a team would have an effect on the overall capabilities of the team. He discusses some approaches for seeking expertise from outside sources and the need for developing trusted contacts. Smith also pointed out that one of the "common attributes between existing CSIRTs [is] that they are under-funded, under-staffed, and overworked." He also suggested that one full-time technical person could comfortably handle one new incident per day (with a maximum of 20 incidents in some type of active state) [Smith 94]. Those, however, were statistics for the AusCERT operation almost 10 years ago. Such statistics may no longer be valid in today's CSIRT environment. The larger numbers of incidents that are being reported today and the sophistication of attacks may mean that an incident handler cannot handle that many incidents at a time. Our survey did not research the number of incidents that can be handled by CSIRT staff, so we have no statistics for comparison today. However, this type of information is being collected as part of the eCSIRT.net initiative in Europe, so in the future we may have some statistics on how long it takes CSIRT staff to handle particular types of incidents.[72]

3.5.2 Staff Positions

Although there is not a standard number of staff for a team, there are some standard, agreed-upon positions that a team might consider. These are described in this section. In addition, Section 4.5 of the *Handbook for CSIRTs* provides additional details concerning staffing issues [West-Brown 03].

---

72 For more information on eCSIRT.net, see <http://www.ecsirt.net/>.

Most of the documents we reviewed described various approaches for constructing or organizing a team, and regardless of the CSIRT model chosen, there were a few roles that all consistently identified as needed:

- team lead (or manager, coordinator, principal investigator, senior technical lead)

  The manager, team lead, or coordinator role has the overall responsibility for managing the team and overseeing the handling of incident activities. This person can allocate or request additional resources when needed, and may have budgetary control and authority to take actions within the boundaries of certain predefined conditions (e.g., may be empowered to schedule overtime, have systems disconnected from a network, purchase software or hardware, etc.).

- technical staff (incident handlers, vulnerability or artifact analysts)

  The technical staff provides the primary support for incident handling, as well as supporting other CSIRT services[73] that may be provided and for which they have the expertise. Staff can be full-time CSIRT members or may be adjunct members who are approved to work with the CSIRT as needed. These part-time staff may be from other departments or sections of the parent organization or constituency or they may be external security experts who have a working agreement with the CSIRT.

- first responders

  This can include those who handle the first report of an incident, whether they are help desk personnel, CSIRT hotline staff, or some other type of staff.

- experts

  These may be computer security experts, platform specialists, or network administrators who are brought in to provide guidance and advice during an incident, but are not full time members of a team.

- other professional or administrative support staff

  The professional support category could include staff from IT, human resources, legal, corporate security, disaster recovery, or public relations departments. It may also include media specialists, criminal investigative staff, and other management contacts that can assist the CSIRT. The other administrative category includes administrative and secretarial staff support (either full-time or part-time staff) who may be called upon to assist during heightened periods of increased incident activity, major events, or other times (holidays, new school semester terms, fiscal/calendar year roll-overs, etc.).

We have also noticed through discussion with other CSIRTs that many teams implement the concept of a core team and an extended team as their model for CSIRT operations. The core team usually consists of first responders and incident and vulnerability analysts. The ex-

---

[73] See the *CSIRT Services* list at <http://www.cert.org/csirts/services.html>.

tended team is formed by temporarily adding on other professionals or specialists depending on the type of activity and type of response and analysis required.

The list that follows provides a more detailed sample of the types of staffing and tasks related to positions that might be part of a core and extended CSIRT. A review of the CSIRT literature and discussions with other teams about their organizational structure show that these are common types of positions in CSIRTs. It should be pointed out, however, that not all teams would have all these positions. CSIRT staffing will depend not only on the main mission of a team, but also on the funding and expertise available in the parent organization. It will also depend on what services and capabilities are provided by other parts of the parent organization or constituency.

A core team might include

- manager or team lead
  - provides strategic direction
  - enables and facilitates work of team members
  - supervises team
  - represents CSIRT to management and others
  - interviews and hires new team members
- assistant managers, supervisors, or group leaders
  - provides day-to-day operational guidance for team
  - supports strategic direction of assigned functional area
  - supports the team lead as needed
  - provides direction and mentoring to team members
  - assigns tasks and duties
  - participates in interviews with new team members
  - handles management tasks in team lead's absence
- hotline, help desk, or triage staff (can also be referred to as first responders)
  - handle main CSIRT telephone(s) for incident or security reports
  - provide initial assistance, depending on skills
  - undertake initial data entry and the sorting and prioritizing of incoming information
- incident handlers
  - undertake incident analysis, tracking, recording, and response
  - coordinate the reactive and proactive guidance that will be provided to the constituency (develop material such as documentation, checklists, best practices, and guidelines)
  - disseminate information
  - interact with the CSIRT team, external experts, and others (such as sites, media, law enforcement, and legal personnel) as appropriate, by assignment from team lead or other management staff
  - undertake technology-watch activities if assigned
  - develop appropriate training materials (for CSIRT staff and/or the constituency)
  - mentor new CSIRT staff as assigned
  - monitor intrusion detection systems, if this service is part of the CSIRT activities

  - perform penetration testing, if this service is part of the CSIRT activities
- vulnerability handlers
  - analyze, test, track, and record vulnerability reports and vulnerability artifacts
  - determine exposure of constituency or parent organizational sites
  - research or develop patches and fixes as part of the vulnerability response effort
  - interact with the constituency, the CSIRT, software application developers, external experts (CERT/CC, FedCIRC, vendors) and others (media, law enforcement, or legal personnel) as required
  - disseminate information on vulnerabilities and corresponding fixes, patches, or workarounds

Professional staff that may be asked to work as part of an extended CSIRT include

- platform specialists who assist in analysis and response efforts by providing expertise in supported technologies or operating systems (e.g., UNIX, Windows, mainframes, applications, databases). They may also perform incident handling, vulnerability handling, or infrastructure tasks if needed.
- network or system administrators to administer CSIRT equipment and peripheral devices and maintain the infrastructure for CSIRT services. This could include deploying and maintaining secure servers, secure email, an incident tracking system and data repository, and any other internal systems required by the CSIRT.
- web developers to maintain any CSIRT internal or external web site. The web developers would also work in conjunction with CSIRT staff to create new content and corresponding designs for any team web site.
- trainers to develop and deliver curriculum for teaching not only new incident handlers in the CSIRT, but also perhaps to teach constituency members. They may also develop and provide security awareness training to the constituency and any parent organization.
- technical writers to assist and facilitate the CSIRT in the development of publications such as advisories, best practices, or other technical documents
- representatives from the legal department to help develop and review any non-disclosure agreements, outsourcing contracts, or service level agreements. They may also provide guidance regarding liability issues related to ongoing incidents and advise the CSIRT regarding any laws or regulations with which the organization and the team must comply.
- representatives from human resources to develop policies and procedures for removing internal employees found engaging in unauthorized or illegal computer activity. They may also help implement security training within the constituency and help develop job descriptions and interview processes for finding and hiring CSIRT staff.
- representatives from public or media relations who work with the CSIRT to handle any media inquiries and help develop information disclosure policies and practices
- existing security groups, including physical security, that will work with the CSIRT to exchange information about computer incidents and possibly share responsibility for resolving issues involving computer or data theft

- audit and risk management specialists who help the CSIRT develop threat metrics and risk assessments for constituency systems
- law enforcement liaisons or investigators involved in evidence collection, forensic analysis, and any resulting prosecution or court cases

Support staff is usually required to help CSIRT members as needed by performing administrative services.

3.5.3 Staff Skills

Finding and retaining skilled CSIRT staff is not an easy task. Many teams have relayed how they have had open positions for long periods of time before finding someone who had the right skill set and personality to work in their CSIRT.

Many of the authors of various incident handling books and articles discuss the types of skills required for CSIRT staff [Schultz 02, Smith 94, van Wyk 01, West-Brown 03]. Most agree that not only is it important for staff in the CSIRT to have the technical depth and breadth of experience to handle incidents, it is equally important (sometimes even more so) to have "people" skills as well.

It is obvious in many of the publications reviewed that CSIRT members are viewed as providing a "customer service" role. Van Wyk and Forno state that it is paramount that every team member have a positive, customer service-oriented attitude and that care be taken in hiring the right staff [van Wyk 01]. For many CSIRTs, a large portion of the interaction with others occurs through oral communication (telephone conversations, presentations) or the written word (email, documents, reports, alerts, advisories, etc.), so it is imperative that CSIRT staff be able to carry out these communications clearly and concisely, be able to describe activity accurately, and provide information to their constituency or others that is easy to understand. CSIRT staff may also be dealing with constituency members under great stress because of the current damage resulting from any incident activity, so they must be able to relate to the situation and often even calm people down to be able to obtain the needed information to handle the incident. This is another reason why personal skills are so important.

Trustworthiness is paramount to the success of a CSIRT. This is one of the key lessons learned that is discussed in CERT/CC incident handling courses. Other authors agree that CSIRT members must be trustworthy [Kossakowski 94a, Schultz 02, Smith 94, West-Brown 03]. The words and actions of each member of the team can affect the reputation and constituent perceptions of the team.

Smith says that in his opinion the attributes that any CSIRT staff member should have are (in order of priority)

- integrity
- operating system administration experience
- programming experience
- communication skills
- security experience [Smith 94]

Schultz provides a summary of the types of skills typically required in the CSIRT, including the need for strong management experience to lead the team and ensure that it is meeting its mission and the need for technical staff with proficiency in different applications, systems, and networks found in the team's constituency. He also lists other equally important traits such as people, teamwork and communications skills, all of which contribute to effective interactions between the team and its constituency [Schultz 02].

In addition to identifying the right skills for the CSIRT staff, Oppenheimer et al. suggest that some security precautions be implemented during the hiring process to screen resumes for "red flags." Employers should perform reference and background checks, require new employees to sign appropriate non-disclosure agreements or acceptable use documents, and provide security awareness training as part of new-employee orientation [Oppenheimer 97].

Smith also discusses the importance of paying careful attention to hiring regulations with regard to advertising, interviewing, and screening applicants. He raises the issues that management will need to determine if hired staff will be required to complete non-disclosure agreements and if they will need security clearances to perform their work (depending on the sensitivity of the constituency's information) [Smith 94].

Another issue that CSIRT managers must take into consideration concerns any CSIRT staff members who will provide expert testimony in any judicial proceedings. If a team's services include forensics evidence collection, then the team members may be required to act as expert witnesses in court. This may require specialized skills and training for the analyst. Also, any staff member undertaking such tasks must be willing and able to stand up in court and provide the testimony.

Having well-defined job descriptions that include a list of the roles and responsibilities for each of the CSIRT positions along with the necessary skills, experience, educational background and/or certifications and clearances required can be a helpful tool in identifying and hiring the right staff.

As the field of incident handling and CSIRT functions is still relatively new, in many cases, managers who are seeking trained staff will turn to the more traditional system administrator position descriptions and skills. For example, SAGE,[74] the international organization for professional system administrators, provides information about various job descriptions that might be useful to organizations seeking to staff a CSIRT.[75] The core job descriptions cover the range of novice to senior-level system administrator, listing the required background and desirable skills for these positions.

More information on CSIRT required skills can be found in the CSIRT Basic Skills document on the CERT/CC web site at <http://www.cert.org/csirts/csirt-staffing.html>.

3.5.4 Staff Burnout

Because of the amount of detailed work done by incident handlers and the increasing work loads, many of the authors of the books and articles reviewed in the literature identified staff burnout[76] as a problem for CSIRTs.

Most encourage managers of teams to foster an environment where professional development of staff is given a high priority. As the technology improves and evolves, the CSIRT staff must have opportunities to improve their skills and experiences. This may mean providing a particular percentage of staff time for professional development. This professional development could include working in other areas of the team or parent organization or attending conferences and training in an effort to stay current with necessary incident handling skills.

A number of the authors identify the need to provide opportunities for the CSIRT staff to "rotate" or take on other roles to avoid incident response burnout [Smith 94, van Wyk 02, Wack 91, West-Brown 03]. They recommend seeking ways to invigorate or energize staff by allowing them to spend a portion of their time (or some other dedicated timeframe) working on new projects, investigating new technologies, writing, participating in workshops or training sessions, developing software tools that may be of use to the team or constituency, or performing other research that will take them away from day-to-day incident handling activities.

The *Handbook for CSIRTs* suggests that only 80% of staff time should be devoted to incident response activity [West Brown 03]. Van Wyk and Forno suggest that "incident response pro-

---

74 SAGE is a Special Technical Group (STG) of the USENIX Association. For more information about SAGE, see <http://sageweb.sage.org/>.

75 The SAGE short topics booklet series includes one booklet focused on job descriptions, edited by T. Darmohray. A brief overview of the booklet is available at <http://sageweb.sage.org/resources/publications/8_jobs/>.

76 *Webster's Ninth New Collegiate Dictionary* defines burnout as "exhaustion of physical or emotional strength."

fessionals be utilized only 55–65 percent with the rest of the time available for training" [van Wyk 01].

Schultz also discusses the problem of burnout and management's responsibility to identify techniques and approaches to provide incident response staff with opportunities to do other types of work [Schultz 02, p. 90]. Smith suggests that staff should rotate through high-stress positions and have opportunities to work on other activities that are less stressful (although, of course, they should be available if emergency situations necessitate pulling them back into incident handling activities) [Smith 94].

3.6 Training and Certification

As more and more CSIRTs were created during the 1990s, a common issue that many teams (and individuals) faced was the general lack of training resources for incident handling. Although training was widely available for various technical skills[77] that an incident handler may need (e.g., system and network administration), few training providers taught how to secure those hosts and networks, let alone how to apply this knowledge to the arena of incident handling activities—receiving incident reports, analyzing the incident, sharing relevant information with others, and providing an effective response.

The CERT Coordination Center was one of the first organizations to provide training courses specifically designed for CSIRT managers and technical staff. Originally developed for the U.S. Army, these courses are now offered to the public, and have been attended by hundreds of CSIRT members from around the world.[78]

Today, there are a number of sources that provide some level of training in incident response and incident handling activities, as well as more training sources in special focus areas such as computer forensics. Many organizations offer "hands-on" courses, as well as online or webcast courses or seminars that can be attended without having to incur travel expenses.

Training in the general fields of information security and information assurance is quite abundant. Many colleges and universities are now offering courses and curriculums in information security or assurance, at both the graduate and undergraduate levels. In the United States, since 1999 the National Security Agency has designated 50 universities as Centers of Academic Excellence in Information Assurance Education, part of an outreach program to

---

77 See the CERT/CC document at <http://www.cert.org/csirts/csirt-staffing.html>, which lists the basic skills, both technical and non-technical (e.g., personal and communication skills), that the CERT/CC has found essential for providing effective incident response.

78 <http://www.cert.org/training/>

promote "higher education in information assurance" and produce "a growing number of professionals with IA expertise in various disciplines."[79]

A relatively new development in incident handling training is the certification of CSIRT incident handling staff or teams. In 2000, the SANS Institute[80] began offering individual certifications for Global Information Assurance Certification (GIAC)[81] Certified Incident Handler (GCIH).[82] And in 2003, the CERT Coordination Center began offering the CERT-Certified Computer Security Incident Handler certification.[83]

The U.S. Department of Defense has mandated that all Computer Network Defense Service Providers (CNDSP) be certified and accredited in order to continue providing security services to their subscribers. The CNDSP certification and accreditation process is means by which providers can become certified according to the guidelines identified in DoD Directive 8530.1 "Computer Network Defense" and DoD Instruction 8530.2 "Support to Computer Network Defense."[84] The Certification and Accreditation process is an evaluation of the protect, detect, respond, and sustain capabilities of the CND service provider, as well as an evaluation of the ability of the provider to deliver these services to its subscribers.

Previous to these more specialized incident handling certifications, more generalized certifications in the field of information security have been available to individuals. The most recognized is the Certified Information Systems Security Professional (CISSP),[85] offered through "(ISC)^2" the International Information Systems Security Certifications Consortium, Inc.[86] The CISSP Certification examination covers a working knowledge of ten domains of information security that comprise the Common Body of Knowledge (CMK).[87] Some of the other types of information security certifications that are recognized are listed in Appendix C.

In reviewing the results of the CSIRT Organizational Survey, there was no standard type of certification or degree required for incident handling staff by the teams participating in the

---

79 <http://www.nsa.gov/isso/programs/coeiae/index.htm>

80 <http://www.sans.org/>

81 <http://www.giac.org/>

82 <http://www.giac.org/GCIH.php>

83 <http://www.cert.org/certification/>

84 Policy documents are available to .mil sites via links on <http://iase.disa.mil/policy.html> or <http://www.cert.mil/>; access requires a DoD PKI Certificate.

85 <http://www.isc2.org/cgi/content.cgi?category=19>

86 <http://www.isc2.org/>

87 <https://www.isc2.org/cgi-bin/content.cgi?category=8>. The ten domains of the CBK are Security Management Practices; Security Architecture and Models; Access Control Systems & Methodology; Application Development Security; Operations Security; Physical Security; Cryptography; Telecommunications, Network, & Internet Security; Business Continuity Planning; and Law, Investigations, & Ethics.

survey. Ten percent required a bachelor's degree, 6% required the CISSP certification, 6% required Microsoft Certified Systems Administrator (MCSA)[88] certifications, and 3% required GIAC GCIH certification.

Along with external training, many teams have their own internal training to teach CSIRT staff the specifics of their particular services. Fifty-five percent of the participating CSIRTs stated that they had a formal training program for the CSIRT staff.

Appendix C lists some current sources for CSIRT training. In addition to the URLs listed in this appendix, a search on the World Wide Web can provide an ever-growing menu of other sites and organizations that now offer some level of incident handling training. In assessing any training providers, it is important to try to determine whether the type of training being offered meets the needs of the team and individual members of the team.

3.7 Processes

In this section we look at how CSIRTs go about receiving, categorizing, tracking, and responding to computer security incidents. Information was gathered through the CSIRT Organizational Survey, literature search, our own experiences, and discussions with other teams.

We will begin with a look at the definition of computer security incidents and other incident response terminology. Next we will look at what is involved in creating an incident response plan. We will move on from there to discuss various CSIRT operational processes such as

- receiving incident data
- recording and tracking CSIRT data
- categorizing and prioritizing incident reports
- performing incident response
- answering the hotline
- performing forensic analysis
- coordinating and sharing information

We will also discuss defining the hours of operation.

---

[88] <http://www.microsoft.com/traincert/mcp/mcsa/>

3.7.1 Defining Computer Security Incidents and Other Incident Response Terminology

One of the problems facing the CSIRT community today is the lack of a standard taxonomy or a standard set of definitions for describing incident response activities and events. This has caused much confusion when trying to exchange data between teams or with sites. In particular, the actual definition of the term "incident" varies from team to team. For example, definitions for "incident" in the literature reviewed included the following:

- The CSIRT FAQ defines an incident as "any real or suspected adverse event in relation to the security of computer systems or computer networks." Another definition is "the act of violating an explicit or implied security policy" [CSIRT 02].
- Allen, in *The CERT Guide to System and Network Security Practices*, describes an incident as "a collection of data representing one or more related attacks. In addition, a set of steps are described that are comprised of a series of practices used to respond to incidents, e.g., analyze, communicate, collect, and protect. These are followed with practices to contain, eliminate, return systems to operations, and improve the process" [Allen 99].
- A draft version of The State of Vermont's incident reporting procedures for their CSIRT defines an incident as "any irregular or adverse event, which can be electronic, physical, or social that occurs on any part of the State's infrastructure" [Vermont 01].
- In a joint survey from AusCERT, Deloitte Touche Tohmatsu, and the New South Wales Police in May 2002, a computer security incident is defined as "an attack against a computer or network, either real or perceived" and "any type of computer network attack, computer-related crime, and the misuse or abuse of network resources or access" [AusCERT 02].
- The SANS *Incident Handling Step-by-Step* guide defines an incident as "an adverse event in an information system and/or network, or the threat of the occurrence of such an event" [SANS 03].
- The Department of the Navy incident response guidebook uses the same definition as SANS [Navy 96].
- Van Wyk and Forno describe an incident (in its most basic terms) as "a situation in which an entity's information is at risk," without explicitly saying whether it is an event or an attack [van Wyk 01].
- Mandia defines incidents as "events that interrupt normal operating procedure and precipitate some level of crisis" [Mandia 01].
- Howard describes an incident as "a group of attacks that can be distinguished from other incidents because of the distinctiveness of the attackers and the degree of similarity of sites, techniques, and timing." He also defines computer security as "preventing attackers from achieving objectives through unauthorized access or unauthorized use of computers and networks" [Howard 97].

- Schultz defines incidents as "adverse events that threaten security in computing systems and networks." In addition, events are described as "any observable thing that happens in a computer and/or network" [Schultz 01].
- As far back as 1991, Wack described "computer security incident" in a NIST document on establishing a response team as "any adverse event whereby some aspect of computer security could be threatened" [Wack 91].
- In RFC 2828, "Internet Glossary," Shirey defines a security incident as a security-relevant system event in which the system's security policy is disobeyed or otherwise breached [Shirey 00].

These varieties of definitions also mean that comparing incident statistics across teams is difficult and often meaningless.

Although there are many definitions of the term "incidents," some similarities exist. In most of the literature reviewed, the definition of "incident" related to some type of unauthorized activity against a computer or network that results in a violation of a security policy. Whether it is an action, an event, a situation, or collection of data relating to an attack, all generally agree that the CSIRT should identify the threat and then take the appropriate action, based on guidance defined in the team's policies and procedures. This is generally referred to as incident response.

Definitions for incident response include the following:

- Van Wyk describes the goal of incident response as being "to minimize the impact of an incident to a company and allow it to get back to work as quickly as possible." Incident response, according to van Wyk, is the discipline of handling situations in a manner that is cost effective, business-like, efficient, repeatable, and predictable. It involves prevention, planning, detection, analysis, containment, investigation, eradication, and a post-mortem [van Wyk 01].
- Mandia also describes incident response as a framework for a formalized process to respond to incidents. The methodology includes pre-incident preparation, detection, initial response, response strategy formulation, forensic backups, investigation, implementation of security measures, monitoring, recovery, reporting, and follow-up [Mandia 01].

Additionally, these actions, events, or situations are generally handled by some group of individuals who follow established incident response processes, whether they be staff from an IT department, an ad hoc team of security staff called upon as needed, or a more formalized and dedicated CSIRT staff. All authors reviewed in the literature search agree that to effect the response, a plan is needed.

3.7.1.1 Security Incident Taxonomy

Developing a taxonomy is a complicated endeavor, so much so that the new Incident Handling Working Group (INCH WG of IETF)[89] choose not to address that issue in their work on developing a format and methodology for exchanging incident data. Instead they have created a format that identifies various fields such as incident, vulnerability, or artifact. Each team using this format can place in those fields information according to their own definition of each term.

In 1997 a doctoral dissertation was done by John Howard called "An Analysis of Security Incidents on the Internet 1989–1995" [Howard 97]. One of the outcomes of this dissertation was the development of a taxonomy for the classification of Internet attacks and incidents. This document is still referenced in today's CSIRT community.

The eCSIRT project also is using a taxonomy that was based on one developed by staff in TeliaCERTCC.

3.7.2 Having a Plan

In February 2002 *CIO* published a report on "Cyberthreat Response and Reporting Guidelines" [CIO 02] that was jointly sanctioned by the FBI and the U.S. Secret Service. This report suggests that the better prepared an organization is to respond to security events, the better chance it has to minimize the damage.

This is one of the main functions of a CSIRT, to be prepared to effectively handle incidents when they occur and to help prevent incidents from happening. Whether the team is formalized or ad hoc, many of the authors reviewed in our literature search [Allen 01, Duffy 01, SANS 03, Schultz 02, Symantec 01, van Wyk 01, West-Brown 03] agree that the team should have a plan for handling incidents and should back up the plan with documented policies and procedures. This is a concept also widely embraced by the CSIRT community.

This incident response plan identifies the mission and goals of the team; the team roles and responsibilities; the services provided; and policies, procedures, processes, and guidelines related to incident handling. The incident response plan is not only for the CSIRT staff members (in their role as incident handlers), but also for the constituency that they serve, so those individuals are knowledgeable about what to report, how to report it, and to whom it should be reported. The plan should also provide some notion of the expected level of service that will be provided. RFC 2350, "Expectations for Computer Security Incident Response" [Brownlee 98], is a best practice document created by the IETF GRIP working group that

---

[89] <http://www.ietf.org/html.charters/inch-charter.html>

documents the type of information a CSIRT should make public to its constituents and external contacts.

Anyone who is familiar with handling computer security events knows that incidents come in all shapes and sizes. Some are quite straightforward, easy to understand and mitigate. Others can be quite serious and very complex, or can affect many hundreds of systems and require coordination to respond to effectively.

A white paper published by Internet Security Systems, "Security Architecture and Incident Management for E-Business," written by M. S. Sokol, with contributions from D. A. Curry, describes a set of best practices to reduce the risk of attacks and discusses a process for incident management. They reference the British Standard (BS) 7799[90] which was the forerunner of ISO 17799[91] (also referred to as BS EN ISO17799) a well-known set of best practice standards for implementing information security in organizations. Sokol and Curry write "Incident management responsibilities and procedures should be established to ensure a quick, effective, and orderly response to security incidents" [Sokol 00].

Having a plan in place will enable sites or organizations to not only quickly identify unauthorized activity occurring on their systems or networks, but will also facilitate responding to such events. This can eliminate or mitigate any potential risks that might be faced (loss of reputation, trust, or financial status, or even loss of life).

Even if you cannot define a robust plan, having some basic guidelines will help. The State of Vermont has a set of incident handling procedures that are used as a guideline until their CSIRT can enhance and update their existing document. This 10-page document includes sections on setting the scope (e.g., having a plan to approach handling incidents), areas of responsibility, and general and specific procedures. Their guidelines also include an incident response checklist that can be used [Vermont 01]. Another set of guidelines used by Nebraska similarly has procedures for reporting security breaches. It outlines their procedure for what type of activity to report and how that information should be reported. A copy of these guidelines can be seen in Appendix E [Nebraska 02].

Most of the authors in our literature search agreed on common areas that an organization should consider implementing when planning a response capability, including

- establishing a centralized method or point of contact (POC) for reporting incidents
- identifying the goals, functions, and responsibilities of the team

---

90 For more information on BS7700, see <http://www.thewindow.to/bs7799/>.

91 For more information on ISO 17799, see <http://www.iso-17799.com/>.

- identifying the staff and necessary expertise and training required
- identifying and defining the proactive and reactive services to be provided by the team
- providing guidance for reporting and handling incident reports
- providing security awareness and incident response training for CSIRT staff and constituency
- establishing and encouraging well-defined incident handling and security policies and procedures for the CSIRT and for the constituency
- sharing lessons learned with others
- establishing a method for evaluating how effective the CSIRT has been
- establishing a method for coordination between the CSIRT and internal and external parties

All of these issues and areas define the basic framework of the CSIRT.

In addition, many of these authors provide a set of processes or steps that are used in incident response activities. Selections of these processes from several authors are highlighted in Appendix B. Each process is outlined from each of the books or articles reviewed.

In reviewing the materials in the appendix, it can be seen that the basic steps for incident management and response are very similar across the authors. They basically break down into some form of

- prepare/protect
- detect
- contain
- analyze
- respond
- improve

The "prepare" or "protect" functions refer to proactive mechanisms to have in place to effectively respond to an incident. This includes having incident reporting guidelines available to the constituency and defined incident handling procedures for CSIRT staff. It also involves the implementation of security best practices to protect systems. These best practices can include applying appropriate security configurations for software and hardware; keeping up to date with patches and operating system upgrades; monitoring system and network activity; disabling unneeded services; enabling maximum auditing; installing internal and external defenses such as firewalls, routers, and intrusion detection systems; and raising user awareness regarding computer security issues.

In the CSIRT community, we often say "Reuse, with appropriate attribution, is good." Being able to learn from the actions and experiences of other response teams can be very effective in helping a team to develop their own plans. For example, in building a team for the German Research Network back in 1993, Kossakowski pointed out that they were able to gain a lot of knowledge about what they needed to launch their CSIRT from talking to other teams [Kossakowski 94b]. He also pointed out that it can be challenging to prepare a successful plan for a CSIRT, especially if starting from scratch. One of the lessons learned was that talking with other teams, reviewing information that is available on CSIRTs in general, and where possible and appropriate, visiting other CSIRTs, will go a long way towards helping you to build an effective plan for your own CSIRT [Kossakowski 94a].

3.7.3 Incident Handling Process or Methodology

As mentioned in the previous section, many authors provide a set of processes, steps, or methodologies that are recommended for handling incident activity, threats, and intruder attacks.

Some teams have very formalized processes with flowcharts and checklists that team members must follow to handle an incident. Other teams handle this process in a more ad hoc fashion. For example, the representation for the incident life cycle referenced in Section 3.4.1 of the *Handbook for CSIRTs* shows a visual representation for how a report moves through the incident handling cycle [West-Brown 03].

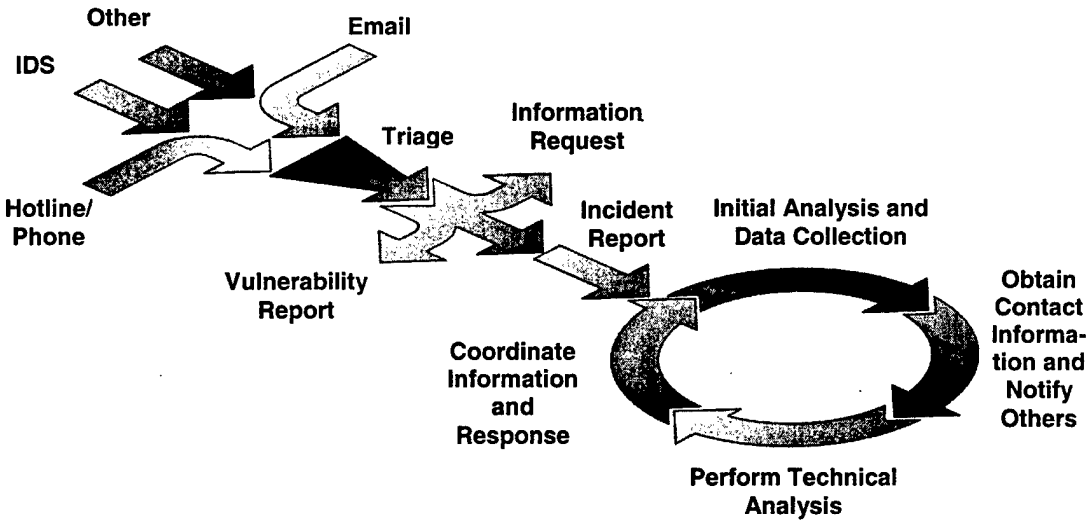


Figure 13: The Incident Life Cycle

Reproduced From
Best Available Copy

Other flow diagrams and charts have also been referenced in the literature [Kruse 02, Steele 02]. These are included in Appendix E of this document and referenced in Section 3.12.2, "Sample Templates, Checklists, Process Guides and Flowcharts."

An incident handler may not initially be able to determine whether an incident has actually occurred, and there is some amount of "discovery" that must happen to confirm or verify whether the report is valid or not. Once confirmation is obtained, the response provided will depend on the range and level of services the CSIRT provides to the constituency. The response might range from an acknowledgement of the report and pointers to resources to help the reporter of the incident, to on-site support by the CSIRT to undertake remedial actions to resolve the incident.

Once an incident has been handled (depending on the type or severity), teams might conduct a postmortem to discuss what occurred, how the CSIRT processes were or were not followed, identify any missing steps or other issues in the process that need to be revised or refined; and subsequently, update the CSIRT procedures and processes as necessary. The incident review can also provide an opportunity for the CSIRT to discuss with their constituency what security weaknesses or procedural problems led to the incident occurring and how to fix these problems to prevent future occurrences. A more detailed look at this process is discussed in Sections 3.7.4 through 3.7.7.

3.7.4 Receiving Incident Data

Most CSIRTs today have some identified mechanism for receiving reports, alerts, or requests. These usually include an email alias for the CSIRT where reports can be emailed. Others have a hotline or help desk that can be called, while others have an online or paper-based form that can be filled out to report an incident.

Other teams receive alerts and reports automatically through IDS, network monitoring programs, or other network sensors.

The CSIRT Organizational Survey asked participants what mechanism they used to receive incident reports. The results showed that the majority received reports and requests via electronic mail. The breakdown was

- 93% of the participants receive reports via email
- 79% receive reports via phone
- 69% receive reports via IDS

- surprisingly, 41% receive walk-in reports[92]
- only 17% receive reports via paper incident reporting forms
- 38% have an incident reporting form (IRF) on their web site

The following trends by sector: were identified:

- Banking and finance CSIRTs: 100% receive reports via phone, email, paper IRF, and walk-ins.
- Education CSIRTs: 100% receive reports via email and IDS; 83% receive reports via phone. 0% of the education CSIRTs stated that they used a paper or web IRF.
- Communication and Information CSIRTs: 100% receive reports via phone and email; 75% receive them via web IRF, IDS, and walk-ins.
- Other Commercial CSIRTs: Similar to the banking and finance CSIRTs, 100% receive reports via phone, email and IDS.
- Non-Profit CSIRTs: 100% receive reports via email; 66% receive them also by phone.

The following trends by CSIRT model were identified:

- Ad hoc teams: 75% receive reports via email and none have a paper or web IRF.
- Coordination centers: 100% receive reports via email and phone and none had a web IRF.
- Centralized CSIRTs: 90% receive reports via email; 80% also received them via phone.
- Combined teams: 100% receive reports via email and IDS; 75% receive them via phone and a web IRF.
- Distributed teams: 100% receive reports via phone and email; 86% receive them via IDS. Breaking that down by the type of distributed team, 100% of the distributed dedicated teams receive reports via phone and email and 100% of the distributed part-time teams receive reports via phone, email, and IDS.

3.7.5 Recording and Tracking CSIRT Data

Tracking and recording of information in a logical and methodical way can be a challenge for newly forming teams because they may not know what they need to collect and the way in which that information might need to be accessed, used, and archived.

In 1991, Garfinkel and Spafford provided two succinct rules to follow when responding to incidents. These still hold true more than a decade later:

---

[92] A "walk-in" report is when a person physically comes to the CSIRT and reports a problem verbally.

- Rule #1: Don't Panic!
- Rule #2: Document! [Garfinkel 91]

There are myriad reasons to track and record information:

- maintaining an archive of the types of incidents a CSIRT handles over the course of a year
- identifying and compiling trends and statistics
- keeping detailed information that will be admissible in a court of law (should criminal investigation of an incident be pursued)
- managing incident workload across staff
- providing reports on the status of an incident or incident report
- identifying work tasks that must be completed for an incident
- handing over an incident to another staff member for completion
- identifying large-scale incidents that might not be apparent when reviewing individual incident reports
- correlating incident activity across the enterprise

Depending on the mission and goals of a team, these reasons will vary; however, there are some common bits of data that will be useful to collect no matter what the end goal.

Each CSIRT needs to decide what data should be recorded and tracked. This will help to ensure that the team is providing effective response services, is meeting any management and funding requirements, and may also help to determine needed staffing levels.

Many teams recommend starting a log immediately to begin capturing critical information about a reported activity. Keeping accurate information about the date and time, what has occurred, who has been contacted, and what actions have been taken or need to be taken all need to be included in such a chronological log [Mandia 01, p. 31]. This is most important during times when incident activity is increasing and team members are handling multiple events or incidents. In the early 1990s, for example, it was not uncommon for the CERT/CC incident handling staff to be managing anywhere from 20-25 "active" open incidents concurrently. This collection of assigned incidents could include activity such as

- newly received reports
- on-going interactions with previously reported incidents
- contacting/interacting with other identified sites related to previously reported incidents
- closed incidents that had been reopened because additional activity reports were received
- other types of requests for information

Attempting to manage (or remember) the specific details for any one of these incidents could be a challenge; when incidents involve hundreds (or thousands) of hosts or sites, remembering what happened, who was contacted, and the current status can be very difficult. Whatever techniques are used for recording and tracking CSIRT data, it is worthwhile to identify in the requirements design that all data can be easily searched, incident reports can be handed off to other staff members (e.g., reassign the responsibility for handling a specific report), and that current summaries of the workload and distribution across CSIRT staff can be determined.

Another consideration in determining what type of system to use for tracking and recording CSIRT data is whether it can effectively incorporate processes for capturing and storing data from other sources, such as telephone calls, facsimile, other types of correspondence, encrypted information, binary files, and other types of files.

Some of the features that a CSIRT might require in recording and tracking data are included in Table 10.

Table 10: Features of a CSIRT Tracking System

Ability to:	**Support for:**	**Fields to capture:**
• modify initial categorization of reports • access and read all related emails • respond to requests via email • assign actions and redistribute to others as needed • search, sort, cross-reference, and correlate hosts, IP addresses, attack types, dates, and names • generate reports and/or statistics as required • review and/or reassign workload of an incident handler • open/close/reopen reports • access library of standard responses • trigger automatic reminders of incidents that need attention	• standardized incident data representation (IODEF for example) • encrypting and decrypting data • documenting chain of custody as part of investigation or law enforcement activity	• contact information • time zone for any times reported or logs sent • system information • resolution and mitigation strategies • recommended steps taken • staff interviewed during incident resolution • follow-up actions • cost of incident • amount of time to resolve (More fields are discussed in section 3.7.5.1)

3.7.5.1 Data Fields

Many CSIRTs have developed an incident reporting form to capture the type of information that helps them to identify the "who, what, when, where, and how" of some activity that is being reported.

A variety of incident reporting forms (or templates) have been developed by different organizations and a few examples are referenced in Table 11. Examples of these forms have been included in Appendix E. Some CSIRTs may make their incident reporting forms available for public download and use by anyone wishing to report an incident to them. Other internal teams[93] may place their forms on intranets or include them as part of procedures or guidelines for reporting.

Table 11: Sample Incident Reporting Forms and Flowcharts

Name/Organization	Source
CIO Magazine	http://www.cio.com/research/security/incident_response.pdf
NITC	http://www.nitc.state.ne.us/standards/
SANS	http://www.sans.org/incidentforms/
U.S. Secret Service	http://www.treas.gov/usss/forms/form_ssf4017.pdf
van Wyk & Forno	*Incident Response*, O'Reilly & Associates, Inc. ISBN 0-596-00130-4
Kruse & Heiser	*Computer Forensics-Incident Response Essentials*, ISBN 0-201-70719-5
CERT/CC	http://www.cert.org/reporting/incident_form.txt

Looking at these incident reporting forms, and others that are available or accessible from the Internet, we can see a standard set of data fields used to collect critical incident information:

- contact information of the individual(s) reporting and/or contact information for other sites involved in the activity
  - name
  - email address
  - address
  - phone (direct dial, mobile/cellular, fax)
- organization reporting incident
- organization that is the victim of the incident
- time of incident and corresponding time zone

[93] By "internal teams" we mean CSIRTs who only serve their internal organization or a specific group or department in their organization and who have no external appearance outside their organization.

- time of report and corresponding time zone
- time of discovery of incident and corresponding time zone
- description of problem or report (summary, technical details)
- type of system(s) involved or affected (owner, mission)
- IP address(es) of involved hosts (source and destination of attacks or scans)
- operating system (versions, patch level, applications installed) of hosts involved
- actions taken (planned), mitigation strategies, resolution
- involvement of law enforcement

In addition to the list above there are often check boxes for identifying

- the specific type of activity (probe, scan, break-in, virus, denial of service, etc.) that is being reported
- whether the activity is currently ongoing or has stopped (i.e., was discovered after the fact)
- questions to gauge the scope of the incident, extent of the damage, severity of the threat, and cost of the incident
- the time zone and/or geographic location of system(s) involved (especially helpful when tracking or handling widespread incidents that span multiple time zones and affect many systems)
- any other sites or organizations that may have been notified

Each CSIRT will need to determine the information that is most appropriate to collect and record, depending on their mission and goals, the needs of the constituency they are supporting, and/or any regulatory requirements that may be imposed—and having tools to support the management of this information is a critical need for an effective CSIRT. Most teams need to customize existing products to meet their functionality requirements.

Teams also need to identify how long they retain information about their incident reports. Some teams will keep information for short periods of time (months), while others may keep information for several years.[94] Different types of teams for different sectors may have various legal requirements that impact how long they can retain information.

Although currently there are no widely accepted standards used by the CSIRT community to record and track CSIRT data, there is ongoing work in the IETF to develop standard data

---

[94] The CERT/CC has kept an archive of all incident reports handled since the team was established in 1988.

formats for exchanging incident data between teams. For example, the IODEF defines a common data format for describing and exchanging incident information [Arvidsson 01]. IODEF has been designed to be compatible with the Intrusion Detection Message Exchange Format (IDMEF) developed for sharing intrusion detection data between intrusion detection systems [Curry 03]. More about this project can be found in Section 3.10.2.1 of this report.

3.7.5.2 Mechanisms for Recording and Tracking Incident Information

Information can be captured and logged in a variety of ways: on paper or in a logbook, in a database or help desk system, or even in text files.

When participants were queried in the CSIRT Organizational Survey about how information was collected, they responded as follows:

- 76% of the teams stated that they used a database to record and track incident data
- 28% use both a database and a paper log
- 10% use only a paper log
- 45% said they used a customized database
- 28% said that they used an off-the-shelf product

There was no particular database product used consistently by the CSIRTs. Products mentioned included

- Remedy HelpDesk and Action Request System
- SQL
- Oracle
- Microsoft Access
- Lotus Notes

A number of teams find they must build customized environments to collect, record, and store CSIRT information because some of the tools do not have the features needed or do not meet the functionality required by the CSIRT.

One example of some of the work that is currently being done to create a customized incident handling tracking system is the development of Request Tracker for Incident Response (RTIR).[95] JANET-CERT is currently funding a project that has led to the development of RTIR, which is a customized version of an earlier general-purpose tracking system called

[95] For more information, see <http://www.bestpractical.com/rtir/>.

Request Tracker.[96] JANET-CERT worked in collaboration with the software vendor, who did the actual programming.

DFN-CERT is also working on a project that has been funded by the German federal CSIRT, CERT-BUND, that involves researching requirements for a CSIRT incident tracking system. The prototype developed by DFN-CERT is based on RT and its extension for incident response, RTIR. The prototype is web-based and is called "Vorfallsbearbeitungssystem," or VBS for short. The VBS extends RT/RTIR by adding specific workflows via roles and data fields specific to incident handling.[97]

Staff from both projects are collaborating and continue to work with the software vendor to extend the requirements for an incident response specific tracking system. They are also looking for other teams who are interested in developing other extensions to this software.[98]

Some other examples of incident tracking systems that are being developed and used for incident tracking within the CSIRT community include

- the CERIAS Incident Response Database, which has specific fields for capturing incident costs[99]
- the University of Chicago Network Security Center (NSC) Freeman Incident Tracking System (FITS)[100]

3.7.6 Categorizing and Prioritizing Incident Reports

There is no clear consensus on the best way to categorize and prioritize incident reports and activity. A variety of ways to identify and prioritize reports have been used by different organizations and discussed by various authors. A few of these are summarized in Table 12.

Table 12: Methods of Categorizing and Prioritizing Incident Reports and Activity

Level/Priority	Type of Incident/Activity
[Kruse 02]	
Highest	e-commerce, authentication/billing server, law enforcement subpoenas
High	DNS/email/web server, router
Medium	External attacks, successful internal attacks

96 Also from Best Practical Software, see <http://www.bestpractical.com/>.
97 This information was provided by DFN-CERT.
98 For more information about these projects, contact JANET-CERT or DFN-CERT.
99 For more information see <https://cirdb.cerias.purdue.edu/website/>.
100 For more information, see <http://security.uchicago.edu/tools/fits/>.

Level/Priority	Type of Incident/Activity
Low	Network switch, news, chat, or shell server
[Schultz 01]	
Level 1	Low impact (affects one location; e.g., virus incident)
Level 2	Local event with major impact on operations (compromise of a privileged account, theft of critical equipment)
Level 3	Minor impact event affecting two or more locations (e.g., non-destructive virus; email spamming)
Level 4	High-impact event affecting many sites (intrusion on critical global application)
[ISS 01]	
Severity 1	Low-level probes/scans on internal systems; known virus (easily handled by AV software)
Severity 2	Probes/scans on external systems; potential threats identified
Severity 3	Significant probes/scans; penetration of denial of service (DoS) attacks attempted without impact on operations; widespread known virus attacks (easily handled by AV software); isolated instances of new viruses
Severity 4	Penetration or DoS attacks with limited impact on operations; widespread new computer virus attacks (not handled by AV software); risk of negative financial/public relations impact
Severity 5	Successful penetration or DoS attacks with significant impact on operations; signification risk of negative financial/public relations impact
[Schultz 90]	
Priority 1	Human life, human safety
Priority 2	Protect classified/sensitive data
Priority 3	Protect other data (proprietary, scientific, managerial, etc.)
Priority 4	Prevent damage to systems (loss/alteration of files, damage to disk drives)
Priority 5	Minimize disruption of computing resources
[Schiffman 01]	Rather than priorities, this methodology rates in terms of attack complexity and technical ability of attacker(s)
Low	"script kiddie" attacks, well understood, no innovation
Moderate	Attack uses publicly known/available attack method, additional modification (e.g., forgery, different attack behaviors)
Hard	Clever and reasonably skilled attacker; exploit may/may not be publicly known; attacker writes own code
Devilish	Attacks indicate domain expertise; extremely skilled, innovative, able to

Level/Priority	Type of Incident/Activity
	cover tracks, can leave covert re-entry channels; difficult to catch by average system and network administrator
[McGlashan 01]	
Priority 1	Preservation of non-critical systems
Priority 2	Continuity of complete service
Priority 3	Preservation of critical systems, proprietary* strategic information
Priority 4	Classified or (legally) sensitive data
Priority 5	Life and health

For an interesting comparison, here are the hurricane severity levels developed by the National Hurricane Preparedness Center:[101]

Table 13: Severity Levels of the National Hurricane Preparedness Center

Level	Description
CAT 1	Winds of 74 to 95 miles per hour
CAT 2	Winds of 96 to 110 miles per hour
CAT 3	Winds of 111 to 130 miles per hour
CAT 4	Winds of 131 to 155 miles per hour
CAT 5	Winds greater than 155 miles per hour

Some other levels include

- AusCERT – Priority 1-5 (lowest is non-critical systems; highest equals life and death) [AusCERT 01]
- The ISS paper on "Computer Security Incident Response Planning," discusses levels of severity from 1-5 (severity 1 being a low-impact incident and 5 being "significant)" [ISS 01]

Most authors believe that something as simple as establishing or assigning rankings such as Category 1, 2, or 3 or High, Medium, or Low will assist in prioritizing incident reports. Over time these may need to be expanded to meet the requirements or needs of the CSIRT and constituency being served. At one of our CSIRT development courses, one attendee discussed their categories for intruder activity and response. They used colors as indicators for the level of "threat" associated with an incident or other activity being handled by the team: red (high priority), yellow (cautionary alert, has potential to escalate), green (everything normal).[102]

---

[101] <http://www.disastersrus.org/emtools/acronyms.htm#sectC>

[102] CERT CSIRT Development Team personal communication, 2002.

These alert banners would be strategically located in the CSIRT offices as visual reminders of current activity levels. The yellow alert was also used to let part-time members of the CSIRT know that they may get called in if the priority went higher.

Because there are not consistent severity scales across CSIRTs, one of the more unfortunate problems that can occur is that scales can be contradictory. In some cases the priority scales used have just the exact *opposite* level of severity compared to some of the others. While a selected priority setting works very well within an organizational constituency, it could lead to confusion in those cases where incidents affect multiple sites beyond a single constituency base. If a clear understanding of the relative priorities or criticality is not understood by all, the response actions taken may seriously (and detrimentally) affect the ultimate resolution of the activity.

In looking at the lifetime of an incident, it must be recognized that the priority of the incident may change as new information comes to light. The priority of a specific type of incident might also change over time as changes in mission and services occur.

3.7.7 Incident Response Processes

CSIRT response strategies vary as much as CSIRTs themselves do. The response that a CSIRT provides is based on its mission, services, and service levels. Response options can include

- providing guidance and solutions via phone or email
- going to the site or affected machine and helping repair and recover the systems
- analysis of logs, files, or other artifacts
- assistance in legal investigations and prosecution
- capturing and documenting evidence from affected computers
- development and dissemination of patches, fixes, workarounds, advisories, alerts, or technical documentation
- notification to sites involved in the activity (both victim and source sites)
- none (forward to others to handle)

Once an incident report has been received and reviewed, the response provided will depend on the CSIRT's mission, purpose, expertise, and policies and procedures. For example, a state law enforcement CSIRT's mission may be to pursue legal investigations; when they receive a report, they begin an investigation to collect evidence for prosecution, and they are not responsible for helping to repair the affected systems. However, an internal CSIRT in a commercial company or an MSSP incident response provider, after analyzing an incident report,

may go to the site of the affected systems and physically perform the recovery operations to collect forensic evidence and also repair the affected systems.

In the CSIRT Organizational Survey, we were interested in seeing the level of involvement that CSIRTs had in the recovery and repair operations. We asked not only how CSIRTs affected their response but also who in the organization actually performed the repair and recovery operations.

The majority of the CSIRTs reported that the type of response they provide is either advice via phone and email (74%) or the development and distribution of technical documents and alerts (59%). Only 41% say they actually perform the recovery and repair of affected systems. And only 21% pass reports on to others to handle.

Trends by sector include

- All of the banking and finance, information and communication, other commercial, and 83% of the education CSIRTs stated that they provide guidance via phone and email as their primary method of response.
- None of the CSIRTs in the banking and finance, education, or information and communication sectors stated that they passed on incident reports.
- 75% of the non-profit CSIRTs said that they provide response via phone and email guidance or by passing on the incident. No non-profit stated that they repaired or recovered the affected systems.

Trends by CSIRT model include

- None of the ad hoc teams stated that they passed on incidents.
- Coordination centers: 100% said that they provide advice via phone and email and by publishing advisory. None stated that they passed on incidents.
- Combined teams: 100% stated that they provide response via phone and email guidance, while none passed on incidents.
- Distributed dedicated teams: 100% provide response by phone and email guidance; 66% also repair the systems themselves.
- Distributed part-time CSIRTs: 75% said they provide response via phone and email and by repairing and recovering systems themselves.

It makes sense that distributed teams would be involved in the actual recovery and repair of systems, as they are most likely located on-site, in comparison to centralized or coordinating teams who are not on-site and who provide more guidance and support functions. In the same way, the combined and coordination centers seem to rely more on coordination of response and mitigation strategies. The centralized teams had no particular set of response options

across the participating teams; they provide response across all categories of response options.

3.7.7.1 Who Rebuilds Systems?

When asked explicitly who rebuilds and recovers any affected systems, the participating CSIRTs provided the following information:

- 59% of participants stated that the IT department, not the CSIRT, recovers and rebuilds affected systems.
- All of the CSIRTs in the commercial sector said that the IT department recovers and rebuilds systems.
- Most of the other sectors stated that both the IT and CSIRT did recovery and rebuilding.

All of the teams identified as distributed dedicated teams said that only the IT department recovered and rebuilt systems. All other types had either IT or CSIRT or both. No matter where the CSIRT reported—to the IT department or security department, or if the CSIRT was its own department—there was no consistent answer to who recovered and repaired the systems; it was IT, CSIRT, or both.

3.7.8 Computer Forensics Activities

One area of incident analysis and response that is receiving a lot of attention is computer forensics or forensic evidence collection. More teams are learning this analysis technique and more tools are becoming widely available.

There is also growth in reference materials and training available concerning forensics. Many of the authors in the literature refer to investigating computer security incidents (events, attacks, other unauthorized activity) as "computer forensics" [Caloyannides 01, Kruse 02] or "cyber forensics" [Marcella 02].

In 2002 *Information Security* magazine conducted a review of selected books on the topic of forensics and highlighted what was covered in each.[103] This magazine also devoted much of their April 2002 issue to articles on computer forensics and a few case studies [Kessler 02]. Schultz devotes two chapters to an overview of forensics, describing approaches for several types of searches that can be performed, what to look for, how to conduct the investigation, and some of the tools that are used (SafeBack,[104] EnCase,[105] The Coroner's Toolkit[106]) [Schultz 02].

---

[103] For a summary, see <http://www.infosecuritymag.com/2002/apr/pdfs/forensicscomparison.pdf>.
[104] <http://www.forensics-intl.com/safeback.html>

A large portion of Mandia's *Incident Response* is devoted to forensics analyses ("Putting on the Gloves"). This publication includes very specific and detailed descriptions for investigative guidelines (conducting initial assessments to developing response strategies), handling evidence, trap and trace guidance, and surveillance techniques. The book also has sections that focus on specific platforms (Windows NT/2000, UNIX), other specific attacks, and how to investigate incident activity [Mandia 01].

The SANS *Incident Handling Step-by-Step* guide also highlights the importance of understanding and identifying every piece of evidence [SANS 03].

There are other books that focus solely on the issues of computer forensics [Caloyannides 01, Kruse 02, Marcella 02]. Caloyannides focuses on providing information to law enforcement professionals who need technical and procedural training to conduct forensic examinations that will be admissible in court or for business professionals who want to ensure their information is not stolen by anyone. It can also be used by the average reader to further their understanding of technical issues related to computer forensics.

Kruse has organized his publication to provide an introductory course in computer forensics. He suggests that the book can be used as a handbook. It covers evidence collection, tools, and utilities that can be used in the process of investigating incident activity. It also provides guidance on investigating activity involving Windows and UNIX computers.

Van Wyk [van Wyk 01] provides an overview of the "tools of the trade" that CSIRT incident handlers might need to support their investigation of incident activity. He describes not only the investigative tools used (network security monitoring tools) but also other communications "tools" that may be needed during response activity. These tools may include wireless or cellular access and other hardware/software needs, such as CD drives, tape drives, and other removable media.

There seems to be no standard group in an organization that provides forensic analysis. We have seen a wide variety of staff members perform this task. We have seen companies that train their CSIRT staff to perform this type of work. We have also seen organizations that outsource this capability, others that turn it over to law enforcement agencies, and others, particularly government agencies, that turn it over to their investigative units.

Whoever does this work must not only be trained in the technology but must also understand search and seizure and privacy rights laws, along with other relevant laws. Collecting evi-

---

[105] <http://www.guidancesoftware.com/products/EnCaseForensic/>
[106] <http://www.porcupine.org/forensics/tct.html>

dence that may be used in court has legal and personnel issues as well. Anyone who does this kind of work must be prepared to stand up in court as an expert witness.

3.7.9 Answering the CSIRT Hotline

Not all teams manage or operate a help desk or hotline.[107] Some teams use an existing IT help desk phone system to report incidents and then pass the incidents on to the CSIRT. In response to the survey's questions about who staffs the CSIRT hotline and what hours the hotline operates, participants answered as follows:

- 66% said that the CSIRT staff manned the hotline or help desk during business hours.
- 34% said that the CSIRT answered the hotline after business hours.
- Others who answered after business hours were the IT staff (10%) and a message center (14%).
- 83% of the education CSIRTs, 75% of the information and communication CSIRTs, and 50% of the military CSIRTs stated that the CSIRT staff answered the hotline during business hours.

3.7.10 Hours of Operation

Depending on the type and number of staff in the CSIRT, there can be different types and hours of operation. Many who do not have full-time staff on site after hours still may be able to provide support through alternative approaches, such as the use of cell phones, pagers, or third-party answering services.

The CSIRTs participating in the survey had varying hours of operation:

- 59% have standard business hours, starting at 0700, 0800, or 0900 and ending by 1700 or 1800.
- Only 24% have 24x7x365 hours of operation.

A common complaint in the CSIRT community is that many teams do not provide after hours support, therefore, it is not always apparent who to contact in an emergency.

3.7.11 Types of Incidents

There does not seem to be a standard type of incident that is most frequently handled by CSIRTs. This was surprising, as we expected to see almost all teams handling virus and DoS

[107] A hotline is a method for reporting computer security incidents to a CSIRT via a particular telephone number.

attacks. In fact, for the 2003 CSI/FBI Computer Crime and Security Survey, these types of incidents were in the top five types of incidents reported [Richardson 03].

The types of incidents most frequently handled by survey respondents were, not surprisingly, probes and scans. Fifty-one percent of the participating CSIRTs said that they dealt with these incidents most frequently. The next most frequent types of incidents handled were viruses, worms, and Trojan horses (38%).

Sixty-six percent of the participating teams reported that they did not handle theft of data, unauthorized access to data, user compromises, and DoS events frequently.

Looking at the data based on the sector in which the CSIRT is located revealed the following:

- Educational CSIRTs primarily dealt with viruses, misuses of resources, and probes and scans.:
- Non-profit teams stated that the majority of the incidents they handled were viruses or probes and scans.

Other types of incidents mentioned that had not been itemized in the survey list were spamming (10%) and harassment (3%).

In the Information Security Breaches Survey 2002, a thousand telephone interviews were conducted with various information security professionals from different sectors in the United Kingdom (UK). Supplementing these interviews were face-to-face interviews and web-based "polls." An Executive Summary (and pointer to the full technical report) of the survey results are available from Potter [Potter 02]. Sectors included in the survey were finance, telecommunications, technology, travel/leisure/entertainment, utilities/energy/mining, manufacturing, retail/distribution, property/construction, government/health/education/volunteer services, and professional/other services. Fifty-two percent of the participants were in IT management functions.

The following categories of security incidents suffered by UK businesses during the timeframe covered in the survey included the following categories of incident activity:

- virus infections
- unauthorized access to confidential data
- systems failure or data corruption
- hacking attacks on web sites
- staff misuse of company system
- fraud or theft using computer systems

- deletion of files
- "others"

Seventy-seven percent of the UK businesses reported security incidents caused by premeditated or malicious intent. Virus incidents were listed as the worst incidents (33%). The survey also indicated an increase in the percentage of attacks from external sources (66%) [Potter 02].

The survey also indicated that the UK businesses were most focused on resuming normal business operations (73%), followed by preventing similar incidents (68%), and preventing damage to the organization's reputation (61%). Reporting to law enforcement tended to be the least important concern to UK businesses (41%).

The 2003 Australian Computer Crime and Security Survey reported that 80% of computer attacks were virus-related, followed by insider abuse of Internet access/email/computer system resources (62%) [Australia 02].

3.7.12 Number of Incidents

The number of incidents handled varies greatly by team. Some handle one incident a day, some handle hundreds. Of the teams participating in the survey, most handle less than 10 incidents per day:

- 38% handle 1–3 incidents per day
- 18% handle 4–8 per day
- 18% handle more than 15 per day

The participating teams reported the following regarding incidents handled per year:

- 10% handle under 50 incidents per year
- 24% handle 100–500 incidents per year; 14% handle 600–1,000 incidents per year
- 10% handle over 8,000 incidents per year (these were all military, research network, or non-profit CSIRTs)
- All of the banking and finance CSIRTs handle over 450 incidents per year.
- Education CSIRTs, on the average, handle between 1,000 and 4,000 incidents per year.
- One of the non-profit CSIRTs handles over 8,000 incidents per year.

3.7.13 Secure Communications Mechanisms Used

CSIRTs must protect confidential and sensitive data at all times. This often means that a secure method of communication must be established when this data needs to be collected from another source or shared with other appropriate entities.

There are a variety of secure communications mechanisms used by CSIRTs. These can include

- public key cryptography
- secure faxes and phones
- secure intranets or extranets

The majority of the teams participating in the survey stated that they used Pretty Good Privacy (PGP) for secure communications (75%). This could be influenced by the fact that many of the participating teams were FIRST members and FIRST requires use of PGP. Other reported information included the following:

- All of the participating banking and finance teams use PGP and digital certificates.
- All of the education, information and communication, and other commercial CSIRTs use PGP.
- 63% of the military CSIRTs use secure intranets or extranets.
- 66% of the participating non-profit CSIRTs use PGP.
- All of the combined teams use PGP.
- 80% of the centralized dedicated teams use PGP.
- 75% of the distributed part-time teams use PGP and digital certificates to communicate securely.
- The distributed dedicated teams use the most number of tools, with 66% using PGP, digital certificates, secure phones, and secure intranets and extranets.

3.7.14 Coordination and Information Sharing

With the global interconnectedness of the Internet, it is likely that a team will need to coordinate with other external entities at some point. How those interactions occur, with whom, and at what level, will depend on a number of factors (guidance or direction from the parent organization, potential for investigations to occur, the mission and goals of the team, and the services provided). In most cases, the CSIRT is a third-party to the activity—generally they are not the victim or the perpetrator. However, they can be the liaison between affected sites in their constituency and other CSIRTs, external sites, law enforcement, or the media.

Effective teams will have a plan in place for how such coordination and interaction occurs so that when an event happens, the team is positioned to quickly and efficiently orchestrate such activities. This could include having pre-determined contacts set up (names, phone numbers, email addresses, encryption keys) and/or tools to support disseminating information (tools to extract relevant log information, mailing lists and mail merge tools to automate contacting sites, automated tools to look up contact information from whois servers, etc.). There may be pre-arranged non-disclosure agreements that are signed between the CSIRT and other external contacts (for example, trusted experts who might assist in incident or vulnerability analysis).

Identifying the appropriate level of detail for what data is shared with others might be worked out or negotiated prior to an event, but it has also been the case that such arrangements may need to be made as an incident is unfolding and the incident is being analyzed. To the extent that it is possible to determine beforehand who the team will share information with, how to contact them, at what level of detail data is provided, and the method for dissemination or access to that data, the more the CSIRT will be able to undertake such information sharing efficiently and effectively. Some level of trust will also have to be discussed and agreed to. This will involve what will be done with shared information, how confidential information will be exchanged, and also with whom this information will be shared.

Van Wyk discusses pulling together the key players and having a Crisis Action Meeting to determine appropriate actions for coordination and communication with others [van Wyk 01]. Part of such activity will determine what needs to be done allowing the team to then prioritize those actions. Schultz also provides suggestions for establishing relationships with external entities similar to those mentioned above [Schultz 01].

Depending on the CSIRT constituency and parent or host organization, who the CSIRT shares information and data with and who a CSIRT coordinates response with can vary. We asked the CSIRTs who participated in the survey with whom they coordinated their response and with whom they shared data. Their responses are discussed in the following two sections.

3.7.14.1 With Whom Does the CSIRT Coordinate Activities?

CSIRTs coordinate response activities with internal departments and externally with other CSIRTs, law enforcement agencies, and security experts. Of the CSIRTs that participated in the survey,

- 66% coordinate their response activities with their CIO, IT and telecommunications departments, or law enforcement
- 58% coordinate with other CSIRTs
- 41% coordinate with their legal department

Other areas not included on the survey list that were mentioned as coordination partners include government organizations, investigators, CEOs, and system owners.

Looking at this information by sector,

- All of the participating banking and finance CSIRTs coordinate with their CIO, physical security department, law enforcement and investigators.
- All of the information and communication CSIRTs coordinate their response activities with their CIO, legal department, and public relations department. 75% of the information and communication CSIRTs also stated that they coordinated with law enforcement and other CSIRTs.
- All of the other commercial CSIRTs coordinate with business managers, the legal department, the public relations department, and other CSIRTs.
- There were no specific trends for educational, military, or non-profit CSIRTs.

Looking at this information by CSIRT model,

- 75% of the ad hoc teams coordinate with other CSIRTs.
- 100% of the coordination centers coordinate with their CIO and law enforcement.
- 83% of the centralized teams coordinate with law enforcement. 60% coordinate with their CIO. 50% stated that they coordinate with the CERT/CC. 50% also coordinate with other CSIRTs and security experts.
- 80% of the combined teams coordinate with law enforcement, while 60% coordinate with their CIO and their legal department.
- 100% of the distributed dedicated teams coordinate with their CIO and public relations department. 66% coordinate with law enforcement, other CSIRTs, and with their legal departments.
- 75% of the distributed part-time teams coordinate with other CSIRTs; 50% coordinate with their CIO, business managers, human resources department, physical security, legal department, public relations department, and law enforcement.

3.7.14.2 With Whom Does the CSIRT Share Information?

The majority of CSIRTs share information with the CIO (66%), the IT and telecommunications departments (58%), law enforcement (58%), and other CSIRTs (55%). Others that were mentioned and not included in the original survey list of options were investigators. An interesting question to ask in future surveys would be what type of information is shared.

Looking at this information by CSIRT sector,

- 100% of the banking and finance CSIRTs share information with their CIO, their audit department, law enforcement, and their IT and telecommunications departments.

- 83% of the education CSIRTs share information with their CIO; 66% share information with business mangers, their IT and telecommunications department, and their legal department.
- 75% of the information and communication CSIRTs share information with their CIO, other CSIRTs, and law enforcement.
- 63% of military CSIRTs share information with other military organizations, their IT and telecommunications department, and their CIO.
- 100% of other commercial CSIRTs share information with their CIO and with other CSIRTs.
- 75% of the participating non-profit CSIRTs share information with law enforcement and other CSIRTs.

Looking at this information by CSIRT model,

- 100% of identified coordination centers share information with the CIO, law enforcement, and the IT and telecommunications departments.
- 70% of the centralized CSIRTs share information with their CIO and IT and telecommunications departments; 80% share information with law enforcement.
- 80% of the combined teams share information with other CSIRTs and law enforcement.
- 100% of the distributed dedicated teams share information with the CIO; 75% share information with business managers, IT and telecommunications departments, and law enforcement.
- 75% of distributed part-time teams share information with other CSIRTs and the IT and telecommunications departments; 50% share information with the CIO, business managers, and the human resources department.

3.7.15 Documenting Policies and Procedures

Documenting policies and procedures is one of the most important activities a CSIRT must undertake to be successful over the long term. Oppenheimer et al., in a booklet for system administrators published by SAGE, state that "security policies are among the most crucial elements of a security infrastructure." They go on to discuss key elements to consider in the policy design and implementation phase:

- How specific should the policy be?
- How much control should the policy enforce?
- What is the appropriate security policy structure? [Oppenheimer 97]

While these questions relate to system administration and security policies, they are still valid key elements in the design of policies and, modified slightly to focus on incident response issues, can apply equally well in the CSIRT environment.

Mandia captures it very nicely: "Words that go together: Sonny and Cher, Donnie and Marie, and Policies and Procedures. You cannot talk about one without the other" [Mandia 01]. In the CERT CSIRT Development Team training courses, we define CSIRT policies as "what you want to do" and CSIRT procedures as "the step-by-step instructions for how you do it."

In the absence of well-defined policies and procedures, incident handling staff (and your constituency for that matter) will make up their own rules and guidelines. The lack of these documents can be detrimental to the success of the CSIRT.

The *Handbook for CSIRTs* provides an overview of policy attributes, listing management endorsement, clarity, need, usability, implementation, and enforcement [West-Brown 03]. Included in the description of each of these attributes are tips or sample statements to help the reader in developing such policies. Some of the typical policy content features are also identified, along with suggestions about how these might be defined in the policy.

In a recent *InfoSecurity News* magazine devoted to computer forensics articles, Rothke discusses having an incident response staff and comprehensive policies and procedures, and states, "If there are no policies and procedures in place, there is no way to ascertain that things are being done properly" [Rothke 02].

Symantec's white paper on planning for incident response discusses the need to establish policies and procedures. "Without policies and procedures, employees have no understanding about what is and is not acceptable" [Symantec 02].

3.8 Changes in Intruder Attacks and Tools

As time goes by, the types of computer security incidents and attacks, along with methods, tools, and techniques used by intruders, continue to evolve. During the 1980s, intruders primarily exploited passwords and known vulnerabilities to gain unauthorized access to computer systems. Later, intruders moved on to exploit protocol flaws, examine source code for new security flaws, install network sniffer programs, use IP source address spoofing in attacks, and conduct widespread, automated scanning of the Internet to identify additional targets. In each of these progressions, the more knowledgeable intruders have transferred their "expertise" to novices by creating easy-to-use exploitation scripts and increasingly sophisticated toolkits, while taking advantage of the currently available technologies.

Figure 14 demonstrates how the required intruder knowledge (curved line) has decreased over time in comparison to the increase in the sophistication of attacks and intruder tools (straight line). Today intruders with little knowledge can execute sophisticated attacks with the click of a button, as the intruder tools have combined and automated tools for finding and exploiting vulnerable systems.

Reproduced From
Best Available Copy

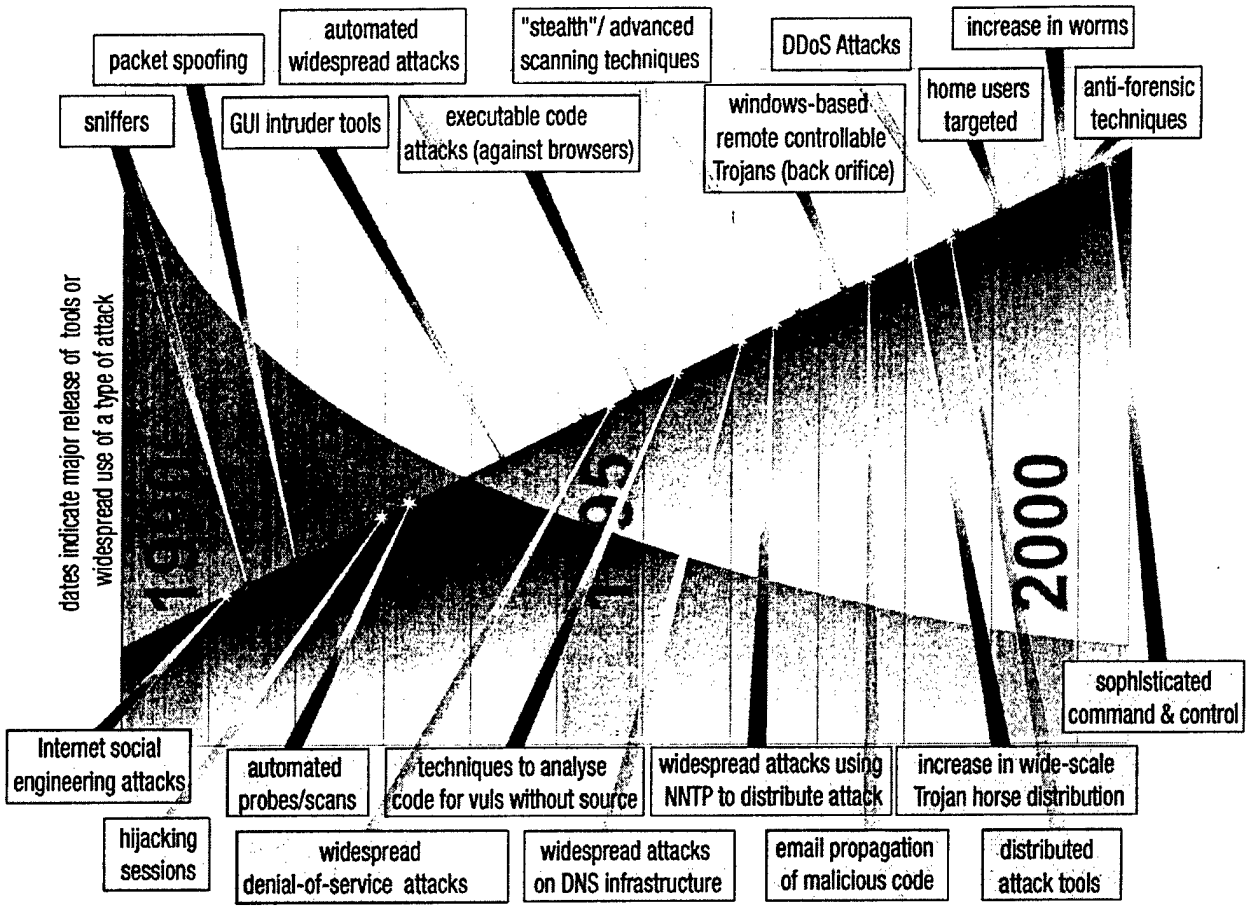


Figure 14: Attack Sophistication Versus Required Intruder Knowledge

In 2002, the CERT/CC published a short paper, "Overview of Attack Trends" [CERT 02b], which highlighted these major trends:

- automation and speed of attack tools

  The level of automation of attack tools continues to increase. Today's scanning tools use more advanced scanning patterns to maximize impact and speed. Some tools exploit identified vulnerabilities as part of the scanning activity, and others may self-initiate a new attack on those compromised systems, increasing the speed of propagation. Distributed attack tools have enabled attackers to manage and coordinate large numbers of deployed attack tools distributed across the Internet. These distributed attack tools can not only launch DoS attacks more efficiently, but also scan for other potential victims and compromise vulnerable systems, while taking advantage of readily available public communications protocols (such as Internet Relay Chat and instant messaging) to coordinate their functions.

- increasing sophistication of attack tools

  Attack tools are more difficult to detect and discover, due to the anti-forensic nature, dynamic behavior, and modularity of these tools. Attack tool developers use techniques to

hide the nature of their attack. Some tools can vary the patterns and behaviors at random, through predefined decision paths, or through direct intruder management. And the modularity of some tools can allow polymorphic tools to self-evolve, as well as tools that can run on multiple operating system platforms.

- faster discovery of vulnerabilities

  The number of newly discovered vulnerabilities reported to the CERT/CC continues to double each year, making it more difficult for administrators to keep up to date with patches.

- increasing permeability of firewalls

  Although firewalls are often relied upon to provide primary protection from intruders, technologies and protocols are being designed to bypass typical firewall configurations. Some of this also arises from increased demands for off-site access and more complex protocols being allowed through the firewall.

- increasingly asymmetric threat

  A single attacker can relatively easily employ a large number of distributed systems to launch devastating attacks against a single victim. Each Internet system's exposure to attack depends on the state of security of the rest of the systems attached to the global Internet.

- increasing threat from infrastructure attacks

  Attacks that affect key components of the Internet can broadly affect organizations and users who have increasing dependency on the Internet. Distributed DoS attacks, worms and viruses, attacks on the Internet Domain Name System (DNS)), and attacks against routers are among the infrastructure attacks that have the potential to disrupt day-to-day business. The impacts of these infrastructure attacks are denial of service, compromise of sensitive information, misinformation, and having time and resources diverted from other tasks.

These trends still hold true at the date of the publishing of this report. One trend that has actually continued to increase, creating a major impact on CSIRTs and their related constituencies, is the speed of attacks. With worms such as Slammer and Blaster, and mass email spreading viruses like Sobig.F, the time to respond to an incident has become drastically reduced. Because of this, CSIRTS and their constituencies need to be more prepared to take actions that previously might not have been acceptable, such as blocking certain types of traffic or shutting down certain services to stop the spread of activity. Some of the actions taken may cause undesirable affects. For example, when the Slammer worm hit in January 2003, many sites had to block SQL traffic, causing an impact on legitimate services running on non-infected systems, as part of a way to stop the worm from spreading. In cases such as these, CSIRT and IT staff have to take quick action; there may not be time for discussion with service managers or customers. Such emergency situations need to be addressed in any response plans and in any authority given to the CSIRT.

The speed with which such malicious attacks spread have reinforced the need for a good incident response plan to be in place, including established channels of communication, identified response staff, notification lists, and established recovery policies and procedures. Involvement of the CSIRT in the configuration of the constituency infrastructure is also important, as the only response is often to stop the incident from happening at your site, by ensuring your site is not vulnerable or has good perimeter defenses and host configurations.

Other trends previously noted by the CERT/CC have warned of attacks against Windows-based targets, especially in DoS attacks,[108] as well as attackers increasingly targeting home users' systems because of their wide availability, high bandwidth, and relative lack of security. The CERT/CC has created a section on their web site for home users,[109] containing a number of articles, as well as a document titled "Home Network Security."[110]

These trends outlined by the CERT/CC indicate that organizations relying on the Internet face significant challenges to ensure that their networks operate safely and that their systems continue to provide critical services even in the face of attack.

3.8.1 Impact on Incident Response

The growing threats caused by intruder attack trends have affected the way in which CSIRT staff must respond. The sheer number of attacks that are detected and reported continues to rise, with many CSIRTs typically seeing a doubling (or more) in the rate of new incident reports with each passing year. Annual incident statistics posted by the CERT/CC[111] and the CSI/FBI Computer Crime and Security Surveys[112] are frequently cited as examples of the growing rate of incident reports.

---

108 "Trends in Denial of Service Attack Technology" <http://www.cert.org/archive/pdf/DoS_trends.pdf>

109 <http://www.cert.org/homeusers/>

110 "Home Network Security" <http://www.cert.org/tech_tips/home_networks.html>

111 <http://www.cert.org/stats/cert_stats.html>

112 <http://www.gocsi.com/press/20030528.jhtml>

Reproduced From
Best Available Copy

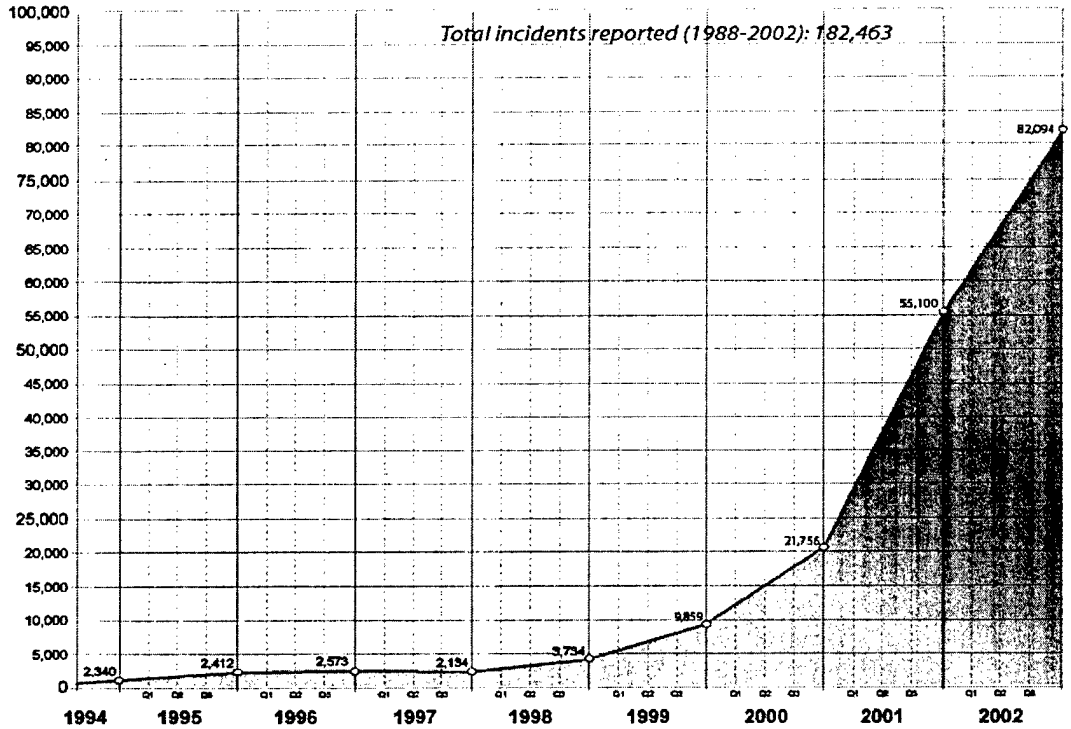


Figure 15: CERT/CC statistics on Incidents Reported from 1994 to 2002

In addition to the ever-increasing volume of incident reports, the rate at which new vulnerabilities are discovered also continues to increase.

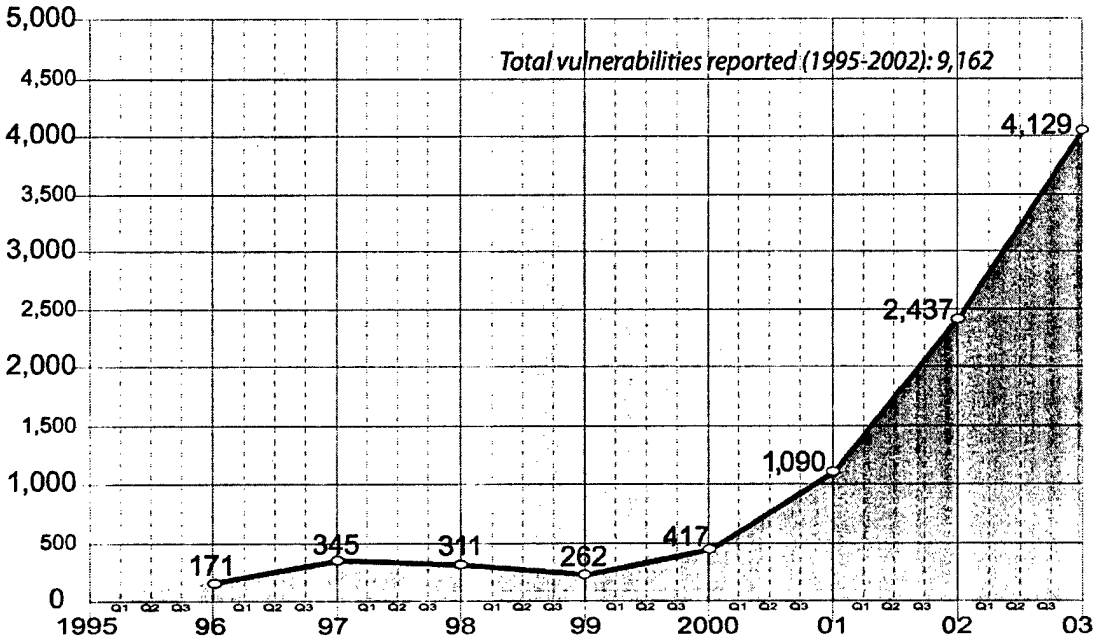


Figure 16: CERT/CC Statistics on Vulnerabilities Reported from 1995 to 2002

As the volume of incident and vulnerability reports continue to rise,[113] and the automation and speed of many attack tools continue to increase, CSIRT and information security staff members now have less time to react to new threats. For example, where the 1999 Melissa virus propagated around the Internet within days, the 2000 Love Letter worm circulated the globe in one day, the 2001 Code Red and Nimda worms reached global saturation in less than 18 hours, and the 2003 SQL/Slammer Worm reached saturation on vulnerable servers within in 10-18 minutes. Every passing minute of unprotected exposure or delayed response against an attack increases the likelihood that that attack may succeed or have some detrimental effects against the vulnerable target. The rapid spread of attacks points to the fact that reactive activities alone cannot sustain CSIRT work. CSIRTs must work with organizations to proactively protect systems and resources.

3.9 Legal Issues and Cyber Crime Laws

Although the analysis of computer security incidents often focuses on the technical issues of an incident (primarily the "what" and the "how"), there may be occasions when a CSIRT might need to become involved in the investigative process (the "who" and the "why"), or at least work closely with those who have such an investigative role. If there is any intention to report an incident to the appropriate law enforcement agencies, it will be important for CSIRT members to understand the legal issues involved and to have some familiarity with the relevant laws in the affected jurisdiction.

Generally, computer crimes include traditional crimes (such as theft and fraud) that are committed with the use of computers, and cyber crimes that are committed against computers (viruses, denial of service attacks). In addition to statutory laws that have been enacted by legislatures, there are also common laws or case laws that are the result of court decisions and judicial opinions. While the statutory computer crime laws continue their slow growth and evolution, new case laws are also developing on an ongoing basis.

It is important for CSIRT members to also be familiar with any privacy laws that provide protection to others, in order to avoid the possible suppression of any improperly gathered evidence that is intended to be presented in a court of law, as well as to avoid potential criminal or civil liability. (In many jurisdictions, for example, laws may prohibit the unlawful interception of, or access to, transmitted and stored data and communications; this may also include prohibiting access to that data by system administrators or incident handlers if certain conditions are not met.)

---

[113] See <http://www.cert.org/stats/cert_stats.html and http://www.kb.cert.org/vuls>.

Furthermore, CSIRT members must be familiar with any laws or regulations that may affect their incident response and coordination efforts, such as requirements to notify others in the event of a security breach. (For example, a 2003 law in the state of California requires anyone who "conducts business" with any California resident to disclose any breach of security of a system involving the unauthorized acquisition of the resident's unencrypted personal information.[114]) Several specific laws and regulations will be mentioned in the next sections.

In recent years, guidelines and standards for obtaining and handling computer evidence have been developed by a number of sources. For example, the International Organization on Computer Evidence (IOCE)[115] developed a short set of principles for standardizing the recovery of computer-based evidence.[116] In the United States, the Department of Justice has published detailed manuals for "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations"[117] and the National Institute of Justice (NIJ) guide "Electronic Crime Scene Investigation: A Guide for First Responders."[118]

The U.S. Secret Service and the International Association of Chiefs of Police[119] have published "Best Practices for Seizing Electronic Evidence."[120] And the Internet Society has published a Best Current Practice (BCP 55/RFC 3227) on "Guidelines for Evidence Collection and Archiving."[121]

As applicable laws may be varied and numerous, and the interpretation of some laws might not be obvious or straightforward, it is highly recommended to seek the guidance of knowledgeable legal counsel, as well as management, in determining the response to a computer security incident. Such legal guidance should be incorporated into all incident response policies and procedures. Because of this, it is often recommended that a team should look to establish a working relationship with local law enforcement and with their own legal counsel.

3.9.1 International Cyber Crime Laws

It is still the case that many nations do not yet have effective laws to address computer crimes. But recent efforts by a number of different countries and organizations are setting the stage for the harmonization of substantive and procedural laws among multiple nations, and

---

114 California Civil Code Section 1798.82 <http://www.leginfo.ca.gov/>
115 <http://www.ioce.org/>
116 <http://www.ioce.org/G8_proposed_principles_for_forensic_evidence.html>
117 <http://www.cybercrime.gov/s&smanual2002.htm>
118 <http://www.ojp.usdoj.gov/nij/pubs-sum/187736.htm>
119 <http://www.theiacp.org/>
120 <http://www.secretservice.gov/electronic_evidence.shtml>
121 <ftp://ftp.rfc-editor.org/in-notes/rfc3227.txt>

enabling better cooperation and assistance between nations during the course of computer crime investigations involving systems in different jurisdictions.

On the international front, the Council of Europe[122] worked for over four years to draft a Convention on Cybercrime (ETS no. 185),[123] which was adopted by the Committee of Ministers of the Council of Europe and opened for signatures in 2001. Although this Convention has not yet entered into force as of this writing (it is still awaiting ratification in 2003), this is the first international treaty focused on computer crimes. The chapters in the Convention on Cybercrime include measures to be taken at the national level (by each party acceding to the treaty) on both substantive criminal law (defining certain criminal offenses, to allow national laws to be harmonized) and procedural law (defining investigation and criminal prosecution methods appropriate to a computer environment and enabling national criminal procedures to be brought more closely into line with each other). The criminal offenses defined in the Convention include

- offences against the confidentiality, integrity and availability of computer data and systems (illegal access; illegal interception; data interference; system interference; and misuse of devices)
- computer-related offences (computer-related forgery; and computer-related fraud)
- content-related offences (offences related to child pornography)
- offences related to infringements of copyright and related rights

The CoE Convention on Cybercrime also addresses principles relating to international cooperation and mutual assistance (including setting up a 24x7 point of contact for facilitating investigations of computer crimes). In 2003, the first Additional Protocol to the Convention on Cybercrime (ETS no. 189)[124] was opened for signatures, which would extend the Cybercrime Convention's scope to also criminalize acts of a racist or xenophobic nature committed through computer systems.

The European Union (EU[125]) has also taken steps to fight high-tech crime and illegal content on the Internet.[126] In 1999, the EU adopted a four-year funding program, the Safer Internet Action Plan, or IAP (Decision No. 276/1999/EC[127]) "on promoting safer use of the Internet by combating illegal and harmful content on global networks"; an amendment (Decision No.

---

122 <http://www.coe.int/>

123 <http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=185>

124 <http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=189>

125 <http://europa.eu.int/>. The European Union's three primary decision-making bodies are the European Parliament, the Council of the European Union, and the European Commission. See The European Union at a glance <http://europa.eu.int/abc-en.htm>, and Institutions of the European Union <http://europa.eu.int/inst-en.htm>.

126 <http://europa.eu.int/information_society/topics/telecoms/internet/crime/text_en.htm>

127 <http://europa.eu.int/eur-lex/pri/en/oj/dat/1999/l_033/l_03319990206en00010011.pdf>

1151/2003/EC[128]) was adopted in 2003, calling for a two-year extension of the IAP (through 2004) and adapting its scope and implementation. The European Commission also adopted a proposal for a Council Framework Decision on attacks against information systems,[129] consistent with the CoE Convention on Cybercrime, to approximate criminal law for illegal access to and interference with information systems, and to ensure the greatest possible police and judicial cooperation in the area of criminal offences related to attacks against information systems. This proposal for a decision was amended and approved by the European Parliament, and is now (as of this writing) waiting final decision and signature to be enacted. The European Commission's Information Society Directorate-General has also commissioned and funded a CSIRT Handbook of Legislative Procedures,[130] to assist European CSIRTs with a guide that "matches technical descriptions of incidents to the legal framework of the country in question and details procedures for working with law enforcement to respond to incidents."[131] This handbook was published in paper form in September 2003.[132]

The "Group of 8" (G8) major industrial democracies[133] has held summits, meetings, and workshops and has proposed recommendations for the fight against high-tech and Internet-based crimes, which may influence the standardization of other laws in the future. The G8 Lyon Group[134] (formerly the Senior Experts Group on Transnational Organized Crime) has worked on technical as well as legal issues (judicial cooperation, law enforcement projects, high-tech crime) to fight transnational organized crime, including the establishment of a network of 24-hour points of contact in many countries around the world.[135] Recent G8 meetings have focused on safety and confidence in cyber space, and on combating high-tech crime.[136]

In 2000, the United Nations (UN) General Assembly adopted the "United Nations Convention Against Transnational Organized Crime"[137] to promote cooperation to prevent and combat transnational organized crime more effectively. Although not specifically focused on cyber crimes, the articles in the Convention will apply to high-tech criminal investigations, by providing the legal framework to harmonize different legal systems and to overcome traditional problems associated with international cooperation and mutual assistance.

---

128 <http://europa.eu.int/eur-lex/pri/en/oj/dat/2003/l_162/l_16220030701en00010004.pdf>

129 <http://europa.eu.int/eur-lex/en/com/pdf/2002/com2002_0173en01.pdf>

130 <http://www.iaac.org.uk/csirt.htm>

131 <http://www.iaac.org.uk/CSIRT Handbook workplan.pdf>. "Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries for assisting Computer Security Incident Response Teams (CSIRTs)"

132 The handbook can be obtained from RAND Europe at the following address: RAND Europe - Leiden, Newtonweg 1, 2333 CP Leiden, The Netherlands. Tel. +31 71 524 5151; Fax +31 71 524 5191.

133 <http://www.g8.utoronto.ca/>. The G8 countries consist of Canada, France, Germany, Italy, Japan, Russia, the United Kingdom, and the United States, plus representatives from the European Union.

134 <http://www.g8.utoronto.ca/crime/>

135 <http://www.g8.utoronto.ca/adhoc/crime99.htm>

136 <http://www.mofa.go.jp/policy/i_crime/>

137 <http://www.odccp.org/crime_cicp_convention.html>

3.9.2 United States Cyber Crime Laws

In the United States, the Computer Fraud and Abuse Act (18 U.S.C. 1030[138]) has been one of the primary legal instruments for fighting computer intrusions. In addition to the offenses outlined in Section 1030, dealing with unauthorized access to computers, other sections of Title 18 of the United States Code describe other federal offences related to activity in connection with access devices, destruction and denial of service, and unlawful access to transmitted or stored communications. The U.S. Department of Justice, Computer Crime and Intellectual Property Section (CCIPS), has created a web site to provide information about computer crime and intellectual property crime laws, policies, cases, and other documents. (See list of laws and URLs in Appendix D.)

At the state level, individual states have also created their own legislation addressing computer crime activity within their jurisdictions. Most state laws are available online, and a number of sites that provide links to state computer crime laws are included in Appendix D.

In addition to the above federal and state statutory laws, some industries or sectors may also be subject to additional federal regulations or special requirements that relate to information security, data protection, and privacy issues in their particular industry or sector. For example, in the United States, health insurance and health care providers and the financial services industry (including banks and insurance companies) are required to protect consumer data and establish safeguards to protect the privacy and disclosure of nonpublic personal information, as outlined in the Health Insurance Portability and Accountability Act) (HIPAA)[139] and the Gramm-Leach-Bliley Act,[140] respectively. And U.S. federal government agencies are responsible for ensuring the information security of their systems, including performing annual independent evaluations, as outlined by the Federal Information Security Management Act (part of the E-Government Act of 2002).[141] Under FISMA, all U.S. federal agencies are also required to establish an incident response capability and procedures for detecting, reporting, and responding to security incidents.

3.10 Current Projects

Throughout the CSIRT and computer security community many interesting projects are being organized that may be of benefit to other CSIRTs. This benefit may range from the introduc-

---

138 Search the United States Code for a specific section at <http://uscode.house.gov/usc.htm>.

139 <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=104_cong_public_laws&docid=f:publ191.104.pdf>

140 <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws&docid=f:publ102.106.pdf>

141 <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ347.107.pdf>

tion of knowledge resources, tools, or standards that may help a CSIRT's day-to-day operations to organizational projects that try to facilitate coordination and collaboration between CSIRTs.

The projects below have been grouped into the following categories: Coordination and Collaboration, Standards, Incident Data Collection, Tools, Information Resources, and Research.[142] It is a selection of known projects as of September 2003. This is not a comprehensive list; if you have suggestions for inclusions please send them to csirt-info@cert.org.

Note that these projects are mentioned here for information purposes only. Inclusion in this report does not constitute an endorsement by the CERT/CC.

3.10.1 Coordination and Collaboration

There has been considerable discussion in the CSIRT community about efforts to establish communication and coordination mechanisms between CSIRTs in various geographical regions that have a need to work together due to their close proximity or shared issues. Methods being investigated include establishing operational incident coordination mechanisms and establishing forms or formats for exchanging incident data.

Reviewing and following these types of projects can provide CSIRTs with a resource for keeping up to date on trends, issues, and tools that are discussed. These projects can also provide ideas for other teams that plan to perform similar activities.

3.10.1.1 CSIRT Task Force for European CSIRTs

As discussed in Section 2.3.3, this task force sponsored by TERENA helps coordinate incident response and prevention in the European Community. The TF meets three times a year, provides a mailing list, and is involved in numerous ongoing projects such as the Clearinghouse for Incident Handling Tools and the development of IODEF. The TF works to facilitate collaboration and information exchange between European CSIRTs. The web site for the TF-CSIRT includes meeting minutes and copies of various presentations and CSIRT overviews presented at the meetings [TERENA 03].

For more information see:
<http://www.terena.nl/tech/task-forces/tf-csirt/>

---

[142] Some projects may actually fall in more than one category, but are discussed in just one for ease of organization.

3.10.1.2 Trusted Introducer for CSIRTs in Europe

As discussed in Section 2.3.3, this service was originally sponsored by TERENA to create a method for the validation and introduction of CSIRTs into the European CSIRT community. Besides providing a directory of all known CSIRTs in Europe, the Trusted Introducer (TI) provides an accreditation framework. CSIRTs that meet a set of requirements are designated as accredited teams. These criteria include publishing their contact information and cryptographic keys and key policies. Teams must also agree to support the TI process that ensures that the information available about a team is updated at regular intervals. Part of the information from accredited teams is published, while more internal information about policies is restricted to the community of accredited teams. When accredited status is achieved, teams can participate in additional services such as closed mailing lists and information exchange meetings.

The TI process has been in operation since September 2000 and is supervised by a TI Review Board elected from the accredited teams [T1 03].

For more information see:
<http://www.ti.terena.nl/>

3.10.1.3 eCSIRT.net – The European CSIRT Network

eCSIRT.net is a project funded under the European Information Societies Technology program and started July 1, 2002.[143] The project focuses on the deployment of techniques to help meet the needs of existing teams for cooperating and exchanging incident-related data. The project will also look at methods for CSIRTs to collect shared data for statistical and knowledge-base purposes. The project states that it will serve the following goals [eCSIRT 03]:

- Establish a standardized and unambiguous exchange of incident-related information between the CSIRTs involved.
- Establish the collection of standardized and unambiguous incident statistics to serve the CSIRTs involved and, in a generalized fashion, serve the information needs of a wider audience.
- Establish the collection of standardized and unambiguous incident-related data, followed by intelligent generation of warnings and emergency alerts based on that integrated dataset, to serve the CSIRTs involved.

[143] While there is the recognized need for more European CSIRTs, this project does not address the need for additional CSIRTs in particular, although its results will affect any CSIRT, whether existing or new, as the techniques that will be brought to fruition in the project will be shared with the rest of the European CSIRT community.

The project will first attempt to establish a "standardized and unambiguous" language for data exchange. The project will use and build on IODEF and IDMEF work done by the IETF and TF-CSIRT. eCSIRT.net aims at employing IODEF, IDMEF, and other relevant techniques in an operational setting between European national research network CSIRTs involving two commercial companies active in the CSIRT market.

The technical work is organized as follows:

- preparation phase ("defining a common language")
- usage phase ("using the common language between partners")
- clearinghouse function ("gathering incident statistics from partners using the common language")
- alert function ("gathering incident data from partners to derive early warnings and emergency alerts from, and spread these to partners securely")

More can be read at:
<http://www.ecsirt.net/>

3.10.1.4 European Information Security Prevention Programme

According to its web site, "The European Information Security Promotion Programme (EISPP) is a project co-funded by the European Community under the Fifth Framework Programme. The EISPP project aims to develop a European framework, not only to share security knowledge but also to define the content and ways of disseminating security information to SMEs.[144] By providing European SMEs with the necessary IT security services, they will be encouraged to develop their trust and usage of e-commerce, leading to increased and better opportunities for new business....The project, started in June 2002 with an expected duration of 18 months, is run by a consortium of private sector organisations comprising CERTs, ISP/ASPs, and security professional organisations" [EISPP 03].

One of the objectives of the program is to "Set up a network of expertise among the European CERTs that will allow them to share and enhance their own preventative material and to 'open' it to the other CERTs and organisations involved in prevention" [EISPP 03].

For more information please see:
<http://www.eispp.org/>

[144] "SME" stands for "small and medium enterprises."

3.10.1.5 Asia Pacific Computer Emergency Response Team (APCERT)

As discussed in Section 2.3.4, this coordination initiative "was established to encourage and support the cooperation between CSIRT (Computer Security Incident Response Team) organizations in the Asia Pacific region. The mission of the APCERT is to maintain a trusted contact network of computer security experts in the Asia Pacific region to improve the regions' awareness and competency in relation to computer security incidents" [APCERT 03].

For more information please see:
<http://www.apcert.org/>

3.10.2 Standards for Sharing or Collecting Information

As mentioned earlier, there are no standard mechanisms adopted by all teams to share information, collect incident data, or develop CSIRT publications. There is much discussion today that some standards for performing these tasks would simplify the sharing of information and the synthesis of this information into a picture of overall incident activity around the globe.

A variety of standards for collecting and sharing data and information are currently being presented for review and comment in the CSIRT community. CSIRTs will want to follow these developments and the evolution of standards to determine if they are of benefit to their team. The standards may be able to be adopted as they are or adapted to fit the information exchange needs of the CSIRT. They can also be used to help determine fields and formats for incident tracking systems or be incorporated into other incident handling tools and products.

Teams can actively participate in the standards work by serving on working groups, reviewing and commenting on standards, or testing them in their environment. Some of the current standards work going on is described below.

3.10.2.1 IETF Incident Handling Working Group (INCH WG)

This working group was established to create a standard that will support a representation of common data needed in incident handling. The WG plans to do this by creating a data model that can be used for the exchange of incident or vulnerability data and information. The INCH WG will build on the work started by the IODEF[145] project in the TERENA TF-CSIRT community. This project looked for a structured method of exchanging data between CSIRTs using XML.

---

[145] IODEF is the Incident Object Definition and Exchange Format. More information on this project can be found at <http://www.ietf.org/rfc/rfc3067.txt>.

According to the INCH WG Charter and Scope, "The purpose of the Incident Handling Working Group is to define data formats for communication between

- a CSIRT and its constituency (e.g., users, customers, trusted reporters) which reports system misuse;
- a CSIRT and parties involved in an incident investigation (e.g., law enforcement, attacking site); and
- collaborating CSIRTs sharing information" [INCH 02].

Deliverables and outputs from the working group include:

- "A document describing the high-level functional requirements of a data format for collaboration between CSIRTs and parties involved when handling computer security incidents.
- A specification of the extensible, incident data language that describes the data formats that satisfy the requirements.
- Guidelines for implementing the WG data format (Output #2 of the WG).
- A set of sample incident reports and their associate representation in the incident data language" [INCH 02].

For more information see:
<http://www.ietf.org/html.charters/inch-charter.html>

3.10.2.2 IETF Intrusion Detection Working Group (IDWG)

According to the charter of this working group, "The purpose of the Intrusion Detection Working Group is to define data formats and exchange procedures for sharing information of interest to intrusion detection and response systems, and to management systems which may need to interact with them" [IDMEF 02].

The IDMEF data model and XML data definition document can be read at:
<http://www.ietf.org/internet-drafts/draft-ietf-idwg-requirements-10.txt>

For more information see:
<http://www.ietf.org/html.charters/idwg-charter.html>

3.10.2.3 Common Advisory Interchange Format (CAIF)

The purpose of this project is to design a standardized structure and format for creating and exchanging security advisories [CAIF 02]. A subscriber mailing list and a description of the CAIF requirements are available from the project's web site.

For more information see:
<http://cert.uni-stuttgart.de/projects/caif/>

3.10.2.4 Guidelines for Evidence Collection and Archiving (RFC 3227, Best Practice)

This RFC provides high-level guidelines for collecting and archiving data related to an intrusion. It presents best practice recommendations for determining volatility of data, deciding what to collect, performing the collection, and determining how to store and document the data. It also brings up topics to consider concerning privacy and legal issues when collecting intrusion data.

For more information see:
<http://www.ietf.org/rfc/rfc3227.txt>

3.10.2.5 Australian Standard for Managing IT Evidence (HB-171-2003)

This standard "provides guidance on the management of electronic records that may be used as evidence in judicial or administrative proceedings, whether as a plaintiff, defendant, or witness." It specifically deals with litigation in Australia, but is based on general best practices in forensic evidence collection and IT security [HB171].

For more information see:
<http://www.standards.com.au/catalogue/script/Details.asp?DocN=AS342335504743>

3.10.2.6 Expectations for Computer Security Incident Response (RFC 2350, Best Practice)

One of the older best practice documents that involved CSIRTs was the "Expectations for Computer Security Incident Response" RFC. This document provides guidance on the type of information that should be published to a CSIRT's constituency and to other CSIRTs. It discusses defining the CSIRT's mission, charter, constituency, services, policies, and procedures.

For more information see:
<http://www.ietf.org/rfc/rfc2350.txt>

3.10.3 Incident Data Collection

New teams are always looking for tools to not only help them collect incident data but also to compare how their incident activity compares with other sites and organizations. During an incident, a team will often need to determine if what they are seeing is limited to their systems or is more widespread. Various organizations have been developing tools or mecha-

nisms for collecting, correlating, and synthesizing incident data. Some of these projects and tools are described below.

3.10.3.1 AirCERT

The AirCERT (Automated Incident Reporting) is a development project by the CERT/CC to automate the reporting of incident data in a manner so that data can easily be summarized and queried to provide a view of network activity. It involves the placement of Internet-based security event sensors on the networks of various organizations attached to the Internet. These sensors will log locally selected information on detected security events and anomalies to both a local database and a central database located at the CERT/CC. The local organization can decide what, if any, data is passed to the CERT/CC and can sanitize the data as desired. The CERT/CC has developed a prototype of this system using open source and low-cost components. The current prototype is based on collecting data using Snort, an open source IDS. Future prototypes will look at collecting data from other IDS, including off-the-shelf products.

The following components are available for download and use:

- Snort XML plug-in
- Analysis Console for Intrusion Databases (ACID). ACID is a PHP-based analysis engine for searching and processing a database of security events generated by various IDSes, firewalls, and network monitoring tools.

For more information see:
<http://www.cert.org/kb/aircert/>

3.10.3.2 CERT/CC Current Activity

The CERT/CC Current Activity web page is a regularly updated summary of the most frequent, high-impact types of security incidents currently being reported to the CERT/CC. Any security incidents can be reported to the CERT/CC via their incident reporting form located at <http://www.cert.org/reporting/incident_form.txt> or via email to cert@cert.org.

CERT/CC also summarizes the scanning activity that is currently being reported to it. This information can be viewed at <http://www.cert.org/current/scanning.html>.

Anyone submitting logs and data should ensure that the information has been appropriately sanitized or is submitted in a secure manner.

For more information see:
<http://www.cert.org/current/>
<http://www.cert.org/contact_cert/>

3.10.3.3 Distributed Intrusion Detection System (DShield.org)

DShield.org is an organization that facilitates information collection by providing a method for submitting firewall logs into a database where the information can be tracked and queried. The identities of destination IPs and hosts are protected and information is not shared with third parties. DShield.org allows this information to be summarized to produce various reports and summaries, such as the

- top 10 offending IPs or hosts
- top 10 most probed ports
- lists of ports that sites might want to block

Participants can register or can submit logs anonymously. Logs are submitted using prewritten programs available from the DShield.org site, by using third party programs that are configured to submit logs to DShield.org, or by using programs participants have written themselves. They can also be submitted via a web interface at the site or via email. DShield.org is sponsored by the SANS Institute [DShield 03].

Anyone submitting logs and data should ensure that the information has been appropriately sanitized or is submitted in a secure manner.

For more information see:
<http://www.dshield.org/>

3.10.3.4 Incidents.org

Incidents.org is another organization sponsored by the SANS Institute. Their purpose, according to their web site, is to monitor the current threats to the Internet. This is done through the collection of intrusion detection and firewall data from volunteers around the globe. Instructions for participating are given at the site. Participants receive special client software to use to submit data. There is an analyst on duty who monitors the data for anomalies and threats. Other resources available are a mailing list and a "Handlers Diary" that analyzes the current data collected and provides security resources and technical tips [Incidents 03].

Anyone submitting logs and data should ensure that the information has been appropriately sanitized or is submitted in a secure manner.

For more information see:
<http://www.incidents.org/>
<http://www.incidents.org/faq/>

3.10.4 Tools

There are really very few tools that have been specifically created for incident response and incident handling except for some of the products mentioned in the incident data collection section above and customized tools created by CSIRTs themselves.

Many of the tools that are used by CSIRTs are also tools used by system and network administrators. Various organizations have created tool archives that provide access to or review of security and incident response tools. One of those projects is described below.

3.10.4.1 Clearinghouse for Incident Handling Tools (CHIHT)

Through the TERENA TF-CSIRT, a project and site has been established to serve as a clearinghouse for incident handling tools. The tools listed are based on the experience and usage of various European CSIRTs. The tools are listed for other teams to review and not as recommendations for use. The tools are categorized in the following manner [CHIHT 03]:

- evidence gathering tools
  - examining media
  - examining systems and processes
- evidence investigation tools
  - analyzing evidence
  - checking identities and contacts
- system recovery tools
- CSIRT procedures
  - incident tracking and reporting
  - incident archives
  - communications
- remote access tools
  - remote network access
  - secure dial-up access
  - secure tunnels
- proactive tools
  - network auditing
  - host auditing
  - security management
  - network monitoring and traffic analysis
  - network intrusion detection

For more information see:
<http://chiht.dfn-cert.de/>

3.10.5 Research

CSIRTs and security experts are always looking to understand the intruder community better to help teams and sites proactively protect their systems, networks, and critical assets. With the computer security and incident response discipline still being relatively new, there are different research projects currently in progress related to learning more about securing networks and systems and also about effective incident handling. The following is one project in progress.

3.10.5.1 The Honeynet Project

The Honeynet Project is a non-profit research group composed of volunteers from the security field who are interested in researching tools, techniques, and activities of the intruder community through the use of a Honeynet [Honeynet 03].

A Honeynet is essentially a network of systems deployed in a controlled environment that can be watched and monitored for attacks and intruder activity. By watching attacks and probes against the system or by monitoring how the system is compromised and used to attack others, the system owners can learn about the techniques and tools used by the intruder community. This information can then be used to improve the knowledge and understanding of other computer security professionals.

The Honeynet Project is now in the third of four phases. The first phase provided a proof of concept and provided the opportunity to capture and study attacks. The second phase was to improve the methodology for the implementation, infrastructure, and deployment of a Honeynet. The third phase, starting in 2003, is to develop a bootable CD that will allow participants to easily deploy a standardized Honeynet. The fourth phase will be to develop a system to automatically collect and synthesize data from the various Honeynet research projects. The main purposes of the project are to raise awareness, teach and inform, and do research.

For more information see:
<http://www.honeynet.org/>

3.11 Current Problems

Problems and challenges faced by CSIRTs that are commonly mentioned in classes, conferences, or other discussion venues include

- lack of funding
- lack of management support
- lack of trained incident handling staff

- lack of clearly defined mission and authority
- lack of coordination mechanisms

These issues were echoed by those participating in the CSIRT Organizational Survey when asked about what are the biggest challenges facing their CSIRT. There was not one specific challenge that was consistently listed or more frequently listed by the participating teams. There was also not one particular type of challenge seen more by CSIRTs in any one sector or any category or type of CSIRT. Survey results related to challenges faced by CSIRTs are shown in Table 14.

Table 14: Challenges Faced by CSIRTs

Challenge	Percentage of Respondents
rapid growth of incident volume and workloads (including massive virus and worm incidents)	14%
needing more budget and/or resources	14%
getting and retaining good staff	14%
management's and business managers' attitude about security, and the difficulty in convincing them of the need for secure practices and response procedures	10%
issues relating to the coordination and collaboration between units, CSIRTs, and sites	10%
getting more projects and work as they got better at their job was a challenge since the workload kept growing	7%
collection and dissemination of information and follow-up from sites	7%
defining the role or authority of the CSIRT	7%

Other challenges cited included

- under-reporting and covering up of incidents by customers
- skill and knowledge at customer sites
- difficulty in prioritizing who gets what assistance
- difficulty in telling administrators what to do
- space issues
- setting up the CSIRT

3.12 Resources

3.12.1 Case Study Examples

Many of the books listed in our bibliography contain case studies. Some of the information provided by the authors is based on their own incident handling experiences or comes from discussions with victims who have reported or suffered computer security incidents.

In *Hacker's Challenge*, [Schiffman 01] the author devotes the entire book to analyzing 20 case study "war stories" that test a reader's incident response skills by providing a description of pertinent information relating to the case study. The book contains the solutions to each scenario, providing detailed descriptions of the analyses performed, excerpts of logs and screen captures, and suggestions on response/mitigation strategies.

Other books referenced in this report [Mandia 01, Schultz 01, van Wyk 01] also include example scenarios or case study reports, some containing examples of packet-level captures. Mandia devotes several chapters to specific investigative processes including forensics, tracking and tracing, network surveillance techniques, and response suggestions for platform-specific/application-specific analysis of attacks. Threaded throughout are anecdotes, tips and suggestions, and resources for additional information.

Many of the publications reviewed provide an overview of various tools that have been used in incident handling, including how they operate and what information is obtained by their use; some references include screen captures of the tools as well, illustrating what they look like.

It's also worth noting that some of the books published several years ago [Frisch 95, Garfinkel 91] (books that are probably still on some incident handlers' bookshelves) discuss techniques for investigating incidents or breaches and provide guidance on examining systems—even though they weren't discussed in terms of "forensics" investigations. Some of these techniques are still in use today in reviewing and analyzing data on systems.

3.12.2 Sample Templates, Checklists, Process Guides, Flowcharts

One of the benefits of seeing more information become available to the CSIRT community is the development of a variety of different templates, checklists, guidelines, and flowcharts that are available for review. Having access to such resources can help a new CSIRT in its planning and implementation, providing opportunities to leverage other work that has been successfully implemented as a best practice in parts of the CSIRT community. These types of resources can also provide a way for existing teams to benchmark their procedures and forms

against what others are doing. Appendix E contains copies of some incident reporting forms, which are included with the permission of the author or owner of the material.

As we reviewed the literature, we found that there are similarities in some of the forms and documents that have been developed. For example, as might be expected, the flowcharts illustrated in Mandia [Mandia 01, p. 18] and Nebraska [Nebraska 02] have many similar components, including pre-incident preparation, detection, and decision points for determining the next steps in the process (such as confirming an incident, formulating a response strategy, notifying and/or coordinating with contacts, documenting, and restoring operations). In addition, steps for investigative activities (forensics duplication, network monitoring, etc.) are steps included in the flow diagrams. Other forms and documents contain similarities in the type of information that is collected—what we refer to as the "critical information" that is needed regarding an event that has been reported to the CSIRT. This includes relevant contact information, hostnames, IP addresses, OS versions/patch levels, chronology documenting the activity, and actions for response and follow up.

In Section 3.7.2, "Having a Plan," we referred to the fact that many of the documents we reviewed in the literature search included a variety of different incident response processes or steps. For example, there are copies (or online versions of) incident reporting forms included in a number of publications [DHS 03, FCC 01, Kruse 02, Navy 96, Nebraska 02, SANS 03, USSS 01]. A variety of incident reporting and response flowcharts are referenced [Mandia 01, Kruse 02, Nebraska 02, Steele 02] and process guides or checklists available [Allen 01, Swanson 02, Vermont 01].[146] Descriptions of an incident response process or methodology are included in several sources [Allen 01, SANS 03, Schultz 02, Symantec 01, West-Brown 03]. More detailed guidance on response procedures[147] can be found in some [Allen 01, Mandia, 01, SANS 03, Schiffman 01].

---

146 While the *CERT Guide to System and Network Security Practices* [Allen 01] and the *NIST Contingency Planning Guide for Information Technology Systems* [Swanson 02] are targeted at system and network administrators or other IT professionals, the processes and practices are applicable in many areas of CSIRT work and may be worth reviewing.

147 Response procedures are the specific steps recommended for protecting systems, detecting and responding to intrusions, and returning systems to normal operations.

4 Summary

Our examination of the literature identified a few broad-based observations that will be of interest to new and existing CSIRTs. This information can be used to further increase their overall knowledge and understanding of incident handling, team responsibilities, team composition, techniques and procedures, and policy issues.

- There is a growing base of anecdotal and case study information appearing in print about not only the formation and organization of CSIRTs, but also the general types of activities these teams undertake and how they perform them.
- More information is available about the management and costs related to building and operating incident response teams.
- There are some common functional processes for performing incident handling activities in a CSIRT. Even if these processes are grouped somewhat differently in the articles and publications discussed in this technical report, the basic processes revolve around the following tasks: prepare/protect, detect, respond, improve. See Section 3.7.7 for more detailed information.
- There are many similarities in CSIRT processes; however, in the day-to-day operations of a CSIRT, the way in which these processes are implemented and the depth and breadth of the services that are provided may be very different.

Based on (*a*) our collective experience, (*b*) the reviewed literature, web sites, and CSIRT project information, and (*c*) the collected survey data, we see the current state of the practice for CSIRTs as follows:

- All evidence points to a large growth in the number of incident response teams over the past four to five years. This growth has primarily taken place in the commercial sector. Growth in education and government teams has also continued. Others seeking to create CSIRTs include organizations in critical infrastructures such as the finance/banking and power/energy sectors. Globally we are seeing more interest in implementing CSIRTs, especially national and local government teams.:
- The reasons for the growth in teams include (*a*) the increase in the number of security incidents and the recognition of a need for a planned response, (*b*) new legal requirements, and (*c*) the current view that computer security must be proactive to be successful; being reactive is no longer sufficient.
- Incident handling and incident response teams are still relatively new areas in computer security, and incident response is still an immature field. Because of this there are few

standards for incident handling methodologies or processes that are widely adopted, although there are many projects currently in progress that are attempting to gain acceptance and establish some standard mechanisms.

- Because of the newness of this field there is also no consistent structure or set of services for a CSIRT. The nature of incident response makes it imperative that a team match the goals and objectives of its constituency or parent organization. This means the services offered and the structure of the CSIRT must be set up to support those being served. The majority of teams do, however, offer some form of incident handling, development of security policies, and development of alerts and advisories.
- There is no commonly used taxonomy for incident response and computer security terminology. This can cause confusion when teams share data that has the same classification name, but which may represent different things.
- Employees who are trained and experienced in incident response techniques and practices are difficult to find.
- No established education path for CSIRT professionals exists as of today. Many incident handling activities have evolved out of traditional system, network, and security administration. Various training courses, as well as mentoring by experienced CSIRT members, is what is currently available today to help educate incident handling staff. There are also certification programs, but none has been adopted as a standard.
- There is a lack of publicly available sample templates for policies and procedures for use in the day-to-day operations of a CSIRT.
- Few tools such as tailored help desks or trouble ticket solutions addressing the specific needs of CSIRTs—authenticity and confidentiality, as well as workflows—are readily available.

It has also been observed that CSIRT best practices do not currently exist in the following areas:

- standards for interfaces—a team's location within the organization, with whom they interact (internally and externally), what is reported, how that occurs, etc.
- data management—how teams manage, access, archive, and share their CSIRT data
- professional standards—the formal or official specification for what a CSIRT comprises and the staff who perform the work

In the CSIRT community as a whole, there is general agreement that standards are needed and that some minimal support is needed for automating incident tracking, response, and analysis.[148]

There are various projects and discussions currently under way that address many of these issues. Critical and relevant discussions include

- incident data exchange: how to develop and utilize a common and easy-to-use mechanism to allow sharing of data between teams and synthesis of collected data
- trusted introducers: what type of mechanisms are needed to help identify and verify teams
- operational coordination: what types of mechanisms for incident handling coordination between various geographic areas and groups of CSIRTs in order to quickly control and contain incident activity, share expertise, analysis, and data, and then effect a coordinated response
- formalization of procedures and formats: what types of standards are appropriate and can be applied to teams. Various standards are currently being sought by the community in all areas, from common incident tracking systems to advisory preparation and data collection and exchange.
- requirements for establishing a CSIRT capability: Teams are looking for methods to evaluate their effectiveness. They want to baseline their operations and services against a set of basic requirements and best practices.
- vulnerability disclosure: How, when, and to what extent to disclose vulnerability information has been a highly volatile topic in the incident response and computer security community. Various discussions are underway to determine if there can be any agreed-upon standards or processes in this area.
- certification and training: What types of training and certification should a member of an incident handling team should be required to have? Many teams are struggling with these issues today, along with the fact that just finding skilled incident handlers is not an easy task.

As previously mentioned throughout this report, each of the above depends on a variety of factors, such as the mission or role of the CSIRT and its constituency, along with its organizational structure, funding, and staffing. Because of this, it may not be possible to set standards that every CSIRT would be able to follow. In a general sense, however, some "best practices" should be possible across many CSIRTs—even if the specific implementation for how the practice is performed is different. For example, from our observations and experience, we can generally agree that, to be effective, CSIRTs require the following:

---

[148] An example of standards development is the IODEF activity in the IETF INCH Working Group, which strives to define a common data format for sharing incident handling data between different CSIRTs.

- management support and trust from their constituency
- a plan in place for handling incidents when they occur
- established relationships with a variety of others as appropriate (e.g., constituent members, other CSIRTs, management, law enforcement)
- capable staff who are well trained and knowledgeable in the activities being handled by the team to provide effective response
- a consistent and repeatable process for CSIRT operations in receiving, accessing, and archiving data (including sharing information as appropriate)

5 Future Work

Based on the information collected in this State of the Practice of CSIRTs report, we believe the following areas of work are prime candidates for future development:

- State of the practice survey—continue collection of data with a new and updated survey that can be used to feed information into CSIRT best practice development
- CSIRT best practices—development of a series of best practice recommendations on CSIRT operations based on the current information collected and continued research
- CSIRT criteria—for developing teams, determining staffing skills, and determining team effectiveness
- CSIRT process guidelines—for offering various services

As a starting point, included below is a list of suggested topic areas where we see the need for more discussion or for more specific resources and guidelines to be developed. In many of these areas, work has already begun, or a prototype may even exist that can be used as a basis for further development.

- a new taxonomy specifically for CSIRT processes, incident data, and incident activity that can be accepted throughout the CSIRT community, perhaps through the development of an RFC
- agreed-upon criteria for what constitutes a CSIRT, including different types of teams
- a mechanism or mechanisms to identify and validate teams
- more formalized resources to help new teams, including sample forms, checklists, and templates for CSIRT processes and operations
- tools customized specifically for incident response work
- models for estimating the cost and size of a CSIRT based on sector and services offered:
- guidelines on the services and processes needed for different CSIRT models and CSIRTs in different sectors
- guidelines and references to cyber crime laws and legal issues (on a country basis) for incident handlers
- use of certification criteria to develop new incident handler training and mentoring programs or enhance existing ones

We are seeking opportunities to collaborate with others in the CSIRT community who are interested in working on these types of issues with us. This collaboration can occur at a variety of different levels: provision of information, joint development of white papers and criteria, or even funding some of the needed research and resulting outputs related to these areas. If you are interested in collaborating with us, please contact csirt-info@cert.org.

6 Closing Remarks

This document discusses a wide variety of issues within the practice of establishing and operating a CSIRT. Although many topics were discussed, we realize that the first edition of this technical report could not be a comprehensive, inclusive look at that state of the practice of CSIRTs. But it is an initial attempt to begin to collect information on the history, practice, structure, services, and challenges of CSIRTs.

There is much more information other teams could have contributed to this body of work, but it was not possible to talk or interact with every team. To that end we would like to get your feedback on this technical document: did it meet your expectations, was it helpful, what was missing, and what was beneficial? We would welcome any data you have collected regarding the issues addressed in this document that you are able and willing to share. We would also welcome hearing about any best practices, case studies, success stories, or other experiences that you or your team may have in creating and operating a CSIRT and that we could incorporate into future editions.

Please feel free to contact us at csirt-info@cert.org.

If you are interested in reading more about CSIRT development and operations, a good place to start is the newly revised *Handbook for CSIRTs*, which is available on the CERT web site at <http://www.cert.org/archive/pdf/csirt-handbook.pdf>. You can also find many interesting and helpful articles in the bibliography attached to this document.

If you are interested in learning more about CSIRTs and processes and best practices for incident handling, you may want to attend one of our CSIRT courses. You can find course information and schedules at <http://www.cert.org/nav/index_gold.html>.

Once again we would like to thank everyone who helped us in the creation and production of this document. Without your support, we would not have been able to publish this state of the practice.

Appendix A CSIRT Organizational Survey

CSIRT Information:

CSIRT Name: _____

CSIRT Parent Organization: _____

CSIRT Contact Phone Number: _____

CSIRT Contact Email: _____

CSIRT Address: _____

_____

_____

_____

Your Contact Information:

Name of person filling out survey: _____

Position or title of person filling out survey: _____

CSIRT Background

1. How long has your CSIRT been in operation? _____
2. Does your CSIRT have a defined constituency?
   a. __ Yes
   b. __ No

3. If yes, who is that constituency: _____

_____

4. What is the mission of your CSIRT: _____

_____

_____

_____

_____

_____

_____

_____

5. Where is the CSIRT located within your organizational structure?

   a. __ Information Technology (IT) Department or Telecommunications Department

   b. __ Audit Department

   c. __ Security Department

   d. __ CSIRT is its own department

   e. __ Other: _____

   f. __ Not Applicable (the CSIRT is not within any department but a separate organization or coordination center)

6. To whom does your CSIRT report?

   a. __ Chief Information Officer (CIO)

   b. __ Chief Security Officer (CSO)

   c. __ Manager of IT or Telecommunications

   d. __ CSIRT Manager is the top level of the organization

   e. __ Other: _____

7. In what sector is your CSIRT located?

   a. __ Military

   b. __ Education

   c. __ Information and Communication

   d. __ Electric Power

   e. __ Oil and Gas

   f. __ Water Supply

   g. __ Government Law Enforcement Services

   h. __ Government Fire and Rescue Services

   i. __ Government and Public Administration

   j. __ Transportation

   k. __ Banking and Finance

   l. __ Public Health Services

   m. __ Professional Services

   n. __ Other Commercial Organization

   o. __ Other Non-Profit Organization

   p. __ Other: _____

8. In what country is your CSIRT located? _____

9. Do you have parts of your CSIRT in other countries?

   a. __ Yes

   b. __ No

10. If Yes, how many countries? _____

CSIRT Organization

11. What categories best describe your CSIRT? (Check all that apply.)

   a. __ Ad hoc team (team is called together only when an incident occurs)

b. __ Distributed dedicated team (team is scattered across locations and performs CSIRT work 100%)

c. __ Distributed part-time team (team is scattered across locations and performs CSIRT work part-time)

d. __ Centralized dedicated team (team is in one location and performs CSIRT work 100%)

e. __ Centralized coordination center (team is in one location and coordinates information and incident response between other CSIRTs)

f. __ Combined team (there is a central team and a distributed team)

g. __ Analysis Center (team performs analysis of incident trends and patterns 100%)

h. __ Vendor team (team handles reports of vulnerabilities in their parent organization's software or hardware products)

i. __ Managed Security Services Provider/Incident Response Provider (team provides incident response as a for-fee service)

12. What authority does your CSIRT have? (Check only one.)

a. __ No authority (can influence only)

b. __ Full authority for our constituency (can issue mandates and take systems off the network)

c. __ Partial authority (included in the constituency decision-making process regarding how to respond to an incident)

d. __ Authority is different for various services. Please provide some explanation for differences in authority:

_____

_____

_____

13. How is your CSIRT funded? (Check all that apply.)

a. __ Government funding

b. __ Each service has a fee attached

c. __ Parent organization funding

d. __ Subscriptions

e. __ Research consortium

f. __ Other: _____

14. How many people work full-time (100% of their time) on your CSIRT? _____

15. How many people work part-time (less than 100% of their time) on your CSIRT? _____

    For these part-time workers, please estimate the equivalent number of full-time staff that would account for their effort: _____

16. Do you have a formal training or mentoring program for your CSIRT staff?

    a. ___Yes

    b. ___No

17. What degrees or certifications, if any, do you require for CSIRT staff?

    _____

18. What is your approximate CSIRT budget (including salary costs)?

    a. __ Under $50,000 USD

    b. __ Between $50,000 and $100,000 USD

    c. __ Between $100,000 and $500,000 USD

    d. __ Between $500,000 and $1,000,000 USD

    e. __ Between $1,000,000 and $2,500,000 USD

    f. __ Between $2,500,000 and $5,000,000 USD

    g. __ Above $5,000,000 USD

CSIRT Operations

19. What services does your CSIRT provide? (Check all that apply.)

    a. __ incident handling/response

    b. __ analyzing vulnerabilities in hardware and software

    c. __ analyzing exploits, toolkits, intruder logs and files (artifacts)

    d. __ handling virus reports/incidents

e. __ answering hotline/help desk calls

f. __ monitoring intrusion detection systems

g. __ monitoring network and system logs such as firewalls, routers, mail servers, etc.

h. __ monitoring public security information sites and mailing lists

i. __ publishing advisories and alerts

j. __ publishing technical documents

k. __ penetration testing of constituent systems

l. __ vulnerability scanning of constituent systems and networks

m. __ vulnerability assessments of constituent systems and networks

n. __ security policy development

o. __ developing security product (creating your own patches, incident response or security tools)

p. __ administering security configurations for constituent systems

q. __ constituency training or security awareness

r. __ computer forensics evidence collection

s. __ tracking and tracing intruders

t. __ pursuing legal or law enforcement investigations

20. How do you record and track incident information? (Check all that apply.)

a. __ Paper log book or forms

b. __ Database

c. __ Other: _____

21. If you use a database, what type of product does your CSIRT use?

a. __ Off-the-shelf database. Product: _____

b. __ CSIRT created or customized database

22. Do you provide incident reporting guidelines in hardcopy or electronic form to your constituency?

    a. Yes ____

    b. No ____

23. How do you receive incident reports? (Check all that apply.)

    a. __ Phone

    b. __ Email

    c. __ Paper Incident Reporting Form

    d. __ Web Incident Reporting Form

    e. __ Intrusion Detection Systems

    f. __ Walk-in

    g. __ Other: _____

24. How does your CSIRT provide incident response? (Check all that apply.)

    a. __ Provide recommendations and guidelines only via phone or email

    b. __ Repair and recover affected systems and networks

    c. __ Develop and distribute technical documents and alerts

    d. __ We do not provide a response; we pass incidents to another area to be handled

       To whom are they passed? _____

    e. __ Other: _____

25. If you have a CSIRT hotline or help desk, who answers the phone?

	During Business Hours	After Hours	
a.	_____	____	CSIRT staff
b.	_____	____	IT help desk staff
c.	_____	____	Message center
d.	_____	____	Other: _____

26. What are your business hours? _____

27. Who recovers and rebuilds systems involved in computer security incidents?

    a. __ The CSIRT

    b. __ IT Department/system and network administrators

    c. __ Both

    d. __ Other: _____

28. On average, how many incidents does your team handle per day? _____

29. On average, how many incidents does your team handle per year? _____

30. Please indicate how often you deal with the following types of incident reports:

	Very Frequently	Somewhat Frequently	Not Frequently	Never
a. Viruses, Worms, or Trojan Horse Programs	_____	_____	_____	_____
b. Denial of Service	_____	_____	_____	_____
c. Privileged compromise (root or administrator level compromise)	_____	_____	_____	_____
d. User-level compromise	_____	_____	_____	_____
e. Theft of data	_____	_____	_____	_____
f. Unauthorized access to data	_____	_____	_____	_____
g. Misuse of resources	_____	_____	_____	_____
h. Probes and scans	_____	_____	_____	_____
i. Other: _____	_____	_____	_____	_____

31. What type of mechanisms does your CSIRT use to communicate securely with your constituency? (Check all that apply.)

    a. __ PGP

    b. __ Digital certificates

c. __ Secure phones or fax

d. __ Secure intranet or extranet

e. __ Do not have secure communications capability

f. __ Other: _____

32. With whom does your CSIRT coordinate their response activities? (Check all that apply.)

a. __ Chief Information Officer (CIO) or Chief Security Officer (CSO)

b. __ Internal business managers

c. __ Human Resources Department

d. __ Physical Security Department

e. __ Audit or Risk Management Department

f. __ IT or Telecommunications Department

g. __ Legal Department

h. __ Public Relations Department

i. __ Marketing Department

j. __ Law Enforcement

k. __ Other CSIRTs

l. __ CERT/CC

m. __ Other security experts

n. __ Others: _____

o. __ We do not coordinate with any other units or organizations.

33. With whom does your CSIRT share information? (Check all that apply.)

a. __ Chief Information Officer (CIO) or Chief Security Officer (CSO)

b. __ Internal business managers

c. __ Human Resources Department

d. __ Physical Security Department

e. __ Audit or Risk Management Department

f. __ IT or Telecommunications Department

g. __ Legal Department

h. __ Public Relations Department

i. __ Marketing Department

j. __ Law Enforcement

k. __ Non-Military Government Organizations (City, State, Country, Region)

l. __ Military Organizations

m. __ Other CSIRTs

n. __ CERT/CC

o. __ Other security experts

p. __ Information Sharing Analysis Centers (ISACs)

q. __ Others: _____

r. __ We do not share information with any other units or organizations.

34. May we call you if we need to follow-up on your answers in more detail?

a. __ Yes (Best time to call: _____)

b. __ No

THANK YOU FOR YOUR TIME AND EFFORT! – The CSIRT Development Team, CERT/CC

Appendix B: Comparison of Incident Response Steps and Processes

Type and Title of Publication	Author(s)	Step or Process	Material Covered and/or Other Comments
Books			
CERT Guide to System and Network Security Practices	Julia Allen [Allen 01]	Analyze information Communicate Collect and protect information Contain Eliminate all means of intruder access Return systems to normal operations Implement lessons learned	For comparison with the other references in this table, the "response" steps have been identified. This is a resource book for system/network administrators to harden/secure systems; prepare for, detect, and respond to security events and activity; and improve security configurations and procedures.
Computer Forensics, Incident Response Essentials	Warren G. Kruse II and Jay G. Heiser [Kruse 02]	Discovery and Report Incident Confirmation Investigation Recovery Lessons Learned/ Recommendations	Technical, focusing on the investigation process (not on the incident response issues team management perspective)
Incident Response	Kenneth R. van Wyk and Richard Forno [van Wyk 01]	Identification Coordination Mitigation Investigation Education	Written for management interested in building a team and issues that will need to be faced. Also focuses on responding to incidents and gives technical references/coverage of tools of the trade, typical attacks, etc.
Incident Response: A Strategic Guide to Handling System and Network Security Breaches	Eugene Schultz and Russell Shumway [Schultz 02]	Preparation Detection Containment Eradication Recovery Follow-up	Information relating to the forming, managing, and operating of a team. Good discussion of some of the issues that will be faced by team leads.
Incident Response: Investigating Computer	Kevin Mandia and Chris Prosise [Mandia 01]	Pre-incident preparation Detection Initial response	The primary focus of the book is on investigation and specific techniques that can be used for investi-

Type and Title of Publication	Author(s)	Step or Process	Material Covered and/or Other Comments
Crime		Response strategy formulation Duplication (forensic backup) Investigation Security measure implementation Network monitoring Recovery Reporting Follow-up	gating various types of incidents.
System Security: A Management Perspective	David L. Oppenheimer, David A. Wagner, and Michele D. Crabb [Oppenheimer 97]	Isolate Identify Contain Terminate Eradicate Recover Perform follow-up	Short topics booklet that describes security issues at a high level for management
Articles/Guides/White Papers/Special Publications			
Advance Planning for Incident Response and Forensics	Symantec Corp. [Riptech 01]	Identify vital assets Hire experienced staff Secure individual hosts Secure your network Monitor devices Establish a response strategy Establish policies and procedures	Overview of topic areas. Provides incident managing services
Computer Security Incident Handling Step by Step	The SANS Institute [SANS 03]	Preparation Identification Containment Eradication Recovery Follow-up	Good reference guide, covered at high level. Outlines the list of actions to be taken at each of the six steps listed.
Information Systems Security Incident Response	IA Newsletter, Gordon Steele http://iac.dtic.mil/iatac/resources/related_sites.htm [Steele 02]	References the SANS list	High-level overview of incident response, planning, and management (similar to work covered by SANS, Howard).

Type and Title of Publication	Author(s)	Step or Process	Material Covered and/or Other Comments
NIST Special Publication 800-34 Contingency Planning Guide for Information Technology Systems	Marianne Swanson, Amy Wohl, Lucinda Pope, Tim Grance, Joan Hash, Ray Thomas [Swanson 02]	Protect Sustain Recover/resume	Although focused at IT contingency planning, does contain some references to managing incidents.
Security Architecture and Incident Management for E-business	Internet Security Systems Marc S. Sokol and David A. Curry [Sokol 00]	Incident preparedness Alerting Report and notification Preliminary investigation Decision and resource Allocation Response Recovery Lesson learned	Provides a high-level overview of the IH process.
Securing Information Assets: Planning, Prevention and Response	CIO Focus Guide, CXO Media [CXO 03]	Detect Analyze Contain/eradicate Provide workarounds/ fixes Prevent reinfection Log events Preserve evidence Conduct postmortem/ apply lessons learned	Provides examples of case studies, short reference guides, and checklists. Very high-level senior executive reading material.
Other Documents/Presentations			
Computer Security Incident Response Planning	Internet Security Systems [ISS 01]	Alert Triage Response Recovery Maintenance	Describes "phases" of incident response, once an incident is declared.
Responding to Computer Security Incidents: Guidelines for Incident Handling	E. Eugene Schultz, Jr., David S. Brown, Thomas A. Longstaff [Schultz 90]	Protection Identification Containment Eradication Recovery Follow-up	Although an early work (1990), contains similar information about incident handling issues. Also contains specific guidelines for responding to (these early) incidents, viruses, worm attacks. Some discussion of vulnerability issues (mostly focused on UNIX, VMS, etc.) and some information about early tools that were available to assist the incident handling process.
The Methodology of Incident Handling	Matthew McGlashan, Australian Computer	Identify scope and assess damage Communicate	High level; slide presentation

Type and Title of Publication	Author(s)	Step or Process	Material Covered and/or Other Comments
	Emergency Response Team [McGlashan 01]	Collect and protect Apply short-term solutions Eliminate intruder access Return to normal operations Identify and implement lessons learned	
Security Architecture and Incident Management for E-business	Internet Security Systems [Sokol 00]	Incident preparedness Alerting Report and notification Preliminary investigation Decision and resource allocation Response Recovery Lessons learned	Provides a high-level overview of best practices for the development of an incident response process.
Incident Response and Reporting Procedure for State Government	State of Nebraska [Nebraska 02]	Detect the incident Analyze the incident Contain or eradicate the problem Provide workarounds or fixes Prevent re-infection Log events Preserve evidence Conduct a postmortem/ apply lessons learned	A draft report summarizing the guidelines for CIO Cyberthreat Response and reporting (applicable to non-education state agencies, boards, and commissions receiving appropriation from the state Legislature, or state agencies that have direct connection to the state's network.
State of Vermont Incident Handling Procedure	State of Vermont [Vermont 01]	Protect Identify Contain Eradicate Recover Follow-up	An interim guideline for incident response within the State of Vermont.
RFC 2196 Site Security Handbook	Barbara Fraser, Editor [Fraser 97]	Notification & exchange of information Protect evidence and activity logs Containment Eradication Recovery Follow-up	Revised version of RFC 1244. Provides practical guidance for administrators on developing computer security policies and procedures.

Type and Title of Publication	Author(s)	Step or Process	Material Covered and/or Other Comments
Computer Incident Response Guide-book	Naval Command, Control and Ocean Surveil-lance Center [Navy 96]	Preparation Identification Containment Eradication Recovery Follow-up	Training module for the INFOSEC, developed in 1996. Provides brief high-level guidance and procedures for responding to incidents.

Appendix C: Training Sources for CSIRTs

The following list is a small sample of training sources for CSIRTs and incident handling. Many of these, and other sources, also provide training in related areas of computer forensics or information security. This is not a comprehensive list. Search the web, or follow the links from some of the sites below, to find other sources for relevant training for CSIRTs.

Incident Response Training

@stake – <http://www.atstake.com/>

@stake Academy
<http://www.atstake.com/services/education/>
Lecture and lab courses, including Incident Response and Forensic Readiness

Backbone Security – <http://www.backbonesecurity.com/>

Training
<http://www.backbonesecurity.com/training/>
Attack Postmortem

CERT Coordination Center – <http://www.cert.org>

CERT Training
<http://www.cert.org/nav/index_gold.html>

CSIRT Development
<http://www.cert.org/csirts/>
Courses include Creating a CSIRT, Overview of Managing CSIRTs, Managing CSIRTs, Fundamentals of Incident Handling, and Advanced Incident Handling for Technical Staff

Computer Security Institute (CSI) – <http://www.gocsi.com/>

Annual Conference
<http://www.gocsi.com/annual/>
Conference sessions include Response Teams

CSI Training
<http://www.gocsi.com/training/>

CSI Information Security Seminars
<http://www.gocsi.com/infosec/wkshop.html>

Seminars include Intrusion Detection, Attacks, and Countermeasures and Practical Forensics: How to Manage IT Investigations

Forum of Incident Response and Security Teams (FIRST) – <http://www.first.org/>
FIRST Conferences
<http://www.first.org/conference/>

Foundstone – <http://www.foundstone.com/>
Education
<http://www.foundstone.com/education/>
Courses include Ultimate Hacking, Ultimate Web Hacking, and Ultimate Hacking: Incident Response/Forensics

Global Knowledge – <http://www.globalknowledge.com/>
Course Catalog
<http://www.globalknowledge.com/training/training.asp>
Includes classroom learning, virtual classroom e-learning, and self-paced e-learning

Course Catalog – Security
<http://www.globalknowledge.com/training/category.asp?catid=191>
Courses include Intrusion Detection and Forensics, Network Security, Wireless Security, and others

Free Web Seminars
<http://www.globalknowledge.com/training/category.asp?catid=248>
Various topics

LionTech IT Ltd. – <http://www.liontech-it.com/>
IT Training
<http://www.liontech-it.com/training/>
Courses and seminars, including Ethical Hacking/Penetrating Testing

Megamind, Institute for Advanced Technology Training – <http://www.megamind.org/>
Security Training
<http://www.megamind.org/INFO/ptrain.html#ir>
Courses include Incident Response and Intrusion Detection

MIS Training Institute – <http://www.misti.com/>

InfoSecurity Seminars, Conferences, Symposia, Briefings
<http://www.misti.com/northamerica.asp?page=1&subpage=0>

Incident Response
<http://www.misti.com/northamerica.asp?disp=evfnd&srch=incident%20response>

MIS Training Institute Online
<http://www.misti-online.com/>
Courses include Information Security courses

New Technologies Inc. (NTI) – <http://www.forensics-intl.com/>
Computer Forensics and Security Training
<http://www.forensics-intl.com/training.html>

PRESECURE – <http://www.pre-secure.com/>
Incident Response Teams Development and Training
<http://www.pre-secure.com/ir/courses/>

Red Siren – <http://www.redsiren.com/>
Information Security University
<http://www.redsiren.com/infosecu.htm>
<http://www.redsiren.com/infosecu/>
Online learning courses, including Incident Response and Introduction to Computer Investigations

SysAdmin, Audit, Network, Security (SANS) Institute – <http://www.sans.org/>
Computer Security Education and Information Security Training

SANS Online Training
<http://www.sans.org/onlinetraining/>
Courses include Hacker Techniques, Exploits, and Incident Handling

SANS Webcasts
<http://www.sans.org/webcasts/>
various topics

TheTrainingCo. – <http://www.thetrainingco.com/>
Techno-Security Seminars
<http://www.thetrainingco.com/html/TechnoBriefings.html>

Training of Network Security Incident Teams Staff (TRANSITS) – <http://www.ist-transits.org/>
TRANSITS is a three-year European project to provide Training of Network Security Incident Teams Staff. Organized by TERENA[149] and UKERNA,[150] and funded by the European Commission, TRANSITS will provide public domain CSIRT training course materials and will present CSIRT training workshops over various regions in Europe.

---

149 Trans-European Research and Education Networking Associations (TERENA) - <http://www.terena.nl/>

150 United Kingdom Education & Research Networking Association (UKERNA) - <http://www.ukerna.ac.uk/>

TRANSITS Training Workshop
<http://www.ist-transits.org/events.php>
Participation is limited, accepting only selected applicants.

General Information Security/Assurance

Higher Education – Colleges and Universities

National Security Agency (NSA) - National INFOSEC Education & Training Program – <http://www.nsa.gov/isso/programs/nietp/index.htm>

Centers of Academic Excellence in Information Assurance Education - <http://www.nsa.gov/isso/programs/coeiae/index.htm>

Announcement – <http://www.nsa.gov/isso/programs/nietp/newspg1.htm>
NSA Designates Centers of Academic Excellence in Information Assurance Education. Fifty universities have been designated as Centers of Academic Excellence in Information Assurance under the program:

Universities in the United States noted for their information security programs

Air Force Institute of Technology – <http://www.afit.edu/>
Auburn University – <http://www.eng.auburn.edu/users/hamilton/security/>
Capitol College – <http://www.capitol-college.edu/academics/grad/msns2.html>
Carnegie Mellon University – <http://www.heinz.cmu.edu/infosecurity/>
Drexel University – <http://www.ece.drexel.edu/>
East Stroudsburg University – <http://www.esu.edu/cpsc/courses/scsebs_req.htm>
Florida State University – <http://www.cs.fsu.edu/infosec/>
George Mason University – <http://www.isse.gmu.edu/~csis/>
George Washington University – <http://www.seas.gwu.edu/~infosec/>
Georgia Institute of Technology – <http://www.cc.gatech.edu/>
Idaho State University – <http://security.isu.edu/>
Indiana University of Pennsylvania – <http://www.iup.edu/>
Information Resources Management College of the National Defense University – <http://www.ndu.edu/irmc/>
Iowa State University – <http://www.issl.org/>
James Madison University – <http://www.infosec.jmu.edu/>
John Hopkins University – <http://www.jhuisi.jhu.edu/>
Mississippi State University – <http://www.cs.msstate.edu/~security/>
Naval Postgraduate School – <http://cisr.nps.navy.mil/>
New Jersey Institute of Technology – <http://www.it.njit.edu/BSIT.htm>
New Mexico Tech – <http://www.cs.nmt.edu/>
North Carolina State University – <http://ecommerce.ncsu.edu/infosec/>
Northeastern University – <http://www.northeastern.edu/>
Norwich University – <http://www.norwich.edu/biz/cs/>
Pennsylvania State University – <http://net1.ist.psu.edu/>

Polytechnic – <http://www.poly.edu/>
Portland State University – <http://www.cs.pdx.edu/>
Purdue University – <http://www.cerias.purdue.edu/>
Stanford University – <http://crypto.stanford.edu/seclab/>
State University of New York, Buffalo – <http://www.cse.buffalo.edu/caeiae/>
State University of New York, Stony Brook – <http://www.sunysb.edu/>
Stevens Institute of Technology – <http://www.cs.stevens-tech.edu/>
Syracuse University – <http://www.csa.syr.edu/>
Texas A&M University – <http://cias.tamu.edu/>
Towson University – <http://www.towson.edu/cait/>
University of California at Davis – <http://seclab.cs.ucdavis.edu/>
University of Dallas – <http://gsmweb.udallas.edu/info_assurance/>
University of Idaho – <http://www.csds.uidaho.edu/>
University of Illinois at Urbana-Champaign – <http://ciae.cs.uiuc.edu/>
University of Maryland, Baltimore County – <http://www.cisa.umbc.edu/>
University of Maryland, University College – <http://www.umuc.edu/>
University of Massachusetts, Amherst – <http://www.cs.umass.edu/>
University of Nebraska at Omaha – <http://nucia.ist.unomaha.edu/>
University of North Carolina, Charlotte – <http://www.sis.uncc.edu/LIISP/>
University of Pennsylvania – <http://www.upenn.edu/programs/>
University of Texas, San Antonio – <http://www.utsa.edu/>
University of Tulsa – <http://www.cis.utulsa.edu/>
University of Virginia – <http://www.seas.virginia.edu/>
Walsh College – <http://www.walshcollege.edu/pages/432.asp>
U.S. Military Academy, West Point – <http://www.itoc.usma.edu/>
West Virginia University – <http://www.lcsee.cemr.wvu.edu/>

National Institute of Standards and Technology (NIST) – Computer Security Resource Center (CSRC) – <http://csrc.nist.gov/>

Training & Education
<http://csrc.nist.gov/ATE/te_full.html>
Academia Training and Education Programs
List includes most of the Centers of Academic Excellence in Information Assurance Education (above), plus other universities in other countries:

Queensland University of Technology (Australia) – Information Security Research Centre – <http://www.isrc.qut.edu.au/>

Stockholm University (Sweden) – SecLab - <http://www.dsv.su.se/research/seclab/>

University of Cambridge (UK) – Computer Security Group - <http://www.cl.cam.ac.uk/Research/Security/>

University of London (UK) – Royal Holloway – Information Security Group - <http://www.isg.rhbnc.ac.uk/>

Certification Organizations

Currently, there are few certification programs for CSIRTs. GIAC provides a certification for GIAC Certified Incident Handler (GIAH). Other certifications are available for Certified Information Systems Security Professional (CISSP) and Systems Security Certified Practitioner (SSCP). Technical certifications in other specific areas are widely available through various vendors (e.g., CISCO, Microsoft).

CERT Coordination Center – <http://www.cert.org/>
CERT®-Certified Computer Security Incident Handler
<http://www.cert.org/certification/>

Global Information Assurance Certification (GIAC) – <http://www.giac.org/>
GIAC Certified Incident Handler (GCIH)
<http://www.giac.org/GCIH.php>
<http://www.giac.org/subject_certs.php#GCIH>

Other Security Certifications

CompTIA – <http://www.comptia.org/>
CompTIA Security+ Certification
<http://www.comptia.org/certification/security/>

Global Information Assurance Certification (GIAC) – <http://www.giac.org/>
Overview of Certifications – <http://www.giac.org/certifications.php>
Individual certifications include GIAC Security Essentials Certification (GSEC), GIAC Certified Intrusion Analyst (GCIA), GIAC Certified Forensic Analyst (GCFA), and more.
GIAC Security Expert (GSE)
<http://www.giac.org/GSE.php>
<http://www.giac.org/track_cert.php>

International Information Systems Security Certifications Consortium, Inc. $(ISC)^2$ – <http://www.isc2.org/>
Certification
<http://www.isc2.org/cgi/content.cgi?category=3>
Certified Information Systems Security Professional (CISSP) and Systems Security Certified Practitioner (SSCP)

TruSecure
TruSecure ICSA Practitioner Certification
<http://www.trusecure.com/solutions/certifications/ticsa/>
TruSecure ICSA Certified Security Associate (TICSA)

Other Technical Training Resources

Learning Tree International – <http://www.learningtree.com/>

Security

<http://www.learningtree.com/direct/ilt12.htm>

Web-based training courses

MIS Training Institute – <http://www.misti.com/>

Seminars, Conferences, Symposia

"MIS offers seminars, conferences, and symposia in the areas of Information Security, Internal/IT Auditing, Networks, E-Commerce Applications, Operating Environments, and Enterprise Applications."

MIS Training Institute Online

<http://www.misti-online.com/>

Other Resources and Readings

National Institute of Standards and Technology (NIST)

Computer Security Resource Center (CSRC) – <http://csrc.nist.gov/>

Training & Education

<http://csrc.nist.gov/ATE/te_full.html>

Links to various training programs and providers

SC Magazine – <http://www.scmagazine.com/>

"Shaping Up for INFOSEC TRAINING" – July 2002 cover story

<http://www.scmagazine.com/scmagazine/2002_07/cover/cover.html>

Appendix D: Cyber Crime Law Resources

International Cyber Crime Laws

Council of Europe – <http://www.coe.int/>
Council of Europe – Legal Affairs – Treaty Office – <http://conventions.coe.int/>

Data Protection/Privacy

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (**ETS**[151] **no. 108**)
<http://conventions.coe.int/treaty/en/whatyouwant.asp?nt=108>
[Entry into force 1985-10-01]

Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and trans-border data flows (**ETS no. 181**)
<http://conventions.coe.int/treaty/en/whatyouwant.asp?nt=181>

Cyber Crime
<http://www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/cybercrime/>

Convention on Cybercrime (**ETS no. 185**)
<http://conventions.coe.int/treaty/en/whatyouwant.asp?nt=185>

This Convention defines nine offenses in four categories:

Title 1 – Offences against the confidentiality, integrity, and availability of computer data and systems
- Article 2 – Illegal access
- Article 3 – Illegal interception
- Article 4 – Data interference
- Article 5 – System interference
- Article 6 – Misuse of devices

Title 2 – Computer-related offences
- Article 7 – Computer-related forgery
- Article 8 – Computer-related fraud

Title 3 – Content-related offences
- Article 9 – Offences related to child pornography

Title 4 – Offences related to infringements of copyright and related rights

[151] European Treaty Series

Article 10 – Offences related to infringements of copyright and related rights

Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (**ETS no. 189**)
<http://conventions.coe.int/treaty/en/whatyouwant.asp?nt=189>

This Protocol expands the scope of the Convention on Cybercrime (ETS no. 185) to also criminalise acts of a racist and xenophobic nature committed through computer systems:

Article 3 – Dissemination of racist and xenophobic material through computer systems
Article 4 – Racist and xenophobic motivated threat
Article 5 – Racist and xenophobic motivated insult
Article 6 – Denial, gross minimisation, approval or justification of genocide or crimes against humanity

European Union – <http://europa.eu.int/>

NOTE: It is useful to understand the "institutional triangle" of the European Union and how decision making and legislation work

The European Union at a glance – <http://europa.eu.int/abc-en.htm>
Institutions of the European Union – <http://europa.eu.int/inst-en.htm>

European Parliament (EP) – <http://www.europarl.eu.int/>
626 members, elected by citizens
shares with the Council the power to legislate
exercises supervision over the Commission (approves nomination of Commissioners) and all institutions

Council of the European Union – <http://ue.eu.int/>
one representative from each member state
decision-making role

European Commission – <http://europa.eu.int/comm/>
20 members, appointed by member states after approval by EP
draft legislation and proposals to EP and Council
responsible for implementing legislation adopted
guardian of Treaties and ensures that Community law is applied
represents the Union internationally and negotiates international agreements

EUR-Lex – The portal to European Union Law
<http://www.europa.eu.int/eur-lex/>

EUR-Lex – Legislation In Force
<http://www.europa.eu.int/eur-lex/en/search/search_lif.html>

Analytical structure/register index for
13.20.60 Information technology, telecommunications, and data processing
<http://europa.eu.int/eur-lex/en/lif/reg/en_register_132060.html>

Directive 95/46/EC – on the protection of individuals with regard to the processing of personal data and on the free movement of such data
<http://www.europa.eu.int/servlet/portail/RenderServlet?search=DocNumber&lg=en&nb_docs>=25&domain=Legislation&coll=&in_force=NO&an_doc=1995&nu_doc=46&type_doc=Directive>

Directive 97/66/EC – concerning the processing of personal data and the protection of privacy in the telecommunications sector
<http://www.europa.eu.int/servlet/portail/RenderServlet?search=DocNumber&lg=en&nb_docs=25&domain=Legislation&coll=&in_force=NO&an_doc=1997&nu_doc=66&type_doc=Directive>

Directive 98/84/EC – on the legal protection of services based on, or consisting of, conditional access
<http://www.europa.eu.int/servlet/portail/RenderServlet?search=DocNumber&lg=en&nb_docs=25&domain=Legislation&coll=&in_force=NO&an_doc=1998&nu_doc=84&type_doc=Directive>

Directive 2000/31/EC – on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce")
<http://www.europa.eu.int/servlet/portail/RenderServlet?search=DocNumber&lg=en&nb_docs=25&domain=Legislation&coll=&in_force=NO&an_doc=2000&nu_doc=31&type_doc=Directive>

Decision No 276/1999/EC – adopting a multiannual community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks
<http://www.europa.eu.int/servlet/portail/RenderServlet?search=DocNumber&lg=en&nb_docs=25&domain=Legislation&coll=&in_force=NO&an_doc=1999&nu_doc=276&type_doc=Decision>

Safer Internet Action Plan (IAP)
<http://europa.eu.int/information_society/programmes/iap/index_en.htm>
<http://www.saferinternet.org/>
IAP Action Lines include

- creating a safer environment
  - creating a European network of hotlines
  - encouraging self-regulation and codes of conduct
- developing filtering and rating systems
  - demonstrating the benefits of filtering and rating
  - facilitating international agreement on rating systems
- encouraging awareness actions
  - preparing the ground for awareness actions
  - encouraging implementation of full-scale awareness actions
- support actions

accessing legal implications
coordination with similar international initiatives
evaluating the impact of community measures

Information Society
<http://europa.eu.int/information_society/index_en.htm>
<http://europa.eu.int/pol/infso/index_en.htm>

EUR-Lex – Official Journal
<http://www.europa.eu.int/eur-lex/en/search/search_oj.html>

OJ 2000/C 124 – The Prevention and Control of Organised Crime: A European Union Strategy for the beginning of the new Millennium
<http://www.europa.eu.int/servlet/portail/RenderServlet?search=RefPub&lg=en&nb_docs=25&domain=Legislation&in_force=NO&year=2000&month=5&day=&coll=JOC&nu_jo=124>

OJ 2002/C 203
<http://www.europa.eu.int/servlet/portail/RenderServlet?search=RefPub&lg=en&nb_docs=25&domain=&in_force=NO&year=2002&month=8&day=27&coll=JOC&nu_jo=203&page=109>

Communication COM/2002/0173 final – CNS 2002/0086 – Proposal for a Council Framework Decision on attacks against information systems
<http://www.europa.eu.int/servlet/portail/RenderServlet?search=DocNumber&lg=en&nb_docs=25&domain=Preparatory&in_force=NO&type_doc=COMfinal&an_doc=2002&nu_doc=173>

EUR-Lex – Documents of Public Interest
<http://www.europa.eu.int/eur-lex/en/search/search_dpi.html>

Communication COM/2000/0890 final – Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime (eEurope 2002)
<http://www.europa.eu.int/servlet/portail/RenderServlet?search=DocNumber&lg=en&nb_docs=25&domain=Preparatory&in_force=NO&type_doc=COMfinal&an_doc=2000&nu_doc=890>

Communication COM/2001/0298 final – Network and Information Security: Proposal for A European Policy Approach
<http://www.europa.eu.int/servlet/portail/RenderServlet?search=DocNumber&lg=en&nb_docs=25&domain=Preparatory&in_force=NO&type_doc=COMfinal&an_doc=2001&nu_doc=298>

G8 – G8 Information Centre <http://www.g8.utoronto.ca/>

The Birmingham Summit (1998)
"G8 and International Crime"
<http://birmingham.g8summit.gov.uk/crime/>

G8 Lyon Group - links
<http://www.g8.utoronto.ca/crime/>
<http://www.auswaertiges-amt.de/www/en/aussenpolitik/vn/lyon_group_html>
<http://www.g8j-i.ca/english/experts.html>
<http://www.usdoj.gov/criminal/cybercrime/G8experts.htm>

United Nations – <http://www.un.org/>

United Nations Office for Drugs and Crime (UNODC)
<http://www.unodc.org/>

UNODC Crime Programme
<http://www.unodc.org/unodc/crime_cicp.html>

United Nations Crime and Justice Information Network (UNCJIN)
<http://www.unodc.org/unodc/en/uncjin.html>
<http://www.uncjin.org/> (previous site)

United Nations Convention Against Transnational Organized Crime
<http://www.unodc.org/unodc/crime_cicp_convention.html>

Organization of American States – <http://www.oas.org/>

Cyber Crime
<http://www.oas.org/juridico/english/cyber.htm>

Resolutions of the General Assembly of the OAS Related to Cyber Crime
<http://www.oas.org/juridico/english/cyber_reso.htm>

Best Practices (not necessarily law/legislation)

Organisation for Economic Co-operation and Development (OECD) –
<http://www.oecd.org/>

Information Security and Privacy
<http://www.oecd.org/sti/security-privacy>

OECD Guidelines for the Security of Information Systems and Networks
<http://www.oecd.org/dataoecd/59/0/1946946.pdf>
<http://www.oecd.org/dataoecd/27/6/2494779.pdf>

United States Federal Laws

U.S. House of Representatives – Office of the Law Revision Counsel
<http://uscode.house.gov/>
United States Code (U.S.C.) – a consolidation and codification by subject matter of the general and permanent laws of the United States
Search the United States Code for a specific section at <http://uscode.house.gov/usc.htm>

U.S. Library of Congress – THOMAS, Legislative Information on the Internet
<http://thomas.loc.gov/>
Bills, Public Laws, and other legislation

U.S. Department of Justice – Computer Crime and Intellectual Property Section (CCIPS)
<http://www.cybercrime.gov/>

U.S. Department of Justice - **Federal Computer Intrusion Laws**
<http://www.cybercrime.gov/cclaws.html>
Federal criminal code related to computer crime

Title 18 – Crimes and Criminal Procedure
Chapter 47 – Fraud and False Statements
18 U.S.C. § 1029* – Fraud and related activity in connection with access devices
<http://www.cybercrime.gov/usc1029.htm>
18 U.S.C. § 1030* – Fraud and related activity in connection with computers
<http://www.cybercrime.gov/1030_new.html>
Chapter 65 – Malicious Mischief
18 U.S.C. § 1362* – Communication lines, stations or systems
<http://www.cybercrime.gov/usc1362.htm>
Chapter 119 – Wire and Electronic Communications Interception and Interception of Oral Communications
18 U.S.C. § 2511* – Interception and disclosure of wire, oral, or electronic communications prohibited
<http://www.cybercrime.gov/usc2511.htm>
Chapter 121 – Stored Wire and Electronic Communications and Transactional Records Access
18 U.S.C. § 2701* – Unlawful access to stored communications
<http://www.cybercrime.gov/usc2701.htm>
18 U.S.C. § 2702* – Disclosure of contents
<http://www.cybercrime.gov/usc2702.htm>
18 U.S.C. § 2703* – Requirements for governmental access
<http://www.cybercrime.gov/usc2703.htm>

* USA Patriot Act – Public Law 107-56 (H.R. 3162)
Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001
<http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107.pdf>
Amends 18 U.S.C. § 1029, 1030, 1362, 2511, 2702, 2703

U.S. Department of Justice - **Criminal Intellectual Property Laws**
<http://www.cybercrime.gov/iplaws.htm>
Federal Statutes Protecting Intellectual Property Rights

Copyright Offenses
Title 17 – Copyrights

Chapter 5 – Copyright Infringement and Remedies
17 U.S.C. § 506 – Criminal offenses
<http://www.cybercrime.gov/17usc506.htm>
Title 18 – Crimes and Criminal Procedure
Chapter 113 – Stolen Property
18 U.S.C. § 2318 – Trafficking in counterfeit labels for phonorecords, copies of computer programs or computer program documentation or packaging, and copies of motion pictures or other audio visual works, and trafficking in counterfeit computer program documentation or packaging
<http://www.cybercrime.gov/18usc2318.htm>
18 U.S.C. § 2319 – Criminal infringement of a copyright
<http://www.cybercrime.gov/18usc2319.htm>

Copyright Management Offenses – Digital Millennium Copyright Act (DMCA)
Title 17 – Copyrights
Chapter 12 – Copyright Protection and Management Systems
17 U.S.C. § 1201 – Circumvention of copyright protection systems
<http://www.cybercrime.gov/17usc1201.htm>
17 U.S.C. § 1202 – Integrity of copyright management information
<http://www.cybercrime.gov/17usc1202.htm>
17 U.S.C. § 1203 – Civil remedies
<http://www.cybercrime.gov/17usc1203.htm>
17 U.S.C. § 1204 – Criminal offenses and penalties
<http://www.cybercrime.gov/17usc1204.htm>
17 U.S.C. § 1205 – Savings clause
<http://www.cybercrime.gov/17usc1205.htm>

Bootlegging Offenses
Title 18 – Crimes and Criminal Procedure
Chapter 113 – Stolen Property
18 U.S.C. § 2319A – Unauthorized fixation of and trafficking in sound recordings and music videos of live musical performances
<http://www.cybercrime.gov/18usc2319A.htm>

Trademark Offenses
Title 18 – Crimes and Criminal Procedure
Chapter 113 – Stolen Property
18 U.S.C. § 2320 – Trafficking in counterfeit goods or services
<http://www.cybercrime.gov/18usc2320.htm>
Amended by Pub. L. 107-140, sec. 1, 116 Stat. 12.

Trade Secret Offenses
Title 18 – Crimes and Criminal Procedure
Chapter 90 – Protection of Trade Secrets
18 U.S.C. § 1831 – Economic espionage
<http://www.cybercrime.gov/18usc1831.htm>

18 U.S.C. § 1832 – Theft of trade secrets
<http://www.cybercrime.gov/18usc1832.htm>
18 U.S.C. § 1833 – Exceptions to prohibitions
<http://www.cybercrime.gov/18usc1833.htm>
18 U.S.C. § 1834 – Criminal forfeiture
<http://www.cybercrime.gov/18usc1834.htm>
18 U.S.C. § 1835 – Orders to preserve confidentiality
<http://www.cybercrime.gov/18usc1835.htm>
18 U.S.C. § 1836 – Civil proceedings to enjoin violations
<http://www.cybercrime.gov/18usc1836.htm>
18 U.S.C. § 1837 – Applicability to conduct outside the United States
<http://www.cybercrime.gov/18usc1837.htm>
18 U.S.C. § 1838 – Construction with other laws
<http://www.cybercrime.gov/18usc1838.htm>
18 U.S.C. § 1839 – Definitions
<http://www.cybercrime.gov/18usc1839.htm>

Offenses Relating to the Integrity of Intellectual Property Systems

Title 17 – Copyrights
Chapter 5 – Copyright Infringement and Remedies
17 U.S.C. § 506(c) – Criminal offenses – Fraudulent Copyright Notice
<http://www.cybercrime.gov/17usc506_c-d.htm>
17 U.S.C. § 506(d) – Criminal offenses – Fraudulent Removal of Copyright Notice
<http://www.cybercrime.gov/17usc506_c-d.htm>
17 U.S.C. § 506(e) – Criminal offenses – False Representation
<http://www.cybercrime.gov/17usc506_e.htm>

Title 18 – Crimes and Criminal Procedure
Chapter 25 – Counterfeiting and Forgery
18 U.S.C. § 497 – Letters patent
<http://www.cybercrime.gov/18usc497.htm>

Title 35 – Patents
Chapter 29 – Remedies for Infringement of Patent, and Other Actions
35 U.S.C. § 292 – False marking
<http://www.cybercrime.gov/35usc292.htm>

Offenses Relating to the Misuse of Dissemination Systems

Title 18 – Crimes and Criminal Procedure
Chapter 41 – Extortion and Threats
18 U.S.C. § 875 – Interstate communications
Chapter 63 – Mail Fraud
18 U.S.C. § 1341 – Frauds and swindles
<http://www.cybercrime.gov/18usc1341.htm>
Amended by Pub. L. 107-204, sec. 903(a), 116 Stat. 805.

New note added by Pub. L. 107-204, sec. 901, 116 Stat. 804.

18 U.S.C. § 1343 – Fraud by wire, radio, or television
<http://www.cybercrime.gov/18usc1343.htm>

Amended by Pub. L. 107-204, sec. 903(b), 116 Stat. 805.

Chapter 119 – Wire and Electronic Communications Interception and Interception of Oral Communications

18 U.S.C. § 2512 – Manufacture, distribution, possession, and advertising of wire, oral, or electronic communication intercepting devices prohibited
<http://www.cybercrime.gov/18usc2512.htm>

Title 47 – Telegraphs, Telephones, and Radiotelegraphs
Chapter 5 – Wire or Radio Communication

47 U.S.C. § 553 – Unauthorized reception of cable service
<http://www.cybercrime.gov/47usc553.htm>

47 U.S.C. § 605 – Unauthorized publication or use of communications
<http://www.cybercrime.gov/47usc605.htm>

Other U.S. Privacy Laws

United States Constitution – 4th Amendment – Unreasonable Search and Seizure
<http://www.archives.gov/exhibit_hall/charters_of_freedom/bill_of_rights /amendments_1-10.html>

Title 5 – Government Organization And Employees
Chapter 5 – Administrative Procedure

5 U.S.C. § 552A – Records maintained on individuals

Title 42 – The Public Health And Welfare
Chapter 21a – Privacy Protection

42 U.S.C. § 2000AA – Searches and seizures by government officers and employees in connection with investigation or prosecution of criminal offenses

Other U.S. Federal Laws, Regulations, and Requirements

Presidential Decision Directive 63 (PDD 63) – Critical Infrastructure Protection [1998]
White paper – <http://csrc.nist.gov/policies/paper598.pdf>
Requires federal agencies to protect critical infrastructure, especially cyber-based systems; and creates four new organizations: NIPC, ISACs, NICA, and CIAO. Also assigns lead agencies for sector liaisons.

Public Law 104-106 – National Defense Authorization Act for Fiscal Year 1996 [S. 1124]
Includes the **Clinger Cohen Act** (formerly known as the "Information Technology Management Reform Act of 1996") in Division E
Requires the head of each federal executive agency to ensure that information security policies, procedures, and practices are adequate.

<http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=104_cong_public_laws&docid=f:publ106.104.pdf>

Public Law 106-102 – **Gramm-Leach-Bliley Act** [S. 900] 1999
(aka Financial Services Modernization Act)
Obliges financial institutions to protect the privacy of customers' nonpublic personal information and to implement safeguards; criminalizes fraudulent access to financial information.
<http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws&docid=f:publ102.106.pdf>
15 U.S.C. § 6801-6810 Disclosure of Nonpublic Personal Information
15 U.S.C. § 6821-6827 Fraudulent Access to Financial Information
See also <http://www.ftc.gov/privacy/glbact/>

Public Law 107-296 – Homeland Security Act of 2002 [H.R. 5005]
Includes FISMA in Title X – Information Security
(superseded by P.L. 107-347 Title III)
<http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ296.107.pdf>

Public Law 107-347 – E-Government Act of 2002 [H.R. 2458]
Includes amended version of FISMA in Title III – Information Security
(supersedes Title X in P.L. 107-296)
<http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ347.107.pdf>

Federal Information Security Management Act of 2002
Requires each federal government agency to implement programs and procedures for detecting, reporting, and responding to security incidents, consistent with published standards and guidelines

U.S. Department of Defense (DoD) Information Technology Security Certification and Accreditation Process (DITSCAP)
<http://iase.disa.mil/ditscap/>
DoD Instruction 5200.40 – Implements policy, assigns responsibilities, and prescribes procedures for certification and accreditation of information technology (information systems, networks, and sites) in the Department of Defense

U.S. Office of Management and Budget (OMB) – <http://www.whitehouse.gov/omb/>
Circular No. A-130 (Revised) – Management of Federal Information Resources
<http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html>
Establishes policy for the management of Federal information resources

Executive Order 13231 – Critical Infrastructure Protection in the Information Age
Authorizes protection program to secure information systems for critical infrastructure
<http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=2001_register&docid=fr18oc01-139.pdf>

Federal Trade Commission
16 CFR Part 314 – Standards for Safeguarding Customer Information
<http://www.ftc.gov/os/2002/05/67fr36585.pdf>
Implements sections of the Gramm-Leach-Bliley Act and "sets forth standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information." Financial institutions must implement an information security program.

Other Lists of U.S. IT Laws

Chief Information Officers Council (CIOC) Documents – IT Related Laws and Legislation
<http://cio.gov/index.cfm?function=documents&section=it related laws and regulations>

FedCIRC – Library – Legislation
<http://www.fedcirc.gov/library/legislation/>

GSA Office of Electronic Government and Strategy – <http://www.estrategy.gov/>
E-Government Laws, Regulations, and Policies
<http://www.estrategy.gov/it_policy_documents.cfm>
Key E-Government Related Laws – <http://www.estrategy.gov/elaws.cfm>
All E-Government Related Laws Chronological By Congress –
<http://www.estrategy.gov/lawscongress.cfm>

GSA – Policies, Guidelines, Regulations, and Best Practices
<http://www.gsa.gov/Portal/policies.jsp>

NIST – CSRC – Policies – Federal Requirements
<http://csrc.nist.gov/policies/>

U.S. Department of Education – Office of the Chief Information Officer – Legislation and Guidelines
<http://www.ed.gov/print/about/offices/list/ocio/legislation.html>

Other U.S. Industry Standards

American Institute of Certified Public Accountants (AICPA) – <http://www.aicpa.org/>
Statement on Auditing Standards (SAS) No. 70, Service Organizations
Audit guide for reports on a service organization's controls, and for financial statements of entities that use service organizations
<http://www.sas70.com/>

United States State Laws

National Security Institute – Computer Crime Laws by State
<http://nsi.org/Library/Compsec/computerlaw/statelaws.html>

SecurityFocus Online – Library

Computer Crime
<http://online.securityfocus.com/library/category/9>

U.S. Laws
<http://online.securityfocus.com/library/category/67>

American Law Sources On-Line
<http://www.lawsource.com/also/>

Library of Congress – State and Local Governments
<http://lcweb.loc.gov/global/state/stategov.html>

Law Enforcement Agencies/Organizations

Interpol – <http://www.interpol.int/>

Europol – <http://www.europol.eu.int/>
List of international law enforcement links –
<http://www.europol.eu.int/index.asp?page=links>
World Customs Organization – <http://www.wcoomd.org/>

Officer.Com: Law Enforcement Resource Site <http://search.officer.com/agencysearch/>

International Police Association – <http://www.ipa-iac.org/>

Australia
Australian Federal Police – <http://www.afp.gov.au/>

Canada
Royal Canadian Mounted Police – <http://www.rcmp-grc.gc.ca/>

United Kingdom
Metropolitan Police Service – <http://www.met.police.uk/>
Internet Crime Forum – <http://www.internetcrimeforum.org.uk/>

United States

U.S. Department of Homeland Security (DHS) – <http://www.dhs.gov/>
U.S. Secret Service (USSS) – <http://www.secretservice.gov/>
U.S. Bureau of Customs and Border Protection (CBP) – <http://www.cbp.gov/>
National Infrastructure Protection Center (NIPC) – <http://www.nipc.gov/>

U.S. Department of Justice (DOJ) – <http://www.usdoj.gov/>
<http://www.usdoj.gov/criminal/cybercrime/>
<http://www.cybercrime.gov/>

Bureau of Alcohol, Tobacco, Firearms and Explosives – <http://www.atf.gov/>

Federal Bureau of Investigations (FBI) – <http://www.fbi.gov/>

Internet Fraud Complaint Center – <http://www.ifccfbi.gov/>

Internal Revenue Service – <http://www.irs.gov/>

Defense Criminal Investigative Service – <http://www.dodig.osd.mil/INV/DCIS/>

U.S. Postal Inspection Service – <http://www.usps.com/postalinspectors/>

Law Resources

Australasian Legal Information Institute – <http://www.austlii.edu.au/>

Baker & McKenzie – Global Information Security Law
<http://www.bmck.com/ecommerce/articles-s.htm>

Cornell Law School – Legal Information Institute – <http://www.law.cornell.edu/>
Includes U.S. codes, court opinions, national and international laws

FindLaw – <http://www.findlaw.com>

Internet Law Library (formerly the U.S. House of Representatives Internet Law Library)
The U.S. House of Representatives has discontinued hosting the library, but several other sites continue to carry it, including:
<http://www.priweb.com/internetlawlib/>
<http://www.lawguru.com/ilawlib/>
<http://www.lectlaw.com/inll/>
<http://www.phillylawyer.com/1/1.HTM>

LawResearch (Membership website) – <http://www.lawresearch.com/>
Internet Law Library; International Law; United States Law

Organization of American States – <http://www.oas.org/>
Cyber Crime Links – <http://www.oas.org/juridico/english/cyber_links_list.htm>

U.S. Department of Justice – Computer Crime and Intellectual Property Section (CCIPS)
<http://www.cybercrime.gov/>
<http://www.usdoj.gov/criminal/cybercrime/>
"How to Report Internet-Related Crime" – <http://www.cybercrime.gov/reporting.htm>

U.S. Federal Regulations – <http://www.regulations.gov/>

U.S. Government FIRSTGOV.gov – <http://www.firstgov.gov/>
Citizen's Public Safety and Law –
<http://www.firstgov.gov/Citizen/Topics/PublicSafety.shtml>
Government-to-Government Public Safety and Law –
<http://www.firstgov.gov/Government/State_Local/Safety.shtml>
Businesses – <http://www.businesslaw.gov/>

U.S. Government Printing Office – National Archives and Records Administration
- GPO Access – <http://www.gpoaccess.gov/>
- Code of Federal Regulations (CRF) – <http://www.gpoaccess.gov/cfr/>
- Public and Private Laws – <http://www.gpoaccess.gov/plaws/>

U.S. House of Representatives – Office of the Law Revision Counsel – <http://uscode.house.gov/>

U.S. Library of Congress
Global Legal Information Network – <http://www.loc.gov/law/glin/>
THOMAS Legislative Information on the Internet – <http://thomas.loc.gov/>

Resources on Collecting Evidence

International Organization on Computer Evidence (IOCE) – <http://www.ioce.org/>
"G8 Proposed Principles For The Procedures Relating To Digital Evidence" (2000)
<http://www.ioce.org/G8_proposed_principles_for_forensic_evidence.html>

U.S. Department of Justice – Computer Crime and Intellectual Property Section (CCIPS)
<http://www.cybercrime.gov/>
<http://www.usdoj.gov/criminal/cybercrime/>
"Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" (2002)
<http://www.cybercrime.gov/searching.html#A>
<http://www.cybercrime.gov/s&smanual2002.htm>
Office of Justice Programs – National Institute of Justice
"Electronic Crime Scene Investigation: A Guide for First Responders" (2001)
<http://www.ojp.usdoj.gov/nij/pubs-sum/187736.htm>

U.S. Secret Service and International Association of Chiefs of Police
"Best Practices for Seizing Electronic Evidence" (2001)
<http://www.secretservice.gov/electronic_evidence.shtml>
<http://www.theiacp.org/documents/index.cfm?fuseaction=document&document_id=97>

RFC 3227/BCP 55 – "Guidelines for Evidence Collection and Archiving" (2002)
<ftp://ftp.rfc-editor.org/in-notes/rfc3227.txt>

SC Magazine August 2002
"Crime Issue" – articles on computer forensics, collecting evidence, "The Judiciary and the Digital World"
<http://www.scmagazine.com/scmagazine/2002_08/main.html>

Standards Australia – <http://www.standards.com.au/>
HB 171-2003: "Guidelines for the management of IT evidence" (2003)
<http://www.standards.com.au/catalogue/script/Details.asp?DocN=AS342335504743>
Earlier Draft: <http://www.auscert.org.au/render.html?it=3117&cid=1920>

Appendix E: Sample Incident Reporting Forms and Flowcharts

This appendix includes several guidelines, procedures, and templates related to the incident handling function. Those for which we obtained reprint permission from the author or publisher are reproduced in full as part of this appendix. Others for which we had not received permission as of the publication date are listed with references to their materials and/or a link to online information at the end of the appendix. We encourage our readers to peruse these examples as additional resources that are of interest to CSIRT staff.

CERT Coordination Center

The CERT/CC has both a text-based reporting form and an automated incident reporting form. The text-based form has been included here.

Both forms are available from <http://www.cert.org/nav/index_red.html> (see the "Communicate With Us" box on the right-hand side of the page).

```
-----BEGIN PGP SIGNED MESSAGE-----

version 5.2, April 2000

                    CERT(R) Coordination Center
                      Incident Reporting Form

CERT/CC has developed the following form in an effort to gather incident information.
If you believe you are involved in an incident, we would appreciate your completing
the form below. If you do not believe you are involved in an incident, but have a
question, send email to:
   cert@cert.org

Note that our policy is to keep any information specific to your site confidential
unless we receive your permission to release that information.

We would appreciate any feedback or comments you have on this Incident Reporting Form.
Please send your comments to:
   cert@cert.org

Submit this form to: cert@cert.org
If you are unable to send email, fax this form to: +1 412 268 6989


Your contact and organizational information
1. name......................:
2. organization name.........:
3. sector type (such as banking, education, energy
   or public safety).........:
4. email address.............:
5. telephone number..........:
6. other.....................:

Affected Machine(s)
(duplicate for each host)
7. hostname and IP...........:
8. timezone..................:
9. purpose or function of the host (please be as specific
   as possible)..............:

Source(s) of the Attack
(duplicate for each host)
10. hostname or IP...........:
11. timezone.................:
12. been in contact?.........:

13. Estimated cost of handling incident
    (if known)...............:

14. Description of the incident (include dates, methods of intrusion, intruder tools
    involved, software versions and patch levels, intruder tool output, details of
    vulnerabilities exploited, source of attack, or any other relevant information):


Copyright 2003 Carnegie Mellon University

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.0.6 (GNU/Linux)
Comment: For info see http://www.gnupg.org

iQCVAwUBP410w5Z2NNT/dVAVAQGlCgP/WZlEvbsNW04pRytLssVMEPd4RT7qshxssjtdp5IDFAA4RUnC2UxLGI
HCyqihGawK45XUafD26fulh0yPISxg3Ev5b+4u7lM1GKjVcjtA0jtbW7UfQwBpkaPCJuVyhEOMMLRuWNCUF3Id
FoJfuoFrcQ0tTJ26pUkA
MXrIR2S011U=
=xQHt
-----END PGP SIGNATURE-----
```

Reprinted with permission from the CERT® Coordination Center. Available at <http://www.cert.org/reporting/incident_form.txt>.

CIO/FBI/USSS

These are the *CIO Cyberthreat Response and Reporting Guidelines*, published by *CIO* in conjunction with the FBI and the USSS [CIO 02]. The document provides, in addition to the guidelines, a number of law enforcement contact information, FBI-USSS field contact information, other cyber-threat resources, and a cyber-threat reporting form.

The document is available from
<http://www.cio.com/research/security/incident_response.pdf>.

CIO CYBERTHREAT RESPONSE & REPORTING GUIDELINES

COMPONENTS

- Background and Scope of Project
- CIO Cyberthreat Response & Reporting Guidelines
- Who to Contact: Law Enforcement
- Who to Contact: Reporting Bodies & Resources for Cyberthreat Response
- FBI and USSS Field Office contact list
- Report Form—short, standard, first-alert form
- Contributors

Reprinted through the courtesy of CIO. Copyright © 2003 CXO Media, Inc. ALL RIGHTS RESERVED.

CIO CYBERTHREAT RESPONSE & REPORTING PROJECT

A collaboration among industry professionals, law enforcement and CIO Magazine to develop guidelines for reporting computer security incidents to law enforcement

At the CIO Perspectives conference in Palm Springs in October 2001, audience members (chief information officers and other executives) were encouraged by the U.S. Attorney for Los Angeles to report cybersecurity breaches to law enforcement as part of the war against terrorism. But, as one CIO asked: "We get hit thousands of times a month; do you want us to report all of these incidents? And exactly who do we contact?" Other audience members expressed similar bewilderment, and that's what prompted this initiative.

Goal This project has a modest goal: to provide a basic understanding of what is required for cyberthreat incident response and to make it as easy as possible to report such incidents to law enforcement (including whom to call and what to tell them). For this effort, we restricted our recommendations to reporting incidents that are an attack on information systems or data (computer and/or Internet security). We did not attempt to address other types of cybercrime such as Internet fraud or pornography.

A Complex Issue Creating and maintaining a secure information environment is difficult, expensive and complicated. Risk assessment; control selection and deployment; monitoring/detection; incident response and continuous improvement must all be considered together. Prevention is, of course, the primary objective.

Incident response is itself a complex subject, including the sometimes difficult decision of whether to share any information at all. There are many excellent resources available to help CIOs and CISOs (chief information security officers) understand and address these challenges; you'll find some of them listed at the end of this document under "Resources."

Why You Should Report Cybercrime Only by sharing information with law enforcement and appropriate industry groups will we be able to identify and prosecute cybercriminals, identify new cybersecurity threats and prevent successful attacks on our critical infrastructures and economy. Law enforcement's ability to identify coordinated threats is directly tied to the amount of reporting that takes place.

We understand that you might be reluctant to share information regarding the impact to your business and the sensitivity of the data involved. While we will not make the case here for trusting various agencies or organizations, we encourage you to learn more about how law enforcement and other reporting bodies approach these issues in terms of the likely impact of their investigation on your business and how they handle sensitive information.

Reprinted through the courtesy of CIO. Copyright © 2003 CXO Media, Inc. ALL RIGHTS RESERVED.

CIO CYBERTHREAT RESPONSE & REPORTING GUIDELINES

An organization must respond in some way to a computer security breach—whether it is an intrusion/hack, the implantation of malicious code such as a virus or worm, or a denial of service attack. The better prepared the organization is to respond quickly and effectively, the better chance it will have to minimize the damage. These guidelines are intended to provide a framework and starting point for developing a cyberthreat response and reporting capability.

PLANNING

- Develop an incident response plan and designate people to carry it out. The plan should include details for how you will:
  - detect the incident
  - analyze the incident
  - contain or eradicate the problem
  - provide workarounds or fixes
  - prevent re-infection
  - log events
  - preserve evidence
  - conduct a post-mortem and apply lessons learned
- Educate users to raise security awareness and promote security policies.
- Build a centralized incident reporting system.
- Establish escalation procedures that lay out actions the company should take if an attack turns out to be protracted or especially damaging.
- Make sure your service-level agreements include provisions for security compliance, and spell out reporting requirements and maintenance of systems (including contingency plans) in the event of a cyberattack.
- Decide in advance under what circumstances you'd call the authorities.
- Plan how and when employees, customers and strategic partners will be informed of the problem.
- Establish communication procedures should this become a media event.

PEOPLE

- Have a single contact to whom employees should report suspicious events and who will track changes in contacts or procedures.
- Have a single contact who will report incidents to outside agencies, including law enforcement, regulatory bodies and information sharing organizations such as InfraGard and the industry Information Sharing and Analysis Centers (ISACs).
- Keep a list of the incident response team members' names, titles and 24/7 contact information, along with their role in a security breach.
- Have contact information for vendors contracted to help during a security emergency, as well as ISPs and other relevant technology providers.
- Have contact information for major customers and clients who might be affected.
- In advance, establish contacts at the relevant law-enforcement agencies: typically, the national infrastructure protection and computer intrusion squad at the local FBI field office; the electronic crimes investigator at the local Secret Service field office; and the electronic crimes investigator at your local police. Have their contact information easily accessible.

PROCESS

- Perform a risk analysis on your plan.
- Test/rehearse procedures periodically.
- Develop contingency plans in case your response infrastructure is attacked.

WHAT TO REPORT

You should report cybersecurity events that have a real impact on your organization (when damage is done, access is achieved by the intruder, loss occurs, malicious code is implanted) or when you detect something noteworthy or unusual (new traffic pattern, new type of malicious code, specific IP as source of persistent attacks).

At this time, we do not recommend that you report routine probes, port scans or other common events. Neither law enforcement nor the ISACs are prepared to receive or analyze the enormous volume of data this would entail. While such detailed "hit" data has potential value in identifying and defining trends, and facilities like the Internet Storm Center (at the SANS Institute) or the NIPC may eventually get set up to collect detailed event logs, right now it is generally not useful.

Consequently, the form we recommend is designed to report significant, unusual or noteworthy incidents.

WHEN AND HOW TO REPORT AN INCIDENT

If an attack is under way, you'll want to pick up the phone and call your previously established law-enforcement contact immediately and communicate the

Reprinted through the courtesy of CIO. Copyright © 2003 CXO Media, Inc. ALL RIGHTS RESERVED.

basic information that is included in the CIO Cyberthreat Response Form. There is additional information that will be required to effectively conduct the investigation (see bullet points below), but the form is a good place to start.

Sometimes you will report an incident to law enforcement after the fact—you have detected that something happened, but your systems are functioning normally and whatever damage is likely has already been done. In this case, you will want to gather as much information as possible for the law enforcement agents before you make the call.

Here is some additional information that will help law enforcement agents in their investigation:

- What are the primary systems involved?
- How was the attack carried out?
- What steps have you taken to mitigate or remediate?
- Does a suspect exist? If so, is it a current or former employee/contractor?
- What evidence is available to assist in the investigation (e.g., log files, physical evidence, etc.?)

To track the status of your case once you've filed a report, contact the field office that is conducting the investigation.

CIO CYBERTHREAT RESPONSE & REPORTING GUIDELINES

Reprinted through the courtesy of CIO. Copyright © 2003 CXO Media, Inc. ALL RIGHTS RESERVED.

WHO TO CONTACT

LAW ENFORCEMENT

There is no single answer for which law enforcement agency to contact in the event of a cyber-security breach. The FBI and U.S. Secret Service share jurisdiction for computer crimes that cross state lines. However, most law enforcement agencies, including the FBI and USSS, encourage people to a) preestablish contact with someone in law enforcement who is trained in and responsible for dealing with computer crime, and b) work with the person or people you have the best relationship with, regardless of agency.

FEDERAL AGENCIES, LOCAL CONTACTS

FBI Field Office Call the national infrastructure protection and computer intrusion squad at the local field office.*

U.S. Secret Service Field Office Contact the electronic crimes investigator at the local field office.*

*A list of local field offices follows Page 6.

FEDERAL AGENCIES, WASHINGTON

FBI/National Infrastructure Protection Center (NIPC)
J. Edgar Hoover Building
935 Pennsylvania Avenue, NW
Washington, DC 20535-0001
phone: (202) 323-3205; 888-585-9078
fax: (202) 323-2079
e-mail: *nipc.watch@fbi.gov*
website: *www.nipc.gov*
reporting: *www.nipc.gov/incident/cirr.htm*

Electronic Crimes Branch of the U.S. Secret Service Headquarters
950 H Street, NW
Washington, DC 20223
phone: (202) 406-5850
fax: (202) 406-5031
website & reporting: *www.treas.gov/usss*

STATE & LOCAL AGENCIES

State Attorney General's Office The website for the National Attorney Generals' Association provides a list with contact information by state.
www.naag.org/issues/20010724-cc_list.cfm

Local Police: The CrisNet website offers a list of local law enforcement agencies organized by state.
www.crisnet.com/locallaw/locallaw.html

OTHER REPORTING BODIES & RESOURCES FOR CYBERTHREAT SUPPORT

Most of the following organizations not only serve as coordination points for reporting incidents, but they also offer lots of useful information for network security and incident response.

National Infrastructure Protection Center (NIPC)
Focal point for threat assessment, warning, investigation and response for threats or attacks against United States critical infrastructures.
www.nipc.gov

InfraGard
Public/private information-sharing effort led by the FBI and the NIPC. Local chapters across the United States. Great place to develop appropriate contacts with law enforcement.
www.infragard.net

Electronic Crimes Task Force
Public/private info-sharing effort led by the U.S. Secret Service. Regional task forces located across the United States, and a great place to develop computer-crime law-enforcement contacts.
www.ectaskforce.org/Regional_Locations.htm

Information Sharing & Analysis Centers (ISACs)
Industry specific information sharing for critical infrastructure sectors.
For general information on the ISACs, see https://www.it-isac.org/isacinfowhtppr.php

Electric . . . . . *www.nerc.com*
Financial Services . . . *www.fsisac.com*
IT . . . . . *www.it-isac.org*
Oil & Gas . . . . . *www.energyisac.com*
Telecom . . . . . *www.ncs.gov & www.ncs.gov/Image-Files/ISAC_Fact.pdf*
U.S Govt. . . . . *www.fedcirc.gov*
Water . . . . . *www.amwa.net/isac/*

Forum of Incident Response and Security Teams
A network of computer security incident response teams and info sharing designed for the private sector.
www.first.org

Reprinted through the courtesy of CIO. Copyright © 2003 CXO Media, Inc. ALL RIGHTS RESERVED.

Department of Justice Computer Crime & Intellectual Property Section
Legal analysis and resources related to computer crime, a how-to-report section and a comprehensive list of cybercrime cases pending and resolved.
www.cybercrime.gov

CERT Coordination Center at Carnegie Mellon
Federally funded research center provides training, incident handling, R&D, advisories. Lots of good information resources available to the public.
www.cert.org

SANS Institute
Cooperative research organization offers alerts, training and certification; operates Incidents.org and the Internet Storm Center. Like CERT, has lots of good information resources on its website.
www.sans.org
www.incidents.org

ADDITIONAL RESOURCES

***CIO* Magazine Security and Privacy Research Center**
A collection of articles, guidelines and links for information security issues from an executive perspective.
www.cio.com/research/security

Specific Documents
Practices for Protecting Information Resources Assets
Texas Dept. of Information Resources
www.dir.state.tx.us/IRAPC/practices/index.html

Handbook for Computer Security Incident Response Teams
Carnegie Mellon University
www.sei.cmu.edu/pub/documents/98.reports/pdf/98hb001.pdf

Minimizing Your Potential Vulnerability and Enhancing Effective Response
NIPC
www.nipc.gov/incident/incident3.htm

Sample Incident Handling Procedure
www.csirt.ws/docs/incident.handling.pro.doc

Best Practices for Seizing Electronic Evidence
A Joint Project of the International Association of Chiefs of Police and the U.S. Secret Service
www.treas.gov/usss/electronic_evidence.htm

Reprinted through the courtesy of CIO. Copyright © 2003 CXO Media, Inc. ALL RIGHTS RESERVED.

FBI & USSS FIELD OFFICES

TELEPHONE/FAX
ADDRESS

ALABAMA
Birmingham
FBI 205.326.6166/205.715.0232
2121 8th Avenue N.
Birmingham, AL 35203-2396
USSS 205.731.1144/205.731.0007
Daniel Building
15 South 20th Street, Suite 1125
Birmingham, AL 35233
Mobile
FBI 334.438.3674/251.415.3235
One St. Louis Centre
1 St. Louis Street, 3rd Floor
Mobile, AL 36602-3930
USSS 334.441.5851/334.441.5250
Parkview Office Building
182 St. Francis Street
Mobile, AL 36602
Montgomery
USSS 334.223.7601/334.223.7523
Colonial Financial Center
1 Commerce Street, Suite 605
Montgomery, AL 36104

ALASKA
Anchorage
FBI 907.276.4441/907.265.9599
101 East Sixth Avenue
Anchorage, AK 99501-2524
USSS 907.271.5148/907.271.3727
Federal Building & U.S. Courthouse
222 West 7th Avenue, Room 559
Anchorage, AK 99513

ARIZONA
Phoenix
FBI 602.279.5511/602.650.3024
201 East Indianola Avenue, Suite 400
Phoenix, AZ 85012-2080
USSS 602.640.5580/602.640.5505
3200 North Central Avenue, Suite 1450
Phoenix, AZ 85012
Tucson
USSS 520.670.4730/520.670.4826
300 West Congress Street, Room 4-V
Tucson, AZ 85701

ARKANSAS
Little Rock
FBI 501.221.9100/501.228.8509
24 Shackleford West Boulevard
Little Rock, AR 72211-3755
USSS 501.324.6241/501.324.6097
111 Center Street, Suite 1700
Little Rock, AR 72201-4419

CALIFORNIA
Fresno
USSS 209.487.5204/559.487.5013
5200 North Palm Avenue, Suite 207
Fresno, CA 93704
Los Angeles
FBI 310.477.6565/310.996.3359
Federal Office Building
11000 Wilshire Boulevard, Suite 1700
Los Angeles, CA 90024-3672
USSS 213.894.4830/213.894.2948
Roybal Federal Building
255 East Temple Street, 17th Floor
Los Angeles, CA 90012
Riverside
USSS 909.276.6781/909.276.6637
4371 Latham Street, Suite 203
Riverside, CA 92501
Sacramento
FBI 916.481.9110/916.977.2300
4500 Orange Grove Avenue
Sacramento, CA 95841-4205
USSS 916.930.2130/916.930.2140
501 I Street, Suite 9500
Sacramento, CA 95814-2322
San Diego
FBI 858.565.1255/858.499.7991
Federal Office Building
9797 Aero Drive
San Diego, CA 92123-1800
USSS 619.557.5640/619.557.6658
550 West C Street, Suite 660
San Diego, CA 92101
San Francisco
FBI 415.553.7400/415.553.7674
450 Golden Gate Avenue, 13th Floor
San Francisco, CA 94102-9523
USSS 415.744.9026/415.744.9051
345 Spear Street
San Francisco, CA 94105
San Jose
USSS 408.535.5288/408.535.5292
U.S. Courthouse & Federal Building
280 S. First Street, Suite 2050
San Jose, CA 95113
Santa Ana
USSS 714.246.8257/714.246.8261
200 W. Santa Ana Boulevard,
Suite 500
Santa Ana, CA 92701-4164
Ventura
USSS 805.339.9180/805.339.0015
5500 Telegraph Road, Suite 161
Ventura, CA 93003

COLORADO
Colorado Springs
USSS 719.632.3325/719.632.3341
212 N. Wahsatch, Room 204
Colorado Springs, CO 80903
Denver
FBI 303.629.7171/303.628.3085
1961 Stout Street, 18th Floor
Denver, CO 80294-1823
USSS 303.866.1010/303.866.1934
1660 Lincoln Street
Denver, CO 80264

CONNECTICUT
New Haven
FBI 203.777.6311/203.503.5098
600 State Street
New Haven, CT 06511-6505
USSS 203.865.2449/203.865.2525
265 Church Street, Suite 1201
New Haven, CT 06510

DELAWARE
Wilmington
USSS 302.573.6188/302.573.6190
One Rodney Square
920 King Street, Suite 414
Wilmington, DE 19801

DISTRICT OF COLUMBIA
Washington, D.C.
FBI (HDQRS.)
202.278.2000/202.278.2478
601 4th Street NW
Washington, D.C. 20535-0002
USSS 202.406.8000/202.406.8803
1100 L Street NW, Suite 6000
Washington, D.C. 20005
USSS (HDQRS.)
202.406.5850/202.406.5031
950 H Street NW
Washington, D.C. 20223

FLORIDA
Jacksonville
FBI 904.721.1211/904.727.6242
7820 Arlington Expressway
Jacksonville, FL 32211-7499
USSS 904.296.0133/904.296.0188
7820 Arlington Expressway,
Suite 500
Jacksonville, FL 32211
Miami
FBI 305.944.9101/305.787.6538
16320 NW Second Avenue
North Miami Beach, FL 33169-6508
USSS 305.629.1800/305.629.1830
8375 NW 53rd Street
Miami, FL 33166
Orlando
USSS 407.648.6333/407.648.6606
135 West Central Boulevard,
Suite 670
Orlando, FL 32801
Tallahassee
USSS 850.942.9523/850.942.9526
Building F
325 John Knox Road
Tallahassee, FL 32303
Tampa
FBI 813.273.4566/813.272.8019
Federal Office Building
500 Zack Street, Room 610
Tampa, FL 33602-3917
USSS 813.228.2636/813.228.2618
501 East Polk Street, Room 1101
Tampa, FL 33602
West Palm Beach
USSS 561.659.0184/561.655.8484
505 South Flagler Drive
West Palm Beach, FL 33401

GEORGIA
Albany
USSS 229.430.8442/229.430.8441
Albany Tower
235 Roosevelt Avenue, Suite 221
Albany, GA 31702
Atlanta
FBI 404.679.9000/404.679.6289
2635 Century Parkway Northeast,
Suite 400
Atlanta, GA 30345-3112
USSS 404.331.6111/404.331.5058
401 West Peachtree Street, Suite 2906
Atlanta, GA 31702
Savannah
USSS 912.652.4401/912.652.4062
33 Bull Street
Savannah, GA 31401

HAWAII
Honolulu
FBI 808.566.4300/808.566.4470
Kalanianaole Federal Office Building
300 Ala Moana Boulevard, Room 4-230
Honolulu, HI 96850-0053
USSS 808.541.1912/808.545.4490
Kalanianaole Federal Office Building
300 Ala Moana Boulevard, Room 6-210
Honolulu, HI 96850

IDAHO
Boise
USSS 208.334.1403/208.334.1289
Federal Building - U.S. Courthouse
550 West Fort Street, Room 730
Boise, ID 83724-0001

ILLINOIS
Chicago
FBI 312.421.4310/312.786.2525
E.M. Dirksen Federal Office Building
219 South Dearborn Street, Room 905
Chicago, IL 60604-1702
USSS 312.353.5431/312.353.1225
Gateway IV Building
300 S. Riverside Plaza, Suite 1200 North
Chicago, IL 60606
Springfield
FBI 217.522.9675/217.535.4440
400 West Monroe Street, Suite 400
Springfield, IL 62704-1800
USSS 217.492.4033/217.492.4680
400 West Monroe Street, Suite 301
Springfield, IL 62704

Reprinted through the courtesy of CIO. Copyright © 2003 CXO Media, Inc. ALL RIGHTS RESERVED.

FBI & USSS FIELD OFFICES

TELEPHONE/FAX
ADDRESS

INDIANA
Evansville
USSS 812.985.9502/812.985 9504
P.O. Box 530
Newburgh, IN 47630
Indianapolis
FBI 317.639.3301/317.321 6193
Federal Office Building
575 N. Pennsylvania Street,
Room 679
Indianapolis, IN 46204-1585
USSS 317.226.6444/317.226.5494
Federal Office Building
575 N. Pennsylvania Street,
Suite 211
Indianapolis, IN 46204-1585
South Bend
USSS 219.273.3140/219.271.9301
P.O. Box 477
South Bend, IN 46625

IOWA
Des Moines
USSS 515 284 4565/515.284 4566
210 Walnut Street, Suite 637
Des Moines, IA 50309-2107

KANSAS
Wichita
USSS 316.269.6694/316.269 6154
Epic Center
301 N. Main Street, Suite 275
Wichita, KS 67202

KENTUCKY
Lexington
USSS 859.223 2358/859.223 1819
3141 Beaumont Centre Circle
Lexington, KY 40513
Louisville
FBI 502.583.3941/502 569.3869
Federal Building
600 Martin Luther King Jr Place,
Room 500
Louisville, KY 40202-2231
USSS 502 582 5171/502 582 6329
Federal Building
600 Martin Luther King Jr Place
Room 377
Louisville, KY 40202-2231

LOUISIANA
Baton Rouge
USSS 225 389 0763/225 389 0325
One American Place, Suite 1502
Baton Rouge, LA 70825
New Orleans
FBI 504.816 3000/504 816.3306
2901 Leon C Simon Drive
New Orleans, LA 70126
USSS 504 589 4041/504 589 6013
Hale Boggs Federal Building
501 Magazine Street
New Orleans, LA 70130
Shreveport
USSS 318.676.3500/318 676.3502
401 Edwards Street
Shreveport, LA 71101

MAINE
Portland
USSS 207.780.3493/207.780.3301
100 Middle Street
West Tower, 2nd Floor
Portland, ME 04101

MARYLAND
Baltimore
FBI 410.265.8080/410.281.0339
7142 Ambassador Road
Baltimore, MD 21244-2754
USSS 410.962.2200/410.962.0840
100 S. Charles Street, 11th Floor
Baltimore, MD 21201
Eastern Shore
USSS 410.268 7286/410.268.7903
U.S. Naval Academy
Police Dept., Headquarters Building 257,
Room 221
Annapolis, MD 21402
Frederick
USSS 301.293.6434/301.694 8078
Rowley Training Center
9200 Powder Mill Road, Route 2
Laurel, MD 20708

MASSACHUSETTS
Boston
FBI 617.742.5533/617.223.6327
One Center Plaza, Suite 600
Boston, MA 02108
USSS 617.565 5640/617.565.5659
Thomas P. O'Neill Jr. Federal Building
10 Causeway Street
Boston, MA 02222

MICHIGAN
Detroit
FBI 313.965.2323/313.237 4009
Patrick V. McNamara Building
477 Michigan Avenue, 26th Floor
Detroit, MI 48226
USSS 313.226.6400/313.226.3952
Patrick V. McNamara Building
477 Michigan Avenue
Detroit, MI 48226
Grand Rapids
USSS 616.454.4671/616 454 5816
330 Ionia Avenue NW, Suite 302
Grand Rapids, MI 490503-2350
Saginaw
USSS 989.752 8076/989.752.8048
301 E. Genesee, Suite 200
Saginaw, MI 48607

MINNESOTA
Minneapolis
FBI 612.376.3200/612.376.3249
111 Washington Avenue South,
Suite 1100
Minneapolis, MN 55401-2176
USSS 612.348.1800/612.348.1807
U.S. Courthouse
300 South 4th Street, Suite 750
Minneapolis, MN 55415

MISSISSIPPI
Jackson
FBI 601.948.5000/601.360.7550
Federal Building
100 West Capitol Street
Jackson, MS 39269-1601
USSS 601.965.4436/601.965.4012
Federal Building
100 West Capitol Street, Suite 840
Jackson, MS 39269

MISSOURI
Kansas City
FBI 816.512.8200/816.512.8545
1300 Summit
Kansas City, MO 64105-1362
USSS 816.460.0600/816.283.0321
1150 Grand Avenue, Suite 510
Kansas City, MO 64106
Springfield
USSS 417.864.8340/417.864.8676
901 St. Louis Street, Suite 306
Springfield, MO 65806
St. Louis
FBI 314.231.4324/314.589.2636
222 Market Street
St. Louis, MO 63103-2516
USSS 314.539.2238/314.539.2567
Thomas F. Eagleton U.S. Courthouse
111 S. 10th Street, Suite 11.346
St. Louis, MO 63102

MONTANA
Great Falls
USSS 406.452.8515/406.761.2316
11 Third Street North
Great Falls, MT 59401

NEBRASKA
Omaha
FBI 402.493.8688/402.492.3799
10755 Burt Street
Omaha, NE 68114-2000
USSS 402.965.9670/402.445.9638
2707 North 108 Street, Suite 301
Omaha, NE 68164

NEVADA
Las Vegas
FBI 702.385.1281/702.385.1281
John Lawrence Bailey Building
700 East Charleston Boulevard
Las Vegas, NV 89104-1545
USSS 702.388.6571/702.388.6668
600 Las Vegas Boulevard South,
Suite 600
Las Vegas, NV 89101
Reno
USSS 775.784.5354/775.784.5991
100 West Liberty Street, Suite 850
Reno, NV 89501

NEW HAMPSHIRE
Manchester
USSS 603.626.5631/603.626.5653
1750 Elm Street, Suite 802
Manchester, NH 03104

NEW JERSEY
Atlantic City
USSS 609.487.1300/609.487.1491
Ventnor Professional Campus
6601 Ventnor Avenue
Ventnor City, NJ 08406
Newark
FBI 973.792.3000/973.792.3035
1 Gateway Center, 22nd Floor
Newark, NJ 07102-9889
USSS 973.656.4500/973.984.5822
Headquarters Plaza, West Towers,
Speedwell Avenue, Suite 700
Morristown, NJ 07960
Trenton
USSS 609.989.2008/609.989.2174
402 East State Street, Suite 3000
Trenton, NJ 08608

NEW MEXICO
Albuquerque
FBI 505.224.2000/505 224.2276
415 Silver Avenue SW, Suite 300
Albuquerque, NM 87102
USSS 505.248 5290/505.248.5296
505 Marquette Street NW
Albuquerque, NM 87102

Reprinted through the courtesy of CIO. Copyright © 2003 CXO Media, Inc. ALL RIGHTS RESERVED.

FBI & USSS FIELD OFFICES

TELEPHONE/FAX
ADDRESS

NEW YORK

Albany
FBI 518.465.7551/518.431.7463
200 McCarty Avenue
Albany, NY 12209
USSS 518.436.9600/518.436.9635
39 North Pearl Street, 2nd Floor
Albany, NY 12207

Buffalo
FBI 716.856.780/716.843.5288
One FBI Plaza
Buffalo, NY 14202-2698
USSS 716.551.4401/716.551.5075
610 Main Street, Suite 300
Buffalo, NY 14202

JFK
USSS 718.553.0911/718.553.7626
John F. Kennedy Int'l. Airport
Building 75, Room 246
Jamaica, NY 11430

Melville
USSS 631.249.0404/631.249.0991
35 Pinelawn Road
Melville, NY 11747

New York
FBI 212.384.1000/212.384.2745
or 2746
26 Federal Plaza, 23rd Floor
New York, NY 10278-0004
USSS 212.637.4500/212.637.4687
335 Adams Street, 32nd Floor
Brooklyn, NY 11201

Rochester
USSS 716.263.6830/716.454.2753
Federal Building
100 State Street, Room 606
Rochester, NY 14614

Syracuse
USSS 315.448.0304/315 448.0302
James Hanley Federal Building
100 S. Clinton Street, Room 1371
Syracuse, NY 13261

White Plains
USSS 914.682.6300/914.682.6182
140 Grand Street, Suite 300
White Plains, NY 10601

NORTH CAROLINA

Charlotte
FBI 704.377.9200/704.331.4595
Wachovia Building
400 South Tyron Street, Suite 900
Charlotte, NC 28285-0001
USSS 704.442.8370/704.442.8369
One Fairview Center
6302 Fairview Road
Charlotte, NC 28210

Greensboro
USSS 336.547.4180/336.547.4185
4905 Koger Boulevard, Suite 220
Greensboro, NC 27407

Raleigh
USSS 919.790.2834/919.790.2832
4407 Bland Road, Suite 210
Raleigh, NC 27609

Wilmington
USSS 910.815.4511/910.815.4521
One Rodney Square
920 King Street, Suite 414
Wilmington, DE 19801

NORTH DAKOTA

Fargo
USSS 701.239.5070/701.239.5071
657 2nd Avenue North, Suite 302A
Fargo, ND 58102

OHIO

Cincinnati
FBI 513.421.4310/513.562.5650
John Weld Peck Federal Building
550 Main Street, Room 9000
Cincinnati, OH 45202-8501
USSS 513.684.3585/513.684.3436
John Weld Peck Federal Building
550 Main Street
Cincinnati, OH 45202

Cleveland
FBI 216.522.1400/216.622.6717
Federal Office Building
1240 East 9th Street, Room 3005
Cleveland, OH 44199-9912
USSS 216.706.4365/216.706 4445
6100 Rockside Woods Boulevard
Suite 440
Cleveland, OH 44131-2334

Columbus
USSS 614.469.7370/614.469.2049
500 South Front Street, Suite 800
Columbus, OH 43215

Dayton
USSS 937.225.2900/937.225.2724
Federal Building
200 West Second Street, Room 811
Dayton, OH 45402

Toledo
USSS 419.259.6434/419.259.6437
4 Seagate Center, Suite 702
Toledo, OH 43604

OKLAHOMA

Oklahoma City
FBI 405.290.7770/405.290.3885
3301 West Memorial Drive
Oklahoma City, OK 73134
USSS 405.810.3000/405.810 3098
Lakepoint Towers
4013 NW Expressway, Suite 650
Oklahoma City, OK 73116

Tulsa
USSS 918.581.7272
Pratt Tower
125 West 15th Street Suite 400
Tulsa, OK 74119

OREGON

Portland
FBI 503.224.4181/503.552.5400
Crown Plaza Building
1500 SW 1st Avenue, Suite 400
Portland, OR 97201-5828
USSS 503.326.2162/503.326.3258
1001 SW 5th Avenue, Suite 1020
Portland, OR 97204

PENNSLYVANIA

Philadelphia
FBI 215.418.4000/215.418.4232
William J. Green Jr. Federal
Office Building
600 Arch Street, 8th Floor
Philadelphia, PA 19106
USSS 215.861.3300/215.861.3311
7236 Federal Building
600 Arch Street
Philadelphia, PA 19106

Pittsburgh
FBI 412.471.2000/412.432.4188
U.S. Post Office Building
700 Grant Street, Suite 300
Pittsburgh, PA 15219-1906
USSS 412.395.6484/412.395.6349
1000 Liberty Avenue
Pittsburgh, PA 15222

Scranton
USSS 570.346.5781/570.346.3003
235 N. Washington Avenue, Suite 247
Scranton, PA 18501

RHODE ISLAND

Providence
USSS 401.331.6456/401.528.4394
The Federal Center
380 Westminster Street, Suite 343
Providence, RI 02903

SOUTH CAROLINA

Charleston
USSS 843.747.7242/843.747.7787
5900 Core Avenue, Suite 500
North Charleston, SC 29406

Columbia
FBI 803.551.4200/803.551.4324
151 Westpark Boulevard
Columbia, SC 29210-3857
USSS 803.765.5446/803.765.5445
1835 Assembly Street, Suite 1425
Columbia, SC 29201

Greenville
USSS 864.233.1490/864.235.6237
NCNB Plaza
7 Laurens Street, Suite 508
Greenville, SC 29601

SOUTH DAKOTA

Sioux Falls
USSS 605.330.4565/605.330.4523
230 South Phillips Avenue, Suite 405
Sioux Falls, SD 57104

TENNESSEE

Chattanooga
USSS 423.752.5125/423.752.5130
Post Office Building
900 Georgia Avenue, Room 204
Chattanooga, TN 37402

Knoxville
FBI 865.544.0751/865.544.3590
John J. Duncan Federal Office Building
710 Locust Street, Suite 600
Knoxville, TN 37902-2537
USSS 865.545.4627/865.545 4633
John J. Duncan Federal Office Building
710 Locust Street, Room 517
Knoxville, TN 37902

Memphis
FBI 901.747.4300/901.747.9621
Eagle Crest Building
225 North Humphreys Boulevard,
Suite 3000
Memphis, TN 38120-2107
USSS 901.544.0333/901.544.0342
5350 Poplar Avenue, Suite 204
Memphis, TN 38119

Nashville
USSS 615.736.5841/615.736.5848
658 U.S. Courthouse
801 Broadway Street
Nashville, TN 37203

Reprinted through the courtesy of CIO. Copyright © 2003 CXO Media, Inc. ALL RIGHTS RESERVED.

FBI & USSS FIELD OFFICES

TELEPHONE/FAX
ADDRESS

TEXAS
Austin
USSS 512.916.5103/512.916.5365
Federal Office Building
300 E. 8th Street
Austin, TX 78701
Dallas
FBI 214.720.2200/214.922.7459
1801 North Lamar, Suite 300
Dallas, TX 75202-1795
USSS 972.868.3200/972.868.3232
125 East John W. Carpenter Freeway,
Suite 300
Irving, TX 75062
El Paso
FBI 915.832.5000/915.832.5259
660 S. Mesa Hills Drive
El Paso, TX 79912
USSS 915.533.6950/915.533.8646
Mesa One Building
4849 North Mesa, Suite 210
El Paso, TX 79912
Houston
FBI 713.693.5000/713.693.3999
2500 East TC Jester
Houston, TX 77008-1300
USSS 713.868.2299/713.868.5093
602 Sawyer Street, Suite 500
Houston, TX 77007
Lubbock
USSS 806.472.7347/806.472.7542
1205 Texas Avenue, Room 813
Lubbock, TX 79401
McAllen
USSS 956.630.5811/956.630.5838
200 S. 10th Street, Suite 1107
McAllen, TX 78501
San Antonio
FBI 210.225.6741/210.978.5380
U.S. Post Office Building
615 East Houston Street, Suite 200
San Antonio, TX 78205-9998
USSS 210.472.6175/210.472.6185
727 East Durango Boulevard,
Suite B410
San Antonio, TX 78206-1265
Tyler
USSS 903.534.2933/903.581.9569
6101 South Broadway, Suite 395
Tyler, TX 75703

UTAH
Salt Lake City
FBI 801.579.1400/801.579.4500
257 Towers Building
257 East 200 South, Suite 1200
Salt Lake City, UT 84111-2048
USSS 801.524.5910/801.524.6216
57 West 200 South Street, Suite 450
Salt Lake City, UT 84101

VERMONT
FBI 518.465.7551/518.431.7463
Contact field office located in
Albany, NY
USSS 617.565.5640/617.565.5659
Contact field office located in
Boston, MA

VIRGINIA
Norfolk
FBI 757.455.0100/757.455.2647
150 Corporate Boulevard
Norfolk, VA 23502-4999
USSS 757.441.3200/757.441.3811
Federal Building
200 Granby Street, Suite 640
Norfolk, VA 23510
Richmond
FBI 804.261.1044/804.627.4494
1970 East Parham Road
Richmond, VA 23228
USSS 804.771.2274/804.771.2076
600 East Main Street, Suite 1910
Richmond, VA 23219
Roanoke
USSS 540.345.4301/540.857.2151
105 Franklin Road SW, Suite 2
Roanoke, VA 24011

WASHINGTON
Seattle
FBI 206.622.0460/206.262.2587
1110 Third Avenue
Seattle, WA 98101
USSS 206.220.6800/206.220.6479
890 Federal Building
915 Second Avenue
Seattle, WA 98174
Spokane
USSS 509.353.2532/509.353.2871
601 W. Riverside Avenue, Suite 1340
Spokane, WA 99201

WEST VIRGINIA
Charleston
USSS 304.347.5188/304.347.5187
5900 Core Avenue, Suite 500
North Charleston, SC 29406

WISCONSIN
Madison
USSS 608.264.5191/608.264.5592
131 W. Wilson Street, Suite 303
Madison, WI 53703
Milwaukee
FBI 414.276.4684/414.276.6560
330 East Kilbourn Avenue
Milwaukee, WI 53202
USSS 414.297.3587/414.297.3595
572 Courthouse
517 E. Wisconsin Avenue
Milwaukee, WI 53202

WYOMING
Cheyenne
USSS 307.772.2380/307.772.2387
2120 Capitol Avenue, Suite 3026
Cheyenne, WY 82001

The U.S. Secret Service notes that the Electronic Crimes Branch of the USSS Headquarters in Washington, D.C., is ready to field questions and/or accept computer intrusion reports. Tel: (202) 406-5850. Fax: (202) 406-5031. Online: www.treas.gov/usss.

The FBI notes computer intrusion reports may also be submitted to the National Infrastructure Protection Center. Tel: (202) 323-3205; (888) 585-9078. Fax: (202) 323-2079. Email: nipc.watch@fbi.gov. Online: www.nipc.gov/incident/cirr.htm.

Additional investigative programs may exist within your local law enforcement community (i.e., city, county or state police, district attorney investigative units, and/or state attorney generals' offices).

Reprinted through the courtesy of CIO. Copyright © 2003 CXO Media, Inc. ALL RIGHTS RESERVED.

CIO CYBERTHREAT REPORT FORM

This form outlines the basic information law enforcement needs on a first call. You can use it as an internal worksheet or fill it out and e-mail or fax it to law enforcement. Additional data that will help agents in their investigation is outlined in the CIO Cyberthreat Response & Reporting Guidelines, but the best way to determine what will be most helpful to investigators in the event of an attack is to ask.

STATUS

☐ Site Under Attack ☐ Past Incident ☐ Repeated Incidents, unresolved

CONTACT INFORMATION

Name_____ Title_____

Organization_____

Direct-Dial Phone_____ E-mail_____

Legal Contact Name_____ Phone_____

Location/Site(s) Involved_____

Street Address_____

City_____ State_____ IP_____

Main Telephone_____ Fax_____

ISP Contact Information_____

INCIDENT DESCRIPTION

☐ Denial of Service
☐ Distributed Denial of Service
☐ Malicious Code (virus, worm)
☐ Intrusion/Hack
☐ Unauthorized Electronic Monitoring (sniffers)
☐ Misuse of Systems (internal or external)
☐ Website Defacement
☐ Probe/Scan
☐ Other (specify)_____

DATE/TIME OF INCIDENT DISCOVERY

Date_____ Time_____

Duration of Attack_____

IMPACT OF ATTACK

☐ Loss/Compromise of Data
☐ System Downtime
☐ Damage to Systems
☐ Financial Loss (estimated amount: >$_____)
☐ Damage to the Integrity or Delivery of Critical Goods, Services or Information
☐ Other Organizations' Systems Affected

SEVERITY OF ATTACK, INCLUDING FINANCIAL LOSS, INFRASTRUCTURE, PR IMPACT IF MADE PUBLIC

☐ High ☐ Medium ☐ Low ☐ Unknown

SENSITIVITY OF DATA

☐ High ☐ Medium ☐ Low ☐ Unknown

How did you detect this?_____

Have you contacted law enforcement about this incident before? Who & when?_____

Has the incident been resolved? Explain_____

Reprinted through the courtesy of CIO. Copyright © 2003 CXO Media, Inc. ALL RIGHTS RESERVED.

CONTRIBUTORS

INDUSTRY

Peter Allor
Manager, ISAC Operations
Special Operations Group, X-Force
Internet Security Systems, Inc.

Bruce Moulton
Past Chairman & Current Advisor
Financial Services ISAC

John Puckett
VP and General Manager, Wireless and Internet Technologies
Polaroid Corp.

Howard Schmidt
Vice Chair
President's Critical Infrastructure Board and former Chief Security Officer
Microsoft Corp.

Alan Sonnenberg
Senior Director/Engineering and Security, Wireless and Internet Technologies
Polaroid Corp.

Michael Young
Principal & Chief Information Security Officer
State Street Global Advisors

UNITED STATES LAW ENFORCEMENT

Steven Chabinsky
Principal Legal Advisor, National Infrastructure Protection Center & Assistant General Counsel, Office of the General Counsel, *FBI*

Steve Colo
Assistant Director
U.S. Secret Service

Ronald L. Dick
Director, National Infrastructure Protection Center &
Deputy Assistant Director, Counterterrorism Division, *FBI*

Paul Irving
Assistant Director for Government and Public Affairs
U.S. Secret Service

James Savage
Deputy Special Agent in Charge
U.S. Secret Service
Financial Crimes Division

Bruce A. Townsend
Special Agent in Charge
U.S. Secret Service
Financial Crimes Division

CXO MEDIA

Abbie Lundberg
Editor in Chief,
CIO *Magazine*

Lori Piscatelli
News & Information Assistant

Susan Watson
VP, News & Information

ADDITIONAL REVIEWERS

Steven Agnoli
CIO
Kirkpatrick & Lockhart LLP

William Crowell
Former CIO
Meredith Corp.

Patrick Gray
Manager, Internet Threat Intelligence Center
Special Operations Group, X-Force
Internet Security Systems, Inc.

Scott Hicar
CIO
Maxtor Corp.

Paul Ingevaldson
SVP, Technology and International Operations
Ace Hardware

Scott Kelly
VP of IT
Symtx

Frank O'Connor
CIO
ECom Systems, Inc.

Steven Steinbrecher
CIO
Contra Costa County

Glenn West
Vice President, IT Services
Long John Silvers

Marc West
CIO
Electronic Arts

Ed Winfield
CIO
FX Coughlin Co.

Reprinted through the courtesy of CIO. Copyright © 2003 CXO Media, Inc. ALL RIGHTS RESERVED.

Kruse and Heiser

In their book *Computer Forensics, Incident Response Essentials*, Kruse and Heiser have included an appendix that provides details on "Internet Data Incident Response Guidelines" [Kruse 02]. They cover the goals of incident response, roles and responsibilities of staff involved in incident response, an incident severity chart, and information on incident handling processes. They have provided several process flow charts for handling different types of incident activity (Figures A-10, A-11, and A-12, pages 347, 348, and 349), a few of which have been reproduced here. Appendix B provides an Incident Response Form template (pages 353-361), which has also been included here.

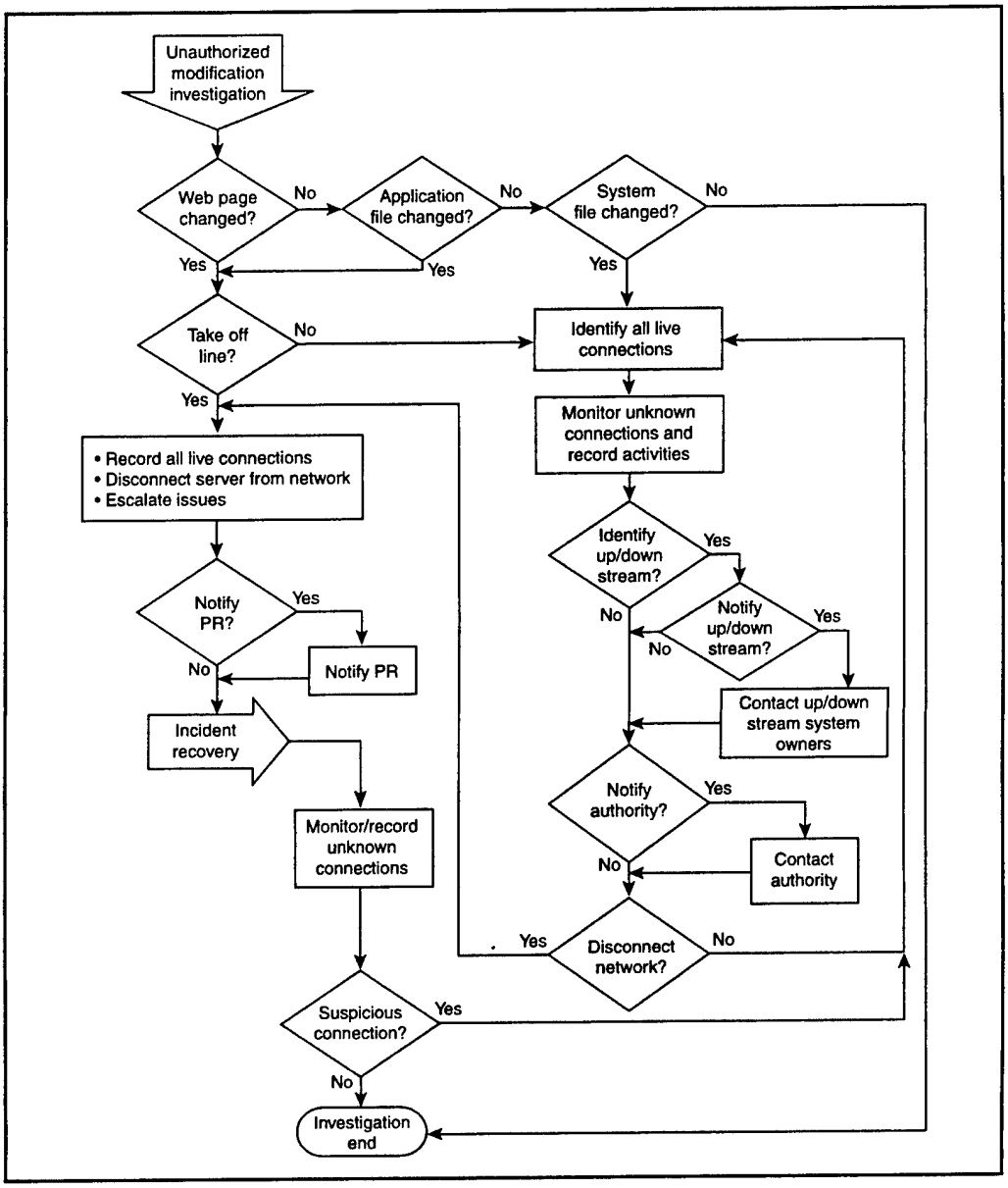


Figure A-10 Process for handling unauthorized modification

Because probing by itself does not pose any direct threat to the target machine and can be easily filtered, no special action is needed to prevent this type of incident. However, it is a good practice to record all detected probing incidents to develop some recognizable patterns as a baseline.

Reprinted with permission of the author (Kruse).
Copyright © 2001. For more information, see <http://www.awl.com/cseng>.

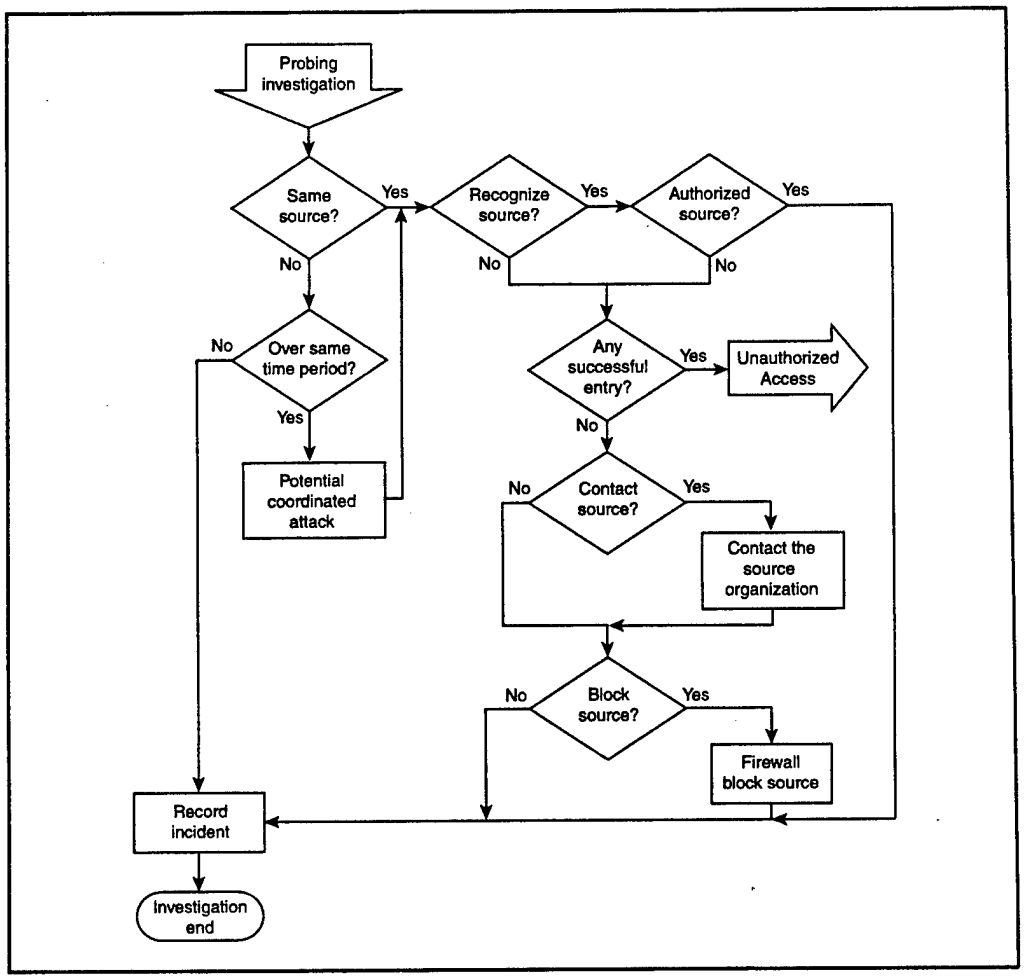


Figure A-11 Process for handling network probing

Recovery

At the recovery stage, the security incident investigation is completed. The flowchart in Figure A-12 depicts the process.

Lessons Learned and Recommendations

The ERCT is responsible for conducting a post mortem session after the system is back to normal to collect the lessons learned. The session should identify weaknesses in the process and suggest areas of improvement. Participants are not limited to the ERCT members, and the meeting is led by the SI.

Reprinted with permission of the author (Kruse).
Copyright © 2001. For more information, see <http://www.awl.com/cseng>.

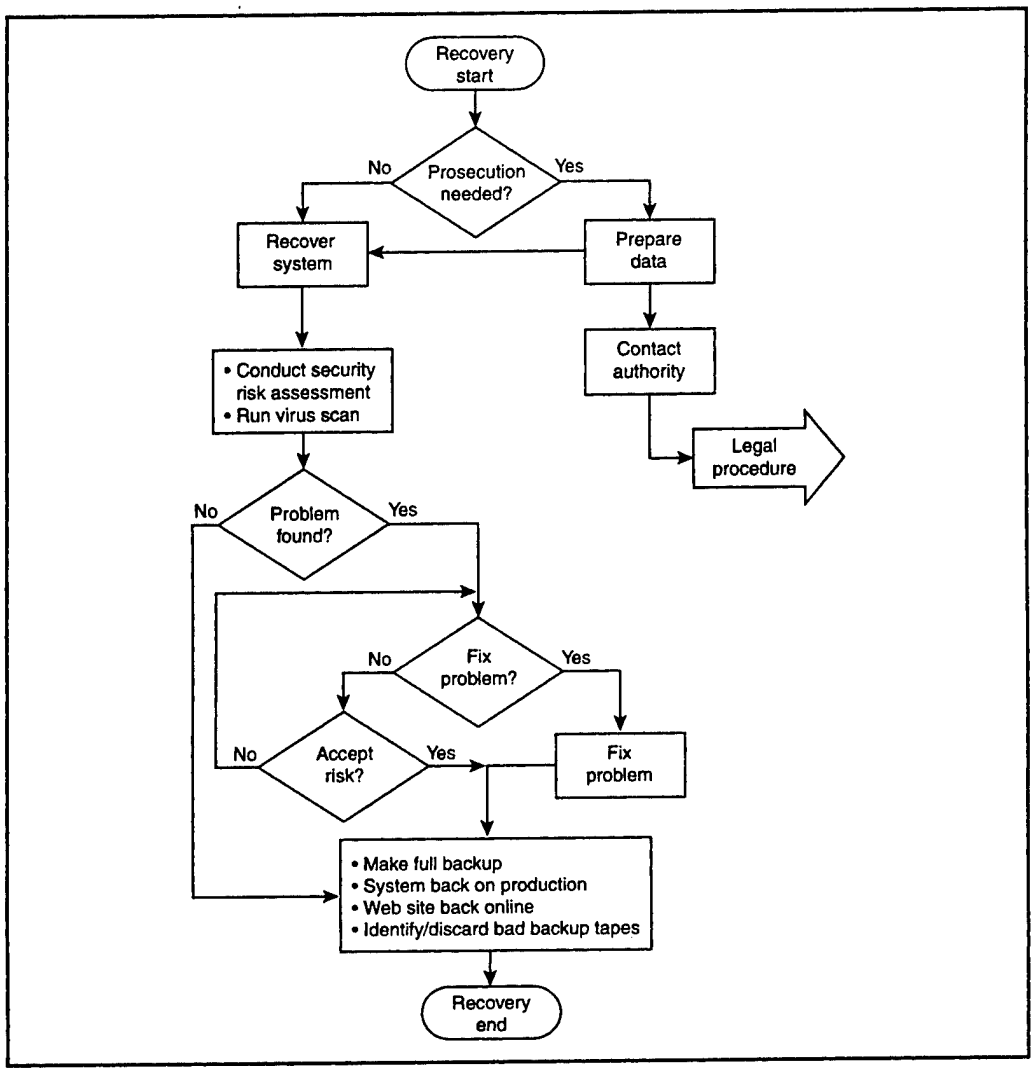


Figure A-12 Process for completing incident recovery

Conclusion

Security incidents will occur regardless of how much effort is devoted to preventing them. When an incident happens, the first priority is to limit the additional damage. The best way to achieve that goal is by preparing for incidents. This guideline must be understood and followed by all personnel involved in all data center applications and servers.

Reprinted with permission of the author (Kruse).
Copyright © 2001. For more information, see <http://www.awl.com/cseng>.

Appendix

B

Incident Response Form

General Data Requested for All Incident Types

- ❑ Site under attack
- ❑ Incident investigation in progress
- ❑ Incident closed

What assistance do you require:

- ❑ Immediate call
- ❑ None needed at this time
- ❑ Follow-up on all affected sites
- ❑ Contact the "hacking" sites

Site involved (name and acronym): _____

Point of contact for incident:

Name _____

- Email address _____
- 7x24 contact information _____

Alternative point of contact for incident:

Name _____

- Email address _____
- 7x24 contact information _____

Type of incident (provide additional details on the appropriate form):

- ❑ Malicious code: virus, Trojan horse, worm
- ❑ Probes/scans (nonmalicious data gathering—recurring, massive, unusual)

Reprinted with permission of the author (Kruse).
Copyright © 2001. For more information, see <http://www.awl.com/cseng>.

- ❑ Attack (successful/unsuccessful intrusions including scanning with attack packets)
- ❑ Denial-of-service event
- ❑ High embarrassment factor
- ❑ Deemed significant by site

Date and time incident occurred (specify time zone): _____

A summary of what occurred: _____

_____

_____

Type of service, information, or project compromised (please provide specifics):

- ❑ Sensitive unclassified such as privacy, proprietary, or source selection

  _____

- ❑ Other unclassified _____

Damage done:

- Numbers of systems affected _____
- Nature of loss, if any _____
- System down time _____
- Cost of incident (for example, unknown, none, <$10K, $10K–$50K, >$50K)

Name of other sites contacted:

Law enforcement _____

Other _____

Details for Malicious Code

Apparent source:

- ❑ Diskette, CD, etc.
- ❑ Email attachment
- ❑ Software download

Primary system or network involved:

- IP addresses or subnet addresses _____
- OS versions _____

Reprinted with permission of the author (Kruse).
Copyright © 2001. For more information, see <http://www.awl.com/cseng>.

- NOS versions _____
- Other _____

Other affected systems or networks (IPs and OSs): _____

_____

_____

Type of malicious code (include name if known):

- ❑ Virus _____
- ❑ Trojan horse _____
- ❑ Worm _____
- ❑ Joke program _____
- ❑ Other _____
- ❑ Copy sent to:
  - _____
  - _____
  - _____

Method of operation (for new malicious code):

- ❑ Type—macro, boot, memory resident, polymorphic, self-encrypting, stealth
- ❑ Payload
- ❑ Software infected
- ❑ Files erased, modified, deleted, encrypted—any special significance to these files
- ❑ Self-propagating via email
- ❑ Detectable changes
- ❑ Other features

Details: _____

_____

_____

How detected: _____

_____

_____

Reprinted with permission of the author (Kruse).
Copyright © 2001. For more information, see <http://www.awl.com/cseng>.

Remediation (actions taken to return the systems to trusted operation):

- ❑ Antivirus product obtained, updated, or installed for automatic operation
- ❑ New policy established on use of email attachments
- ❑ Firewall, routers, or email servers updated to detect and scan attachments

Details: _____

_____

_____

Additional comments: _____

_____

_____

Details for Probes and Scans

Apparent source:

- IP address _____
- Host name _____
- Location of attacking host:
  - ❑ Domestic
  - ❑ Foreign
  - ❑ Insider

Primary systems/networks involved:

- IP addresses or subnet addresses _____
- OS versions _____
- NOS versions _____

Other affected systems or networks (IPs and OSs): _____

_____

_____

Method of operation:

- ❑ Ports probed/scanned
- ❑ Order of ports or IP addresses scanned
- ❑ Probing tool
- ❑ Anything that makes this probe unique

Reprinted with permission of the author (Kruse).
Copyright © 2001. For more information, see <http://www.awl.com/cseng>.

Details: _____

_____

_____

How detected:

- ❑ Another site
- ❑ Incident response team
- ❑ Log files
- ❑ Packet sniffer
- ❑ Intrusion detection system
- ❑ Anomalous behavior
- ❑ User

Details: _____

_____

_____

Log file excerpts: _____

_____

_____

Additional Comments: _____

_____

_____

Details for Unauthorized Access

Apparent source:

- IP address
- Location of host:
  - ❑ Domestic
  - ❑ Foreign
  - ❑ Insider

Primary systems involved:

- IP addresses or subnet addresses _____
- OS versions _____
- NOS versions _____

Reprinted with permission of the author (Kruse).
Copyright © 2001. For more information, see <http://www.awl.com/cseng>.

Other affected systems or networks (IPs and OSs): _____

_____

_____

Avenue of attack:

- ❑ Sniffed/guessed/cracked password
- ❑ Trusted host access
- ❑ Vulnerability exploited
- ❑ Hacker tool used
- ❑ Utility or port targeted
- ❑ Social engineering

Details: _____

_____

_____

- ❑ Level of access gained—root/administrator, user

Method of operation of the attack (more detailed description of actions taken):

- ❑ Ports or protocols attacked
- ❑ Attack tools used, if known
- ❑ Installed hacker tools such as rootkit, sniffers, L0phtCrack, zap
- ❑ Sites hacker used to download tools
- ❑ Hacker tools installed
- ❑ Established a service such as IRC
- ❑ Looked at who is logged on
- ❑ Trojanned, listed, examined, deleted, modified, created, or copied files
- ❑ Left a back door
- ❑ Names of accounts created and passwords used
- ❑ Left unusual or unauthorized processes running
- ❑ Launched attacks on other systems or sites
- ❑ Other

Details: _____

_____

_____

Reprinted with permission of the author (Kruse).
Copyright © 2001. For more information, see <http://www.awl.com/cseng>.

How detected:

- ❑ Another site
- ❑ Incident response team
- ❑ Log files
- ❑ Packet sniffer
- ❑ Intrusion detection software
- ❑ Anomalous behavior
- ❑ User
- ❑ Alarm tripped
- ❑ TCP Wrapper
- ❑ Tripwire
- ❑ Other

Details: _____

_____

_____

Log file excerpts: _____

_____

_____

Remediation (actions taken to return the systems to trusted operation):

- ❑ Patches applied
- ❑ Scanners run
- ❑ Security software installed
- ❑ Unneeded services and applications removed
- ❑ OS reloaded
- ❑ System restored from backup
- ❑ Application moved to another system
- ❑ Memory or disk space increased
- ❑ System placed behind a filtering router or firewall
- ❑ Hidden files detected and removed
- ❑ Trojan software detected and removed
- ❑ System left unchanged to monitor hacker behavior
- ❑ Other

Details: _____

_____

_____

Reprinted with permission of the author (Kruse).
Copyright © 2001. For more information, see <http://www.awl.com/cseng>.

Additional Comments: _____

_____

_____

Details for Denial-of-Service Incident

Apparent source:

- IP address _____
- Location of host:
  - ❑ Domestic
  - ❑ Foreign
  - ❑ Insider

Primary systems involved:

- IP addresses or subnet address _____
- OS versions _____
- NOS versions _____

Other affected systems or networks (IPs and OSs): _____

_____

_____

Method of operation:

- ❑ Tool used
- ❑ Packet flood
- ❑ Malicious packet
- ❑ IP spoofing
- ❑ Ports attacked
- ❑ Anything that makes this event unique

Details: _____

_____

_____

Remediation (actions taken to protect the systems):

- ❑ Application moved to another system
- ❑ Memory or disk space increased
- ❑ Shadow server installed

Reprinted with permission of the author (Kruse).
Copyright © 2001. For more information, see <http://www.awl.com/cseng>.

- ❑ System moved behind a filtering router or firewall
- ❑ Other

Details: _____

_____

_____

Log file excerpts: _____

_____

_____

Additional comments: _____

_____

_____

Reprinted with permission of the author (Kruse).
Copyright © 2001. For more information, see <http://www.awl.com/cseng>.

Nebraska Information Technology Commission

The Nebraska Information Technology Commission (NITC) has developed a set of procedures for reporting security breaches involving Nebraska state agencies. We have reproduced the procedures document in this appendix.

These incident response procedures also include both a short and long form for reporting incidents:

- Computer Incident Reporting Short Form
- State of Nebraska Information Systems Administrator's Incident Reporting Form

The document and forms are available from <http://www.nitc.state.ne.us/standards/> (see the links for the "Security Architecture" section) [Nebraska 02].

Reproduced From
Best Available Copy

Title	Incident Response and Reporting Procedure for State Government
Category	Security Architecture
Date Adopted	June 18, 2002
Date of Last Revision	April 5, 2002
Date of Next Review	June 2004

State Agencies shall prepare procedures for reporting security breaches and incidents. Documentation on security incidents shall be filed with the Chief Information Officer for the State of Nebraska.

Explanation / Key Points

Security is a growing problem. Effective response and collective action are required to counteract security violations and activities that lead to security breaches. Agency management, law enforcement, and others must know the extent of security problems in order to make proper decisions pertaining to policies, programs and allocation of resources. Responding to security alerts will help to prevent incidents from occurring. Quick reporting of some incidents, such as new viruses, is essential to stopping them from spreading and impacting other systems. Reporting computer crimes is the only way for law enforcement to deter and apprehend violators.

These guidelines incorporate most of the "CIO Cyberthreat Response and Reporting Guidelines" jointly sanctioned by the FBI and U.S. Secret Service. A copy of those guidelines is available at: http://www.cio.com/research/security/incident_response.pdf, http://www.usss.treas.gov/net_intrusion.shtml, or http://www.fbi.gov/pressrel/pressrel02/cyberguidelines.htm.

Effective response to security incidents requires quick recognition of problems and fast mobilization of skilled staff to return systems to normal. This requires prior documentation of procedures and responsibilities of everyone with a role in responding to the emergency. Continuous improvement by eliminating points of vulnerability and applying lessons learned is an essential component of incident response.

Centralized reporting serves the goal of increasing awareness of vulnerabilities and threats to state government as a whole. In particular, centralized reporting is necessary to discern patterns, identify areas of vulnerability, allocate resources, and develop statewide solutions. Centralized reporting does not substitute for internal reporting to management, reporting to law enforcement, or mobilizing a computer security incident response team (CSiRT). Agencies should develop procedures for internal and external

Reprinted through the courtesy of the State of Nebraska. Available from <http://www.nitc.state.ne.us/standards/>.

reporting that will meet the needs of centralized reporting with little or no additional work. The centralized reporting is designed to mesh with the postmortem analysis that should follow each incident.

Security incident response should never include retaliation. Defending a system should emphasize preventing security breaches. If there is an intrusion, a defensive response should focus on containing and eradicating the problem, plugging the security hole and getting back to business. Security incident response should never include striking back against attackers. The appropriate law enforcement authorities should handle all punitive actions.

Applicability

These guidelines apply to all non-education state agencies, boards, and commissions, which receive a direct appropriation from the Legislature or any state agency that has a direct connection to the state's network. Educational institutions and other entities are encouraged to develop their own security incident and centralized reporting procedures.

Planning and Preparation

Develop an incident response plan and designate people to carry it out. The plan should include details for how you will:

1. Detect the incident
2. Analyze the incident
3. Contain or eradicate the problem
4. Provide workarounds or fixes
5. Prevent re-infection
6. Log events
7. Preserve evidence
8. Conduct a post-mortem and apply lessons learned

Educate users to raise security awareness and promote security policies. Build a centralized incident reporting system. Establish escalation procedures that lay out actions the agency should take if an attack turns out to be protracted or especially damaging. Make sure your service-level agreements include provisions for security compliance, and spell out reporting requirements and maintenance of systems (including contingency plans) in the event of a cyberattack. Decide in advance under what circumstances you would call the authorities. Plan how and when employees, customers and strategic partners will be informed of the problem. Establish communication procedures, if the media become involved.

Have a single contact to whom employees should report suspicious events and who will track changes in contacts or procedures. Have a single contact that will report incidents to outside agencies, including law enforcement, regulatory bodies and information sharing organizations such as InfraGard.

Reprinted through the courtesy of the State of Nebraska. Available from <http://www.nitc.state.ne.us/standards/>.

Keep a list of the incident response team members' names, titles and 24/7contact information, along with their role in a security breach. Have contact information for vendors contracted to help during a security emergency, as well as ISPs and other relevant technology providers. Have contact information for major customers and clients who might be affected. In advance, establish contacts at the relevant law enforcement agencies: typically, the national infrastructure protection and computer intrusion squad at the local FBI field office; the electronic crimes investigator at the local Secret Service field office; and the electronic crimes investigator at the Nebraska State Patrol. Have their contact information easily accessible.

Perform a risk analysis on your plan. Test and rehearse procedures periodically. Develop contingency Plans in case your response infrastructure is attacked.

What to Report

The ultimate goal of security incident response and centralized reporting is to protect data and prevent obstruction of government operations. It is important to distinguish between problems that stem from mistakes or miscommunications and true security incidents that involve either malicious intent or intent to circumvent security measures. Security incident reporting should be used only for true security incidents. You should report events that have a real impact on your organization (such as when damage is done, access is achieved by the intruder, loss occurs, web pages are defaced, malicious code is implanted) or when you detect something noteworthy or unusual (new traffic pattern, new type of malicious code, specific IP as source of persistent attacks). Do not report routine probes, port scans, or other common events.

A security incident includes, but is not limited to the following events, regardless of platform or computer environment:

1. Evidence of tampering with data;
2. Denial of service attack on the agency;
3. Web site defacement;
4. Unauthorized access or repeated attempts at unauthorized access (from either internal or external sources);
5. Social engineering incidents;
6. Virus attacks which adversely affect servers or multiple workstations;
7. Other incidents that could undermine confidence and trust in the state's information technology systems.

When and How to Report an Incident

If an attack is under way, you should call your previously established law enforcement contact immediately and communicate the basic information that is included in the Computer Incident Reporting Short Form. There is additional information that will be required to effectively conduct the investigation (see bullet points below), but the form is a good place to start. Sometimes you will report an incident to law enforcement after the fact—you have detected that something happened, but your systems are functioning normally and whatever damage is likely has already been done. In this case, you will

Reprinted through the courtesy of the State of Nebraska. Available from <http://www.nitc.state.ne.us/standards/>.

want to gather as much information as possible for the law enforcement agents before you make the call. Here is some additional information that will help law enforcement agents in their investigation:

1. What are the primary systems involved?
2. How was the attack carried out?
3. What steps have you taken to mitigate or remediate?
4. Does a suspect exist? If so, is it a current or former employee/contractor?
5. What evidence is available to assist in the investigation (e.g., log files, physical evidence, etc.)? To track the status of your case once you've filed a report, contact the field office that is conducting the investigation.

Who to Notify

FBI – Omaha Office
InfraGard Coordinator
Phone (405) 290-3685
Fax (405) 290-3885
infragard-om@fbi.gov

Nebraska State Patrol
Capt. Robert E. Thorson
Investigative Services
Nebraska State Patrol
1600 Highway 2
Lincoln, Nebraska 68509-4907
Ph. 402-479-4947; Fax:
rthorson@nsp.state.ne.us

Sgt. Scott Christensen
Coordinator
Internet Crimes Against Children Unit
Nebraska State Patrol - Omaha
4411 So. 108th Street
Omaha, Nebraska 68137
Ph. 402-595-2410; Fax: 402-697-1409
24 hr dispatch number is 402-331-3333.
schriste@nsp.state.ne.us
www.nsp.state.ne.us

Office of the CIO / NITC (state agencies, only)
Steve Schafer
Chief Information Officer
521 South 14th Street, Suite 200
Lincoln, Nebraska 68508-2707
Ph. 402-471-4385; Fax: 402-471-4608
slschafe@notes.state.ne.us

Reprinted through the courtesy of the State of Nebraska. Available from <http://www.nitc.state.ne.us/standards/>.

Step-by-step procedure(s)

The Incident Response and Centralized Reporting Procedure for State Government requires that the agency implement the following steps for a complete security incident handling process.

1. Establish general procedures for responding to incidents;
2. Prepare to respond to incidents;
3. Analyze all available information to characterize an incident;
4. Communicate with all parties that need to be made aware of an incident and its progress;
5. Collect and protect information associated with an incident;
6. Apply short-term solutions to contain an incident;
7. Eliminate all means of vulnerability pertaining to that incident;
8. Return systems to normal operation;
9. Closure: Identify and implement security lessons learned.

Step 1: Establish a computer security incident response team (CSIRT) that can take responsibility for managing security incidents. The CSIRT can be a virtual team that includes people with a wide range of expertise. Agencies should consider forming a CSIRT that serves multiple entities. A clear description of roles and expectations is essential.

Step 2: Set methods for placing the CSIRT on alert status and ready to take preventative measures. It should include procedures for activating the team once an incident occurs.

Step 3: Identify and understand the incident. Use the Information Systems Administrator's Incident Reporting form to document the incident.

Step 4: Contact managers and users affected by an incident, security personnel, law enforcement agencies, vendors, the CERT Coordination Center (**http://www.cert.org/**), and other CSIRTs external to the organization as necessary. It is essential that each agency establishes and follows a single channel of communication. Multiple sources of information while the incident is underway creates confusion, interrupts the work of the response team, and increases vulnerability if the perpetrator is monitoring communications within the agency. It is required that the Computer Incident Reporting Short Form be completed and forwarded to the Nebraska State CIO.

Step 5: Collect and preserve as much evidence in its original form as possible. Take detailed notes of all evidence found and record each piece of evidence. It is important not to rush. Be aware not to destroy or modify any evidence. If necessary, use low-level copying methods to make a complete copy of the disk and memory state of the affected host(s).

Reprinted through the courtesy of the State of Nebraska. Available from <http://www.nitc.state.ne.us/standards/>.

Step 6: As necessary the CSIRT should, (A) physically isolate the affected host(s); (B) change all passwords or disable all accounts on all systems to which the attacker may have had access; (C) disable access to compromised file or date systems that are shared with other computers. Continue to monitor system and network activities

Step 7: The CSIRT should review local operating system and configuration files for signs of intrusion and remove any means for intruder access including changes made by an intruder. Next, determine if there are uncorrected system or network vulnerabilities and correct them. Last, improve protection mechanisms to limit the exposure of networks and systems.

Step 8: Determine the requirements and timeframe for returning the system to normal operation. Members of the CSIRT should restore the operating system, applications and data from trusted media and reconnect the restored system to the network. The CSIRT should validate the restored system for potential vulnerabilities.

Step 9, "Closure" is intended to give the organization an opportunity to learn from the experience of responding to an incident. Every successful intrusion or other incident indicates potential weaknesses in systems, networks, operations, and staff preparedness. These weaknesses provide opportunities for improvement. Steps should include the following points (from CERTCC security practices, http://www.cert.org/security-improvement/practices/p052.html):

1. Hold a post mortem analysis and review meeting with all involved parties. Do this within three to five working days of completing the investigation of an intrusion. Use the attached Information Systems Administrator's Incident Reporting Form to gather information and guide discussion.
2. Prepare a final report for senior management. This ensures awareness of security issues. Use either the Computer Incident Reporting Short Form or the Information Systems Administrator's Incident Reporting Form to report information about the security incident to the Office of the Chief Information Officer. Incidents should be reported no later than 5 working days after returning systems to normal operation.
3. Revise security plans and procedures and user and administrator training to prevent future incidents. Include any new, improved methods resulting from lessons learned.
4. Determine whether or not to perform a new risk analysis based on the severity and impact of an intrusion.
5. Take a new inventory of your system and network assets.
6. Participate in investigation and prosecution, if applicable.

Related Rules

Draft security standards for the federal Health Insurance Portability and Accountability Act (HIPAA) would establish administrative procedures to guard data integrity, confidentiality, and availability. These include security incident procedures (45 CFR

Reprinted through the courtesy of the State of Nebraska. Available from <http://www.nitc.state.ne.us/standards/>.

Part 142.308 (a)(9):

"(9) Security incident procedures (formal documented instructions for reporting security breaches) that include all of the following implementation features:

"(i) Report procedures (documented formal mechanism employed to document security incidents).

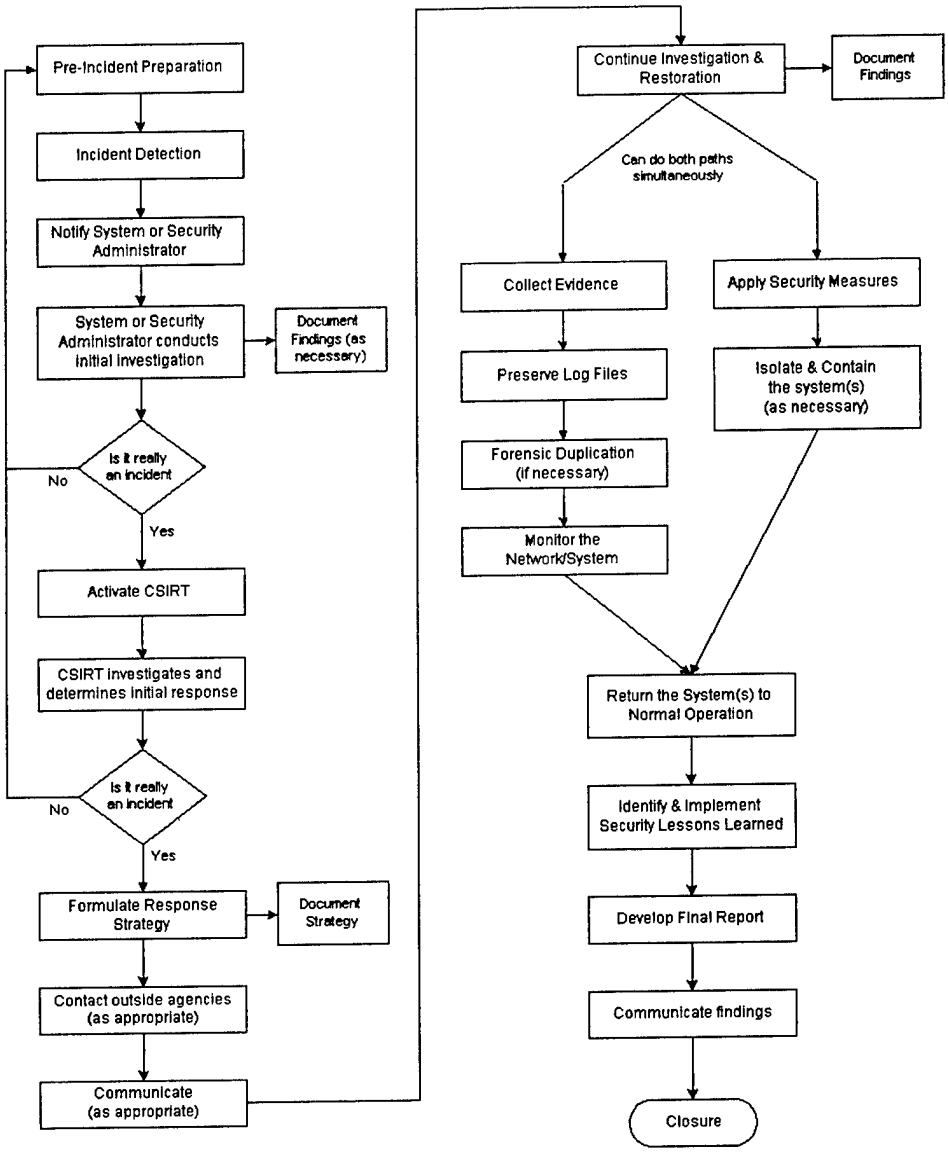
"(ii) Response procedures (documented formal rules or instructions for actions to be taken as a result of the receipt of a security incident report)."

Attachments/ Forms

Incident Response Process Flow Chart
Computer Incident Reporting Short Form
Information Systems Administrator's Incident Reporting Form

Reprinted through the courtesy of the State of Nebraska. Available from <http://www.nitc.state.ne.us/standards/>.

Incident Response Process



Reprinted through the courtesy of the State of Nebraska. Available from <http://www.nitc.state.ne.us/standards/>.

COMPUTER INCIDENT REPORTING SHORT FORM

Use this form to report incidents to the Office of the Chief Information Officer of the State of Nebraska. State agencies should send an electronic copy to slschafe@notes.state.ne.us, or fax it to (402) 471-4608. This form also outlines the basic information that law enforcement needs on a first call.

STATUS

☐ Site Under Attack ☐ Past Incident ☐ Repeated Incidents, unresolved

CONTACT INFORMATION

Name_____ Title_____

Organization_____

Direct-Dial Phone_____ E-mail_____

Legal Contact Name_____ Phone_____

Location/Site(s) Involved_____

Street Address_____

City_____ State_____ ZIP_____

Main Telephone_____ Fax_____

ISP Contact Information_____

INCIDENT DESCRIPTION

☐ Denial of Service

☐ Distributed Denial of Service

☐ Intrusion/Hack

☐ Malicious Code (virus, worm)

☐ Misuse of Systems (internal or external) (Includes inappropriate use by employees)

☐ Probe/Scan

☐ Unauthorized Electronic Monitoring (sniffers)

☐ Website Defacement

☐ Other (specify)_____

DATE/TIME OF INCIDENT DISCOVERY

Date_____ Time_____

Duration of Attack_____

IMPACT OF ATTACK

☐ Loss/Compromise of Data

☐ Damage to Systems

☐ Financial Loss (estimated amount: $_____)

☐ Damage to the Integrity or Delivery of Critical Goods, Services or Information

☐ System Downtime

☐ Other Organizations' Systems Affected

SEVERITY OF ATTACK, INCLUDING FINANCIAL LOSS OR INFRASTRUCTURE

☐ High ☐ Medium ☐ Low ☐ Unknown

SENSITIVITY OF DATA

☐ High ☐ Medium ☐ Low ☐ Unknown

How did you detect This?_____

Have you contacted law enforcement about this incident before? Who & when?_____

Has the incident been resolved? Explain_____

Reprinted through the courtesy of the State of Nebraska. Available from <http://www.nitc.state.ne.us/standards/>.

State of Nebraska
Information Systems Administrator's Incident Reporting Form

Point of Contact Information

Name	
Title	
Telephone/Fax Numbers	
Email	
Agency	

B. Incident Information

1. Background Information:	
a. Agency (if same as above, enter "SAME":	
b. Physical Location(s) of affected computer system/network (be specific):	
c. Date/time of the incident:	
d. Duration of the incident:	
e. Is the affected system/network critical to the agency's mission? (Yes/No)	

2. Nature of Problem (check all that apply):	
a. Intrusion	
b. System impairment/denial of access	
c. Unauthorized root access	
d. Web site defacement	
e. Compromise of system integrity	
f. Hoax	
g. Theft	
h. Damage	
i. Unknown	
j. Other (provide details in remarks)	
k. REMARKS:	

Reprinted through the courtesy of the State of Nebraska. Available from <http://www.nitc.state.ne.us/standards/>.

3. Has your agency experienced this problem before? (Yes/No; If yes, please explain in the remarks section.)
a. REMARKS:

4. Suspected method of intrusion/attack:	
a. Virus (provide name, if known)	
b. Vulnerable exploited (explain)	
c. Denial of Service	
d. Trojan Horse	
e. Distributed Denial of Service	
f. Trapdoor	
g. Unknown	
h. Other (Provide details in remarks)	
i. REMARKS:	

5. Suspected perpetrator(s) or possible motivation(s) of the attack:	
a. Insider/Disgruntled Employee	
b. Former employee	
c. Other (Explain remarks)	
d. Unknown	
e. REMARKS:	

6. The apparent source (IP address) of the intrusion/attack:

7. Evidence of spoofing (Yes/No/Unknown)

8. What computers/systems (hardware and software) were affected (Operating system, version):	
a. Unix	
b. OS2	
c. Linux	
d. VAX/VMS	
e. NT	

Reprinted through the courtesy of the State of Nebraska. Available from <http://www.nitc.state.ne.us/standards/>.

f. Windows	
g. Sun OS/Solaris	
h. Other (Please specify in remarks)	
i. REMARKS:	

9. Security Infrastructure in place. (Check all that apply)	
a. Incident/Emergency Response Team	
b. Encryption	
c. Firewall	
d. Secure Remote Access/Authorization Tools	
e. Intrusion Detection System	
f. Security Auditing Tools	
g. Banners	
h. Packet filtering	
i. Access Control Lists	
j. REMARKS:	

10. Did intrusion/attack result in a loss/compromise of sensitive or information classified as private?	
a. Yes (provide details in remarks)	
b. No	
c. Unknown	
d. REMARKS:	

11. Did the intrusion/attack result in damage to system(s) or data?	
a. Yes (provide details in remarks)	
b. No	
c. Unknown	
d. REMARKS:	

12. What actions and technical mitigation have been taken?

Reprinted through the courtesy of the State of Nebraska. Available from <http://www.nitc.state.ne.us/standards/>.

a. System(s) disconnected from the network?	
b. System Binaries checked?	
c. Backup of affected system(s)?	
d. Log files examined?	
e. Other (Please provide details in remarks)	
f. No action(s) taken	
g. REMARKS:	

13. Has law enforcement been notified? (Check all that apply.)	
a. Yes-local law enforcement	
b. Yes-Nebraska State Patrol	
c. Yes-FBI field office	
d. Not	
e. REMARKS:	

14. Has another agency/organization been informed as assisted with the response?	
a. Yes-Information Management Services	
b. Yes-Division of Communications	
c. Yes-CERT-CC	
d. Yes-Other (provide details in remarks)	
e. No	
f. REMARKS:	

15. Additional Remarks:

If the reported incident is a criminal matter, you may be contacted by law enforcement for additional information.

Reprinted through the courtesy of the State of Nebraska. Available from <http://www.nitc.state.ne.us/standards/>.

C. Closure Information (Optional, Except 9 & 10)

1. (Optional) Did your detection and response process and procedures work as intended? If not, where did they not work? Why did they not work?
REMARKS:

2. (Optional) Methods of discovery and monitoring procedures that would have improved your ability to detect an intrusion.
REMARKS:

3. (Optional) Improvements to procedures and tools that would have aided you in the response process. For example, consider using updated router and firewall filters, placement of firewalls, moving the compromised system to a new name or IP address, or moving the compromised machine's function to a more secure area of your network.
REMARKS:

4. (Optional) Improvements that would have enhanced your ability to contain an intrusion.
REMARKS:

5. (Optional) Correction procedures that would have improved your effectiveness in recovering your systems.
REMARKS:

Reprinted through the courtesy of the State of Nebraska. Available from <http://www.nitc.state.ne.us/standards/>.

6. (Optional) Updates to policies and procedures that would have allowed the response and recovery processes to operate more smoothly.
REMARKS:

7. (Optional) Topics for improving user and system administrator preparedness.
REMARKS:

8. (Optional) Areas for improving communication throughout the detecting and response processes.
REMARKS:

9. (Required) A description of the costs associated with an intrusion, including a monetary estimate if possible.
REMARKS:

10. (Required) Summary of post mortem efforts.
REMARKS:

Reprinted through the courtesy of the State of Nebraska. Available from <http://www.nitc.state.ne.us/standards/>.

SANS

SANS provides the following incident handling forms:

- Incident Contact List
- Incident Identification
- Incident Survey
- Incident Containment
- Incident Eradication
- Incident Communication Log

The forms are available from <http://www.sans.org/incidentforms/> [SANS 03].

INCIDENT CONTACT LIST

DATE UPDATED:_____

Corporate Security Officer:

Name:_____

Title: _____

Phone:_____ Alt. Phone: _____

Mobile: _____ Pager:_____

Fax:_____ Alt. Fax:_____

E-mail: _____

Address: _____

_____

Corporate Legal Affairs Officer:

Name:_____

Title: _____

Phone:_____ Alt. Phone: _____

Mobile: _____ Pager:_____

Fax:_____ Alt. Fax:_____

E-mail: _____

Address: _____

_____

Corporate Public Affairs Officer:

Name:_____

Title: _____

Phone:_____ Alt. Phone: _____

Mobile: _____ Pager:_____

Fax:_____ Alt. Fax:_____

E-mail: _____

Address: _____

_____

Corporate Incident Handling, CIRT, or FIRST Team:

Name:_____

Title: _____

Phone:_____ Alt. Phone: _____

Mobile: _____ Pager:_____

Fax:_____ Alt. Fax:_____

E-mail: _____

Address: _____

_____

CIO or Information Systems Security Manager:

Name:_____

Title: _____

Phone:_____ Alt. Phone: _____

Mobile: _____ Pager:_____

Fax:_____ Alt. Fax:_____

E-mail: _____

Address: _____

_____

Other (Specify):_____

Name:_____

Title: _____

Phone:_____ Alt. Phone: _____

Mobile: _____ Pager:_____

Fax:_____ Alt. Fax:_____

E-mail: _____

Address: _____

_____

© Copyright SANS Institute 2003 Prepared By: Greg Jones All Rights Reserved

INCIDENT CONTACT LIST DATE UPDATED:_____

Local Contacts

Internet Service Provider Technical Contact:

Name:_____

Title: _____

Phone:_____ Alt. Phone: _____

Mobile: _____ Pager:_____

Fax:_____ Alt. Fax:_____

E-mail: _____

Address: _____

_____

Local FBI or Equivalent Agency:

Name:_____

Title: _____

Phone:_____ Alt. Phone: _____

Mobile: _____ Pager:_____

Fax:_____ Alt. Fax:_____

E-mail: _____

Address: _____

_____

Local Law Enforcement Computer Crime:

Name:_____

Title: _____

Phone:_____ Alt. Phone: _____

Mobile: _____ Pager:_____

Fax:_____ Alt. Fax:_____

E-mail: _____

Address: _____

_____

Local CIRT or FIRST Team:

Name:_____

Title: _____

Phone:_____ Alt. Phone: _____

Mobile: _____ Pager:_____

Fax:_____ Alt. Fax:_____

E-mail: _____

Address: _____

_____

Other (Specify):_____

Name:_____

Title: _____

Phone:_____ Alt. Phone: _____

Mobile: _____ Pager:_____

Fax:_____ Alt. Fax:_____

E-mail: _____

Address: _____

_____

Other (Specify):_____

Name:_____

Title: _____

Phone:_____ Alt. Phone: _____

Mobile: _____ Pager:_____

Fax:_____ Alt. Fax:_____

E-mail: _____

Address: _____

_____

© Copyright SANS Institute 2003 Prepared By: Greg Jones All Rights Reserved

INCIDENT CONTACT LIST DATE UPDATED:_____

Other Contacts

Other (Specify):_____

Name:_____

Title: _____

Phone:_____ Alt. Phone: _____

Mobile: _____ Pager:_____

Fax:_____ Alt. Fax:_____

E-mail: _____

Address: _____

_____

Other (Specify):_____

Name:_____

Title: _____

Phone:_____ Alt. Phone: _____

Mobile: _____ Pager:_____

Fax:_____ Alt. Fax:_____

E-mail: _____

Address: _____

_____

Other (Specify):_____

Name:_____

Title: _____

Phone:_____ Alt. Phone: _____

Mobile: _____ Pager:_____

Fax:_____ Alt. Fax:_____

E-mail: _____

Address: _____

_____

Other (Specify):_____

Name:_____

Title: _____

Phone:_____ Alt. Phone: _____

Mobile: _____ Pager:_____

Fax:_____ Alt. Fax:_____

E-mail: _____

Address: _____

_____

Other (Specify):_____

Name:_____

Title: _____

Phone:_____ Alt. Phone: _____

Mobile: _____ Pager:_____

Fax:_____ Alt. Fax:_____

E-mail: _____

Address: _____

_____

Other (Specify):_____

Name:_____

Title: _____

Phone:_____ Alt. Phone: _____

Mobile: _____ Pager:_____

Fax:_____ Alt. Fax:_____

E-mail: _____

Address: _____

_____

© Copyright SANS Institute 2003 Prepared By: Greg Jones All Rights Reserved

INCIDENT IDENTIFICATION DATE UPDATED:_____

General Information

Incident Detector's Information:

Name:_____ Date and Time Detected: _____

Title: _____

Phone:_____ Alt. Phone: _____ Location Incident Detected From: _____

Mobile: _____ Pager:_____ _____

Fax:_____ Alt. Fax:_____ Additional Information:_____

E-mail: _____ _____

Address: _____ _____

_____ _____

Detector's Signature:_____ Date Signed: _____

Incident Summary

Type of Incident Detected:

- Denial of Service
- Malicious Code
- Unauthorized Use
- Unauthorized Access
- Espionage
- Other:_____
- Probe
- Hoax

Incident Location:

Site:_____ How was the Intellectual Property Detected:_____

Site Point of Contact:_____ _____

Phone:_____ Alt. Phone: _____ _____

Mobile: _____ Pager:_____ _____

Fax:_____ Alt. Fax:_____ _____

E-mail: _____ _____

Address: _____ _____

_____ _____

Additional Information: _____

_____

_____

© Copyright SANS Institute 2003 Prepared By: Greg Jones All Rights Reserved

INCIDENT SURVEY

DATE UPDATED:_____

Location(s) of affected systems: _____

_____

_____

_____

Date and time incident handlers arrived at site: _____

_____

_____

Describe affected information system(s) (one form per system is recommended):

Hardware Manufacturer:_____

Serial Number: _____

Corporate Property Number (if applicable): _____

Is the affected system connected to a network? • **YES** • **NO**

System Name: _____

System Network Address:_____

MAC Address: _____

Is the affected system connected to a modem? • **YES** • **NO**

Phone Number: _____

Describe the physical security of the location of affected information systems (locks, security alarms, building access, etcetera):

_____

_____

_____

_____

_____

_____

_____

_____

_____

© Copyright SANS Institute 2003 Prepared By: Greg Jones All Rights Reserved

INCIDENT CONTAINMENT

DATE UPDATED:_____

Isolate affected systems:

Command Decision Team approved removal from network? • YES • NO

If YES, date and time systems were removed: _____

If NO, state the reason: _____

_____

_____

Backup affected systems:

System backup successful for all systems? • YES • NO

Name of persons who did backup:_____

_____

_____

_____

_____

Date and time backups started:_____

Date and time backups complete: _____

Backup tapes sealed? • YES • NO Seal Date: _____

Backup tapes turned over to:_____

Signature:_____ Date: _____

Backup Storage Location: _____

© Copyright SANS Institute 2003 Prepared By: Greg Jones All Rights Reserved

INCIDENT ERADICATION

DATE UPDATED:_____

Name of persons performing forensics on systems: _____

_____

_____

_____

_____

Was the vulnerability identified? • **YES** • **NO**

Describe: _____

_____

_____

_____

_____

_____

What was the validation procedure used to ensure problem was eradicated: _____

_____

_____

_____

_____

_____

_____

_____

© Copyright SANS Institute 2003 Prepared By: Greg Jones All Rights Reserved

INCIDENT COMMUNICATION LOG

DATE UPDATED:_____

Date:_____ **Time:**_____ • **am** • **pm** **Method (mail, phone, email, etc.):**_____

Initiator Name:_____ Receiver Name:_____

Initiator Title: _____ Receiver Title: _____

Initiator Organization: _____ Receiver Organization:_____

Initiator Contact Info:_____ Receiver Contact Info: _____

Details:_____

_____

_____

_____

Date:_____ **Time:**_____ • **am** • **pm** **Method (mail, phone, email, etc.):**_____

Initiator Name:_____ Receiver Name:_____

Initiator Title: _____ Receiver Title: _____

Initiator Organization: _____ Receiver Organization:_____

Initiator Contact Info:_____ Receiver Contact Info: _____

Details:_____

_____

_____

_____

Date:_____ **Time:**_____ • **am** • **pm** **Method (mail, phone, email, etc.):**_____

Initiator Name:_____ Receiver Name:_____

Initiator Title: _____ Receiver Title: _____

Initiator Organization: _____ Receiver Organization:_____

Initiator Contact Info:_____ Receiver Contact Info: _____

Details:_____

_____

_____

_____

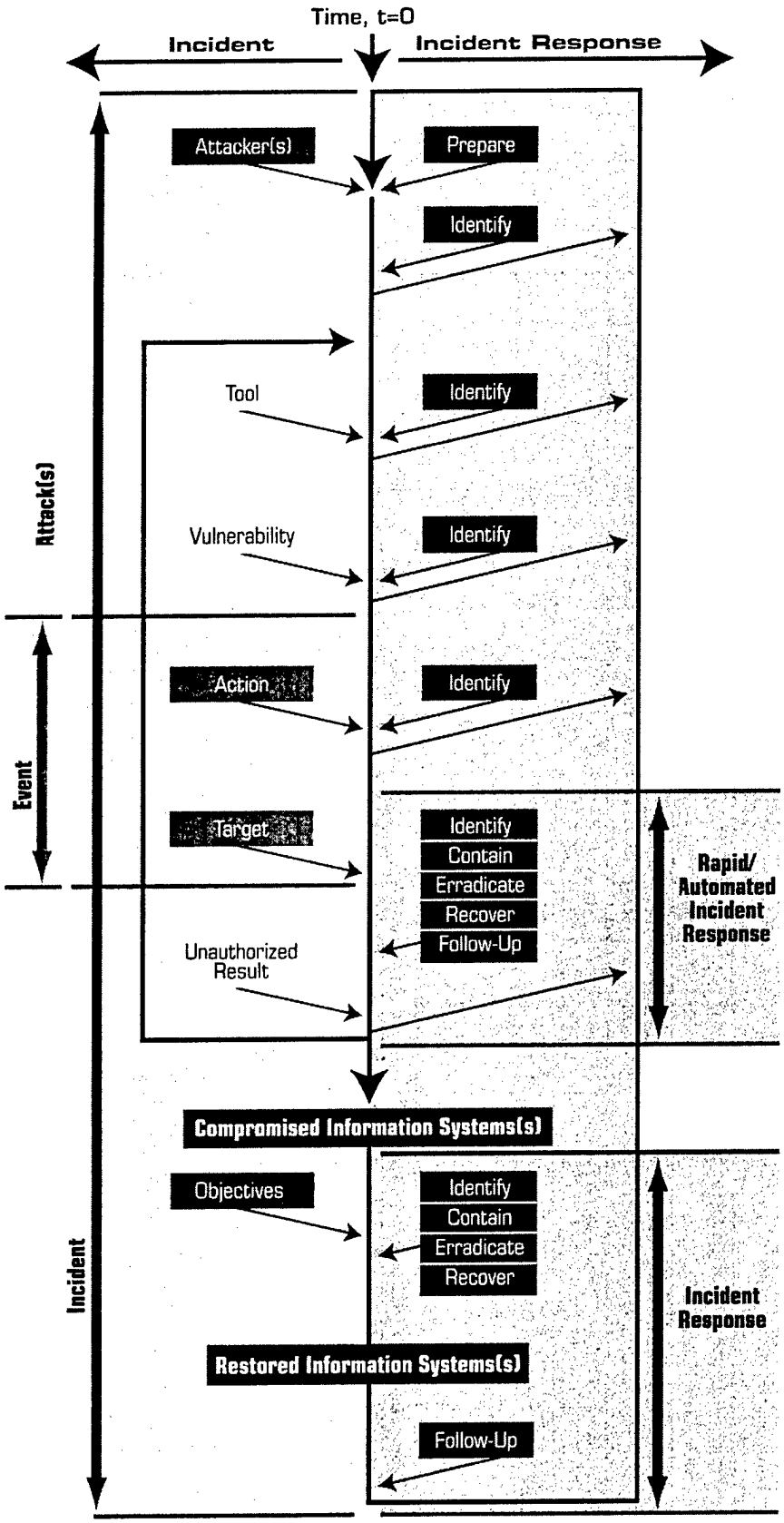
© Copyright SANS Institute 2003 Prepared By: Greg Jones All Rights Reserved

Steele

The Information Assurance Technology Analysis Center (IATAC) Volume 5, Number 1 (Spring 2002) newsletter contains an article, "Information Systems Security Incident Response," by Gordon Steele [Steele 02]. One section of the article provides a graphical abstraction of an incident flow timeline. The author presents this approach as a mechanism to allow incident handlers "to envision where they might be at any given point in time" in the incident response process.

The newsletter is available at <http://iac.dtic.mil/iatac/IAnewsletter/Vol5_No1.pdf>.

Reproduced From
Best Available Copy



Reprinted with permission of IATAC. (IAnewsletter, Volume 5, Number 1, page 22, Spring 2002).
Copyright © 2002
For more information see <http://iac.dtic.mil/iatac/news_events/pdf/Vol5_No1.pdf>

United States Secret Service

The USSS has developed a "Cyber Threat/Network Incident Report," Secret Service Form 4017. It is provided in two different formats, an OmniForm Mailable Filler and an Adobe Acrobat PDF. The PDF version has been included here [USSS 01]. Both formats are available at <http://www.secretservice.gov/net_intrusion_forms.shtml>.

Network Incident Report

United States Secret Service • Financial Crimes Division • Electronic Crimes Branch
Telephone: 202-406-5850 FAX: 202-406-9233 e-mail: ecb@secretservice.gov

Subject:
❑ Site under attack ❑ Incident investigation in progress ❑ Incident closed

What assistance do you require:
❑ Immediate call
❑ None needed at this time
❑ Follow-up on all affected sites
❑ Contact the "hacking" site(s)

Site involved *(name & acronym):*

POC for incident:
• Name / Title _____
• Organization _____
• E-mail _____ • 7 x 24 contact information _____

Alternate POC for incident:
• Name / Title _____
• Organization _____
• E-mail _____ • 7 x 24 contact information _____

Type of Incident:
❑ Malicious code: virus, Trojan horse, worm
❑ Probes/scans (non-malicious data gathering--recurring, massive, unusual)
❑ Attack (successful/unsuccessful intrusions including scanning with attack packets)
❑ Denial-of-service event
❑ High embarrassment factor
❑ Deemed significant by site

Date and time incident occurred *(specify time zone):*

A summary of what happened:

Type of service, information, or project compromised *(please provide specifics):*
❑ Sensitive unclassified such as privacy, proprietary, or source selection
_____
❑ Other unclassified _____

Damage done:
• Numbers of systems affected _____
• Nature of loss, if any _____
• System downtime _____
• Cost of incident: ❑unknown ❑ none ❑<$10K ❑$10K - $50K ❑ >$50K

Name other sites contacted
Law Enforcement _____
Other: _____

UNITED STATES SECRET SERVICE SSF 4017 (03/2002)
Page 1

Reprinted through the courtesy of the United States Secret Service. Available from <http://www.secretservice.gov/net_intrusion_forms.shtml>.

Details for Malicious Code

Apparent source:
- ❑ Diskette, CD, etc.
- ❑ E-mail attachment
- ❑ Software download

Primary system or network involved:
- IP addresses or sub-net addresses _____
- OS version(s) _____
- NOS version(s) _____
- Other _____

Other affected systems or networks (IPs and OSs):

Type of malicious code *(include name if known)*:
- ❑ Virus _____
- ❑ Trojan horse _____
- ❑ Worm _____
- ❑ Joke program _____
- ❑ Other _____

❑ **Copy sent to**
- ❑ _____
- ❑ _____
- ❑ _____

Method of Operation *(for new malicious code)*:
- ❑ Type: macro, boot, memory resident, polymorphic, self encrypting, stealth
- ❑ Payload
- ❑ Software infected
- ❑ Files erased, modified, deleted, encrypted *(any special significance to these files)*
- ❑ Self propagating via e-mail
- ❑ Detectable changes
- ❑ Other features

Details:

How detected:

Remediation *(what was done to return the system(s) to trusted operation)*:
- ❑ Anti-virus product gotten, updated, or installed for automatic operation
- ❑ New policy instituted on attachments
- ❑ Firewall or routers or e-mail servers updated to detect and scan attachments

Details:

Additional comments:

UNITED STATES SECRET SERVICE

Page 2

SSF 4017 (03/2002)

Reprinted through the courtesy of the United States Secret Service. Available from <http://www.secretservice.gov/net_intrusion_forms.shtml>.

Details for Probes and Scans

Apparent source:
- IP address _____
- Host name _____
- Location of attacking host: _____
  - ❑ Domestic
  - ❑ Foreign
  - ❑ Insider

Primary system(s) / network(s) involved:
- IP addresses or sub-net addresses _____
- OS version(s) _____
- NOS version(s) _____

Other affected systems or networks (IPs and OSs):

Method of Operation:	**Details:**
❑ Ports probed/scanned ❑ Order of ports or IP addresses scanned ❑ Probing tool ❑ Anything that makes this probe unique	
How detected: ❑ Another site ❑ Incident response team ❑ Log files ❑ Packet sniffer ❑ Intrusion detection system ❑ Anomalous behavior ❑ User	**Details:**

Log file excerpts:

Additional comments:

UNITED STATES SECRET SERVICE

Page 3

SSF 4017 (03/2002)

Reprinted through the courtesy of the United States Secret Service. Available from <http://www.secretservice.gov/net_intrusion_forms.shtml>.

Details for Unauthorized Access

Apparent source:
- IP address _____
- Host name _____
- Location of attacking host: _____
  - ❑ Domestic
  - ❑ Foreign
  - ❑ Insider

Primary system(s) involved:
- IP addresses or sub-net addresses _____
- OS version(s) _____
- NOS version(s) _____

Other affected systems or networks (IPs and OSs):

Avenue of attack:	**Details:**
❑ Sniffed/guessed/cracked password ❑ Trusted host access ❑ Vulnerability exploited ❑ Hacker tool used ❑ Utility or port targeted ❑ Social engineering	

Level of access gained-root/administrator, user

Method of operation of the attack (more *detailed description of what was done):*	**Details:**
❑ Port(s) or protocol(s) attacked ❑ Attack tool(s) used, if known ❑ Installed hacker tools such as rootkit, sniffers, 10phtcrack, zap ❑ Site(s) hacker used to download tools ❑ Where hacker tools were installed ❑ Established a service such as IRC ❑ Looked around at who is logged on ❑ Trojanned, listed, examined, deleted, modified, created, or copied files ❑ Left a backdoor ❑ Names of accounts created and passwords used ❑ Left unusual or unauthorized processes running ❑ Launched attacks on other systems or sites ❑ Other	

UNITED STATES SECRET SERVICE SSF 4017 (03/2002)

Page 4

Reprinted through the courtesy of the United States Secret Service. Available from <http://www.secretservice.gov/net_intrusion_forms.shtml>.

Details for Unauthorized Access (continued)

How detected:	Details:
❑ Another site ❑ Incident response team ❑ Log files ❑ Packet sniffer/intrusion detection software ❑ Intrusion detection software ❑ Anomalous behavior ❑ User ❑ Alarm tripped ❑ TCP Wrappers ❑ TRIPWIRED ❑ Other	
Log file excerpts:	
Remediation *(what was done to return the system(s) to trusted operation):* ❑ Patches applied ❑ Scanners run ❑ Security software installed: ❑ Unneeded services and applications removed ❑ OS reloaded ❑ Restored from backup ❑ Application moved to another system ❑ Memory or disk space increased ❑ Moved behind a filtering router or firewall ❑ Hidden files detected and removed ❑ Trojan software detected and removed ❑ Left unchanged to monitor hacker ❑ Other	**Details:**
Additional comments:	

UNITED STATES SECRET SERVICE SSF 4017 (03/2002)

Page 5

Reprinted through the courtesy of the United States Secret Service. Available from <http://www.secretservice.gov/net_intrusion_forms.shtml>.

Details for Denial-of-Service Incident

Apparent source:

- IP address _____
- Location of host:
  - ❑ Domestic
  - ❑ Foreign
  - ❑ Insider

Primary system(s) involved:

- IP addresses or sub-net address _____
- OS version(s) _____
- NOS version(s) _____

Other affected systems or networks (IPs and OSs):

Method of Operation:	**Details:**
❑ Tool used ❑ Packet flood ❑ Malicious packet ❑ IP Spoofing ❑ Ports attacked ❑ Anything that makes this event unique	
Remediation ***(what was done to protect the system(s)):*** ❑ Application moved to another system ❑ Memory or disk space increased ❑ Shadow server installed ❑ Moved behind a filtering router or firewall ❑ Other	**Details:**

Log file excerpts:

Additional comments:

UNITED STATES SECRET SERVICE SSF 4017 (03/2002)

Page 6

Reprinted through the courtesy of the United States Secret Service. Available from <http://www.secretservice.gov/net_intrusion_forms.shtml>.

Van Wyk and Forno

In their book *Incident Response*, van Wyk and Forno provide an example for one approach in documenting information in an incident report [van Wyk 02]. The topics covered in the sample report are

- incident chronology
- comments and recommendations
- law enforcement coordination
- damage assessment
- management review

B

Sample Incident Report

This is a sample incident report regarding a real-world situation where a technically-savvy manager arbitrarily shut down a firewall protecting a critical server cluster supporting a major e-commerce company. The names, titles, and locations have been changed.

Incident Chronology

09:10

Eric Austin (Chief Engineer) calls Security stating that he noticed the Denver Internet firewall is down.

09:17

Mark Brackett (Security Director) asks if the firewall is down due to the scheduled on-site work that he knows will happen soon. Steve Dormann (Operations Manager) is located and replies at 09:41 that that work will happen next week and that today's problem is not related to any scheduled work activities. Various conference calls and ad-hoc meetings involving the cognizant managers are held to get a handle on the situation and develop courses of action.

11:24

Paula Neal (Network Architecture Manager) reports that she turned off the Denver firewall from home since she noted that the site was losing 7 out of 10 DNS queries to the rootserver located at that location.

14:30

Word that the Sprint T-1 to Denver (connecting to that rootserver) is down. Operations staff are unable to access the site to determine the scope of the problem.

Reprinted with permission of O'Reilly & Associates, Inc. Copyright © 2001. For more information, see <http://oreilly.com/>.

16:30

Adam Cronin (Rootserver Technical Coordinator) reported that the Denver firewall was brought up earlier this afternoon; however, as of this writing, the T-1 connection from Sprint is still inoperative. Security can see that the firewall is up via the Internet, but is unable to log onto the system since that internal T-1 link is down, and no modems are deployed at that site.

19:10

Steve Dormann reports the T-1 to Denver is reestablished. Operations and Security begin to review each system to determine if any compromises were made.

20:50

Mark Brackett reports to the Operations Department that their review of the nine systems in Denver did not reveal any unknown problems. He recommends a second review of these systems when the tech team is on-site next week, and that both Operations and Security monitor these servers in the interim "just to make sure."

Security Office Comments and Recommendations

The major concerns and security/operational concerns associated with this action include:

1. The arbitrary and unannounced shutdown of a required production firewall to troubleshoot a problem by someone not in the operational chain of command.
2. A failure to notify the appropriate technical staff for that site to investigate a problem.
3. The ability to log onto a production system from home.
4. A failure to notify anyone in Operations or IT Security that one of the company's production environment perimeter defenses were dropped.

The recommended near-term courses of action to resolve this issue and prevent future ones is to:

1. Have Operations staff completely rebuild the Denver firewall during their on-site visit next week.
2. Restrict access to all production firewalls (and routers, as a logical extension to this issue) to their cognizant Operations Manager, members of the Security staff, and the respective Operations technical staff members responsible for maintaining such systems.
3. Conduct a review of all users that have access to production systems in the company—not only in Denver. Anyone not holding operational day-to-day responsibility for system operations on a given system will be removed from the system.

Reprinted with permission of O'Reilly & Associates, Inc. Copyright © 2001. For more information, see <http://oreilly.com/>.

Long-term resolutions to this issue have been verbally-agreed to by both the VP/ Operations (Shreeve) and the respective Operations managers (Delaroche, Brackett, Cronin, Austin, and Dormann), and include developing a formal written policy to be published next week. Key policy and procedural changes include:

1. Passwords to production firewall applications, and the root passwords for production firewalls and routers will be known only to those individuals authorized for such access by the respective Operations Managers. These passwords will be unique for each system; a master roster will be appropriately secured in the NOC safe, with a duplicate stored in the Security Office safe.
2. Downing or modifying the rulesets or Access Control Lists (ACLs) for any production firewall or router will not be done without the advance notification, approval, and coordination of Security staff and the respective Operations Manager.
3. No one may conduct system administrative duties on any production system or router that isn't directly in the published "chain of command" for systems administration, or without documented authorization from the respective Manager.
4. Develop methods to prevent modification of production systems from remote (e.g., home) locations.

Law Enforcement Coordination

None required—Internal Investigation by Security.

Damage Assessment

Approximately six hours of staff time to resolve this issue today, plus the time to conduct a thorough on-site review next week to again confirm that no systems were compromised. No financial losses were reported by the business unit whose servers were involved.

Management Review

Paula Neal was counseled by the Security Director and Jenn Powers, the Chief Technology Officer on her actions. Paula assumed her decision to shut the firewall down was justified to ensure uptime at the Denver site—but was informed she was not authorized to make that decision without coordinating the action with the other members of the Operations Department and her manager. She admitted her actions were wrong and promised to adhere to the policy governing changes to production systems. A management letter of reprimand was signed by both Brackett and Powers and placed in Neal's personnel folder in Human Resources.

Reprinted with permission of O'Reilly & Associates, Inc. Copyright © 2001. For more information, see <http://oreilly.com/>.

Other Incident Reporting Forms Sources

Computer Incident Response Guidebook
Module 19, "Information Systems Security (INFOSEC) Program Guidelines"
<http://www.nswc.navy.mil/ISSEC/Guidance/P5239-19.html>

FCC Computer Security Incident Response Guide
<http://csrc.nist.gov/fasp/FASPDocs/incident-response/Incident-Response-Guide.pdf>

Incident Response: Investigating Computer Crime, by Kevin Mandia and Chris Prosise
Osborne/McGraw-Hill, 2001, page 18.

Cyber Threat and Computer Intrusion Incident Reporting Guidelines
National Infrastructure Protection Center
<http://www.nipc.gov/incident/newincident.htm>

State of Vermont Incident Handling Procedures
<http://www.cio.state.vt.us/pdfs/sov_intrusion_procedures.pdf>

Advance Planning for Incident Response and Forensics
Cupertino, CA: Symantec Corp., November 2001
<http://enterprisesecurity.symantec.com/SecurityServices/content.cfm?ArticleID=1557>

Bibliography

All URLs are valid as of September 2003.

[Alberts 02] Alberts, Christopher & Dorofee, Audrey. *Managing Information Security Risks: The OCTAVE Approach.* Reading, MA: Addison-Wesley, 2002.

[Allen 99] Allen, Julia, et al. *State of the Practice of Intrusion Detection Technologies* (CMU/SEI-99-TR-028). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1999. <http://www.sei.cmu.edu/publications/documents/99.reports/99tr028/99tr028chap01.html>.

[Allen 01] Allen, Julia H. *The CERT Guide to System and Network Security Practices.* Reading, MA: Addison-Wesley, 2001.

[Allgeier 00] Allgeier, Michael. "Digital Media Forensics." *SecurityFocus Online.* <http://online.securityfocus.com/infocus/1253> (2000).

[APEC 03] Asia-Pacific Economic Cooperation (APEC). <http://www.apecsec.org.sg/> (2003).

[APECTELWG 03a] Asia-Pacific Economic Cooperation (APEC) Telecommunications and Information Working Group. <http://www.apectelwg.org/apec/main.html> (2003).

[APECTELWG 03b] Asia-Pacific Economic Cooperation (APEC) Telecommunications and Information Working Group. "Computer Emergency Response Team Awareness Raising and Capability Building In-country Training for Chile, Peru, Mexico, and the Russian Federation." <http://www.apecsec.org.sg/fora/rfp_tender/rfp_tender.html> (2003).

[Arvidsson 01] Arvidsson, J.; Cormack, A.; Demchenko, Y.; & Meijer, J. *TERENA's Incident Object Description and Exchange Format Requirements.* <http://www.ietf.org/rfc/rfc3067.txt> (February 2001).

[Arvidsson 03] Arvidsson, Jimmy, ed. "Taxonomy of the Computer Security Incident related terminology." TERENA Incident Taxonomy and Description Working Group <http://www.terena.nl/tech/task-forces /tf-csirt/iodef/docs/i-taxonomy_terms.html>.

[AusCERT 01] Australian Computer Emergency Response Team. *The Methodology of Incident Handling*. <http://www.mncc.com.my/infosec2k1/panel4-3.pdf> (2001).

[AusCERT 03] Australian Computer Emergency Response Team (AusCERT). <http://www.auscert.org.au/> (2003).

[Australia 02] AusCERT; Deloitte Touche Tohmatsu; & The New South Wales Police. "2002 Australian Computer Crime and Security Survey." <http://www.auscert.org.au/Information/Auscert_info/2002cs.pdf> (2002).

[Australia 03] AusCERT, Australian Federal Police; Queensland Police, South Australian Police, Western Australian Police. "2003 Australian Computer Crime and Security Survey." <http://www.auscert.org.au/download.html?f=65> (2003).

[Berinato 01] Berinato, Scott. "Coming Up ROSI." *cso online.com*, October 26, 2001. <http://www.csoonline.com/alarmed/10262001.html>.

[Berinato 02a] Berinato, Scott. "Finally, a Real Return on Security Spending." *CIO Magazine*, February 15, 2002. <http://www.cio.com/archive/021502/security.html>.

[Berinato 02b] Berinato, Scott. "The Security Spending Mystery." *cso online.com*, April 25, 2002. <http://www.csoonline.com/alarmed/04252002.html>.

[Brezinski 02] Brezinski, D. & Killalea, T. "Guidelines for Evidence Collection and Archiving" (RFC 3227). Internet Engineering Task Force. <ftp://ftp.isi.edu/in-notes/rfc3227.txt> (2002).

[Brownlee 98] Brownlee, N. & Guttman, E. *Expectations for Computer Security Incident Response*. <http://www.ietf.org/rfc/rfc2350.txt?number=2350> (1998).

[Caloyannides 01] Caloyannides, Michael A. *Computer Forensics and Privacy.* Norwood, MA: Artech House, Inc., 2001.

[CanCERT 03] CanCERT. <http://www.cancert.ca/>.

[CERIAS 03] CERIAS Incident Response Database. <https://cirdb.cerias.purdue.edu/website/> (2003).

[CERT 02a] CERT Coordination Center. "Dealing with External Computer Security Incidents." <http://www.cert.org/archive/pdf/external-incidents.pdf> (2002).

[CERT 02b] CERT Coordination Center. *Overview of Attack Trends*. <http://www.cert.org/archive/pdf/attack_trends.pdf> (2002).

[CERT 02c] CERT Coordination Center. "Creating a Computer Security Incident Response Team: A Process for Getting Started." <http://www.cert.org/csirts/Creating-A-CSIRT.html> (2002).

[CERT 02d] CERT Coordination Center. "Computer Security Incident Response Team (CSIRT) Frequently Asked Questions (FAQ)." <http://www.cert.org/csirts/csirt_faq.html> (2002).

[CERT-NL 03] SURFnet Computer Security Incident Response Team (CERT-NL). <http://cert-nl.surfnet.nl/> (2003).

[CHIHT 03] CHIHT – Clearing House for Incident Handling Tools. <http://chiht.dfn-cert.de/> (2003).

[CIO 02] *CIO* Magazine. *CIO Cyberthreat Response & Reporting Guidelines.* <http://www.cio.com/research/security/incident_response.pdf> (2002).

[CSIRT 02] CSIRT Development Team, CERT/CC. *Computer Security Incident Response Team (CSIRT) Frequently Asked Questions(FAQ)* December 2002. <http://www.cert.org/csirts/csirt_faq.html>.

[Curry 03] Curry, D. & Debar, H. *Intrusion Detection Message Exchange Format Data Model and Extensible Markup Language (XML).* <http://www.ietf.org/internet-drafts/draft-ietf-idwg-idmef-xml-10.txt> (January 2003).

[CXO 02] CXO Media. "Fundamentals of Security." cso online.com. <http://www.csoonline.com/fundamentals/security.html> (2002).

[CXO 03] CXO Media Inc. CIO Focus Guide, "Securing Information Assets: Planning, Prevention and Response." <http://www.theciostore.com/guide_product.asp?id=84> (2003).

[DHS 2003] U.S. Department of Homeland Security, Information Analysis Infrastructure Protection, <http://www.nipc.gov/incident/cirr.htm>. (2003) (previously available from the National Infrastructure Protection Center)

[Dittrich 02] Dittrich, David A. "Developing an Effective Incident Cost Analysis Mechanism." *SecurityFocus.* <http://www.securityfocus.com/infocus/1592> (2002).

[DShield 03] Distributed Intrusion Detection System, DShield.org. <http://www.dshield.org/> (2003).

[Duffy 01] Duffy, Daintry. "Don't Press the Panic Button." *Darwin.* <http://www.darwinmag.com/read/090101/panic.html> (2001).

[EISPP 03] European Information Security Prevention Programme (EISPP). <http://www.eispp.org/> (2003).

[FCC 01] "FCC Computer Security Incident Response Guide," Federal Communications Commission, <http://csrc.nist.gov/fasp/FASPDocs/incident-response/Incident-Response-Guide.pdf>. (2001).

[Ferreira 96] Ferreira, Joao Nuno; Hansen, Alf; Klobucar, Tomaz; Kossakowski, Klaus-Peter; Medina, Manuel; Rajnovic, Damir; Schjelderup, Olaf; & Stikvoort, Don. *TERENA Task Force: CERTs in Europe, final report (updated version).* 1996. <http://www.cert.dfn.de/eng/csir/europe/terena/cerie-j7/>.

[FIRST 03] Forum of Incident Response and Security Teams. *FIRST Member Information.* <http://www.first.org/team-info/> (2003).

[Fraser 97] Fraser, B., Editor "Site Security Handbook," RFC 2196, Internet Engineering Task Force, <http://www.ietf.org/rfc/rfc2196.txt>. (1997).

[Frisch 91] Frisch, A. Essential System Administration, 2nd ed. Sebastopol, CA: O'Reilly & Associates, Inc., 1995.

[Gamertsfelder 02] Gamertsfelder, L.; McMillan, Handelsmann, & Hourigan. *E-commerce: The Implications for the Law (Report 4 - E-security).* Lawbook Company, 2002. Can be ordered at <http://onlineecom01.thomson.com.au/thomson/Catalog.asp?EES_CMD=SI&EES_ID=101510> (2003).

[Garfinkel 91] Garfinkel, Simson & Spafford, Gene. *Practical UNIX Security.* Sebastopol, CA: O'Reilly & Associates, Inc., 1996.[152]

[HB171 03] Standards Australia International Ltd. *Guidelines for the Management of IT Evidence* (HB 171-2003). <http://www.standards.com.au /catalogue/script/Details.asp?DocN=AS342335504743> (2003).

[Honeynet 03] The Honeynet Project. <http://www.honeynet.org/misc/project.html> (2003).

[152] A new edition of this book was released in 2003. However the older edition was used as the reference for this technical report.

[Howard 97] Howard, John D. "An Analysis of Security Incidents on the Internet 1989–1995." PhD Thesis, Carnegie Mellon University. <http://www.cert.org/research/JHThesis/Start.html> (1997).

[Howard 98] Howard, John D. & Longstaff, Thomas A. *A Common Language for Computer Security Incidents* (SAND98-8667). Livermore, CA: Sandia National Laboratories, October 1998.

[Incidents 03] Internet Storm Center. <http://www.incidents.org/> (2003).

[ISS 01] Internet Security Systems. "Computer Security Incident Response Planning, Preparing for the Inevitable." Atlanta, GA, 2001. <http://documents.iss.net/whitepapers/csirplanning.pdf>.

[Ito 03] Ito, Yurie. "Introduction of the APCERT, New Forum for CSIRTs in Asia Pacific." Presentation, JPCERT/CC 2003. (Copies of this presentation can be obtained by sending a request to info@jpcert.or.jp)

[JANET-CERT 03] JANET-CERT. "Case Studies: The Costs of Incidents." <http://www.ja.net/CERT/JANET-CERT/prevention/case-studies/> (2003).

[Kaplan 02] Kaplan, Simone. "Criteria for Determining the Cost of a Breach." *CSO Magazine*. <http://www.csoonline.com/read/120902 /cost_sidebar_1_664.html> (2002).

[Kessler 02] Kessler, Gary C. & Schirling, Michael. "Cracking the Cracking." *Information Security Magazine*. <http://infosecuritymag.techtarget.com /2002/apr/crackingbooks.shtml> (April 2002).

[Kossakowski 94a] Kossakowski, Klaus-Peter. *The DFN-CERT Project: The First 18 Months*. <http://www.cert.dfn.de/eng/pre99papers/6csihw1.html> (1994).

[Kossakowski 94b] Kossakowski, Klaus-Peter. *The Funding Process: A Challenging Task*. <http://www.cert.dfn.de/eng/pre99papers/6csihw2.html> (1994).

[Kossakowski 96] Kossakowski, Klaus-Peter & Stikvoort, Don. "Incident Response Teams: the European Perspective". *Proceedings, 8th Workshop on Computer Security Incident Handling*. San Jose, CA: FIRST, July 1996.

[Kossakowski 00] Kossakowski, Klaus-Peter & Stikvoort, Don. "A Trusted CSIRT Introducer in Europe: An Empirical Approach Towards Trust Inside the European Incident Response Scene—The Replacement of Trust by Expectations." Amersfoort, NL: M&I/Stelvio, 2000. (Commissioned by TERENA.)

[Kruse 02] Kruse, Warren G., II & Heiser, Jay G. *Computer Forensics, Incident Response Essentials*. Reading, MA: Addison-Wesley, 2002.

[Lundberg 01] Lundberg, Abbie. "Effective Responses to Security Incidents." <http://www.cio.com/research/security/response.html> (2001).

[Mandia 01] Mandia , Kevin & Prosise, Chris. *Incident Response: Investigating Computer Crime*. Berkeley, CA: Osborne/McGraw-Hill, 2001.

[Marcella 02] Marcella, Albert J. & Greenfield, Robert S., Ed. *Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes*. Boca Raton, FL: CRC Press LLC, 2002.

[McGlashan 01] McGlashan, Matthew. "The Methodology of Incident Handling." *InfoSecurity 2001 Conference Program*. Malaysian National Computer Confederation, 2001. <http://www.mncc.com.my /infosec2001-detail6.html> (2001).

[Mendell 01] Mendell, Ronald L. "Incident Management with Law Enforcement." *SecurityFocus Online*. <http://online.securityfocus.com/infocus/1523> (2001).

[MyCERT 03] Malaysia CERT (MyCERT). <http://www.mycert.mimos.my/>.

[Navy 96] Department of the Navy. *Computer Incident Response Guidebook, Module 19* (NAVSO P-5239-19). <http://www.nswc.navy.mil /ISSEC/Guidance/P5239-19.html> (1996).

[Nebraska 02] State of Nebraska. "Incident Response and Reporting Procedure for State Government" (Draft). Nebraska Information Technology Commission, April 2002. <http://www.nitc.state.ne.us/tp/meetings /documents/20020416/Incident_Reporting_Procedure.pdf>.

[OCIPEP 03] Office of Critical Infrastructure Protection and Emergency Preparedness. <http://www.ocipep.gc.ca/home/index_e.asp> (2003).

[Oppenheimer 97] Oppenheimer, David L.; Wagner, David A.; & Crabb, Michele D. "System Security: A Management Perspective." *Short Topics in System Administration*, Thousand Oaks, CA: SAGE Publications, Inc., 1997.

[Potter 02] Potter, C. & Smith, G "Information Security Breaches Survey 2002, Executive Summary." Available from <http://www.security-survey.gov.uk/> (2002).

[Power 02] Power, Richard. *2002 CSI/FBI Computer Crime and Security Survey*. Computer Security Institute. <http://www.gocsi.com/press/20020407.html> (2002).

[Rand 03] Rand Europe. *Computer Security Incident Response Team Handbook of Legislative Procedures*. <http://www.iaac.org.uk/csirt.htm> (2003).

[Rezmierski 98] Rezmierski, V.; Carroll, A.; & Hine, J. "Incident Cost Analysis and Modeling Project (ICAMP) I." <http://www.cic.uiuc.edu/groups/CIC /listICAMPreports.shtml> (1998).

[Rezmierski 00] Rezmierski, V.; Carroll, A.; & Hine, J. "Incident Cost Analysis and Modeling Project (ICAMP) II." <http://www.cic.uiuc.edu/groups/CIC /listICAMPreports.shtml> (2000).

[Richardson 03] Richardson, Robert. *2003 CSI/FBI Computer Crime and Security Survey*. <http://www.gocsi.com/press/20030528.jhtml> (2003).

[Riptech 01] Riptech, Inc. *Advance Planning for Incident Response and Forensics*. <http://www.riptech.com/securityresources/whitepapers.html> (2001).

[Riptech 02] Riptech, Inc. *Riptech Internet Security Threat Report, Volume II.* <http://enterprisesecurity.symantec.com/content.cfm?articleid=1539&PID=12944879&EID=0> (2002).

[Rothke 02] Rothke, Ben. "Parts of the Plan." *InfoSecurity News Magazine 13*, 8 (2002).

[SANS 98] The SANS Institute. *Computer Security Incident Handling Step-by-Step*. The SANS Institute, October, 1998.

[SANS 03] The SANS Institute. *Computer Security Incident Handling Step-by-Step*. The SANS Institute, October, 2003. Information on how to acquire this guide is available at <http://store.sans.org/>.

[Scalet 02] Scalet, Sarah. "Risk: A Whole New Game." *CSO Magazine.* <http://www.csoonline.com/read/120902/intro.html> (2002).

[Schiffman 01] Schiffman, Mike. *Hacker's Challenge: Test Your Incident Response Skills Using 20 Scenarios*. Berkeley, CA: Osborne/McGraw Hill, 2001.

[Schultz 90] Schultz, E. Eugene, Jr.; Brown, David S.; & Longstaff, Thomas A. "Responding to Computer Security Incidents." Livermore, CA: Lawrence Livermore National Laboratory. <ftp://ftp.cert.dfn.de/pub/docs/csir/ihg.txt.gz> (1990).

[Schultz 02] Schultz, Eugene & Shumway, Russell. Incident Response: A Strategic Guide to Handling System and Network Security Breaches. Indianapolis, IN: New Riders Publishing, 2002.

[SEI 03] Software Engineering Institute. "U.S. Department of Homeland Security Announces Partnership with Carnegie Mellon's CERT Coordination Center" (press release). <http://www.sei.cmu.edu/about/press/US-CERT.html> (2003).

[Shirey 00] Shirey, R. Internet Security Glossary (Network Working Group FYI 36, RFC 2828). <ftp://ftp.rfc-editor.org/in-notes/rfc2828.txt> (2000).

[SingCERT 03] Singapore Computer Emergency Response Team (SingCERT). <http://www.singcert.org.sg/> (2003).

[Smith 94] Smith, Danny. "Forming an Incident Response Team." *Proceedings of the FIRST Annual Conference*. University of Queensland, Brisbane, Australia, July 1994. <http://www.auscert.org.au/render.html?it=2252&cid=1920>.

[Sokol 00] Sokol, Marc S. & Curry, David A. "Security Architecture and Incident Management for E-business." Atlanta, GA: Internet Security Systems, 2000. <http://www.iss.net/support/documentation /whitepapers/technical.php>.

[Steele 02] Steele, Gordon. "Information Systems Security Incident Response." *IANewsletter 5*, 1 (Spring 2002): 14–21.

[Swanson 02] Swanson, Marianne; Wohl, Amy; Pope, Lucinda; Grance, Tim; Hash, Joan; & Ray, Thomas. "Contingency Planning Guide for Information Technology Systems." *NIST Special Publication 800-34*, National Institutes of Standards and Technology. <http://csrc.nist.gov/publications/nistpubs/800-34/sp800-3.pdf> (2002).

[Symantec 01] Symantec Corp. "Advance Planning for Incident Response and Forensics." Cupertino, CA: Symantec Corp., November 2001. <http://enterprisesecurity.symantec.com/SecurityServices /content.cfm?ArticleID=1557>.

[Symantec 02] Symantec Corp. *Symantec Internet Security Threat Report*, Volume II. <http://enterprisesecurity.symantec.com /content.cfm?articleid=1539&PID=12944879&EID=0> (2002).

[Taylor 02] Taylor, Laura. "Incident Response Planning and Management." *Intranet Journal,* <http://intranetjournal.com/articles/200201/pse_01_28_02b.html> (2002).

[TERENA 03] TERENA Task Force. "CSIRT Coordination for Europe." <http://www.terena.nl/task-forces/tf-csirt/> (2003).

[TI 03] Trusted Introducer (T1) for CSIRTs in Europe. <http://www.ti.terena.nl/> (2003).

[US-CERT 03] United States Computer Emergency Response Team (US-CERT). <http://www.us-cert.gov/> (2003).

[USSS 01] United States Secret Service. "Cyber Threat/Network Incident Report," Secret Service Form 4017. <http://www.treas.gov/usss/net_intrusion_forms.shtml> (2001).

[van Wyk 01] van Wyk, Kenneth R. & Forno, Richard. *Incident Response*. Sebastopol, CA: O'Reilly & Associates, Inc., 2001.

[Vermont 01] State of Vermont. *Incident Response Procedure*. <http://www.cio.state.vt.us/pdfs/sov_intrusion_procedures.pdf> (2001).

[Villano 01] Villano, Matt. "I.T. Autopsy." *CIO.com*. <http://www.cio.com/archive/030101/autopsy.html> (2001).

[Wack 91] Wack, John P. "Establishing a Computer Security Incident Response Capability (CSIRC)." *NIST Special Publication 800-3,* National Institutes of Standards and Technology. <http://csrc.nist.gov/publications/nistpubs/800-3/800-3.pdf> (1991).

[West-Brown 03] West-Brown ,Moira J.; Stikvoort, Don; Kossakowski, Klaus-Peter; Killcrece, Georgia; Ruefle, Robin; & Zajicek, Mark. *Handbook for Computer Security Incident Response Teams (CSIRTs)* (CMU/SEI-2003-HB-002). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2003. <http://www.sei.cmu.edu /publications/documents/03.reports/03hb002.html>.

[Wood 01] Wood, Charles Cresson. *Information Security Policies Made Easy*. San Jose, CA: NetIQ Corp., 2001. <http://www.pentasafe.com/publications/ispme.asp>.

[Wright 01] Wright, Timothy E. "How to Design a Useful Incident Response Policy." *SecurityFocus Online.* <http://online.securityfocus.com/infocus/1467> (2001).

[Zeichner 03] Zeichner, Lee & Almosd, Robert. "State Implementation of Federal Cyber-Security Requirements." Zeichner Risk Analytics, 2003. <http://www.zra.com/docs/summaryReport.pdf>.

Index

@stake, 157
abnormal network traffic, 67
abuse of network resources, 82
academic research networks, 27
academic sponsorship, 55
acceptable use documents, 77
accreditation, 26, 28, 40, 80, 120
ACID, 125
actuarial models, 64
ad hoc teams, 53, 56, 69, 71, 83, 89, 99, 107
Additional Protocol to the Convention on Cybercrime, 116
administrative support staff, 73, 76
Advance Planning for Incident Response and Forensics, 152
adverse event, 82
advisories, 55, 67, 75, 98, 123, 134
Air Force Computer Emergency Response Team (AFCERT), 21
AirCERT, 125
alerts, 67, 88, 98, 120, 134
Ames Research Center Computer Network Security Response Team, 21
analysis, 86
    centers, 14
    tools, 57
Analysis Console for Intrusion Databases, 125
anecdotal information, 133
APCERT, 28, 38, 40, 122
APEC, 29
APECTEL, 29
APSIRC Working Group, 28
APSIRT, 30
ArCERT, 31
archives, data, 124
ARPANET, 17
artifact analysis, 21, 68
artifacts, 2
Asia Pacific
    coordination of teams, 28
    CSIRT training, 30
    CSIRTs, 27, 28, 29
Asia Pacific Computer Emergency Response Team. *See* APCERT
Asia Pacific Networking Group (APNG), 28
Asia Pacific region, 23
Asia Pacific Regional Internet Conference on Operational Technologies, 29
Asia Pacific Security Incident Response Coordination (APSIRC), 28
Association of European Research Networks, 22
asymmetric threat, 111
AT&T Latin America - Peru Security Incident Response Team, 30
attack tools, distributed, 110
attacks, 11, 67, 109, 128
    speed of, 111
audit department, 51, 65
auditors, 76
audits, 5, 65
AusCERT, 23, 27, 28, 51, 55, 63, 72, 82, 97
Australian Computer Crime and Security Survey, 104
Australian incidents, 63
Australian Standard for Managing IT Evidence, 124
Australian/Deloitte Touche Tohmatsu/NSW survey, 61
authority, CSIRT, 49, 53, 111, 129
Automated Incident Reporting, 125
automated scanning. *See* scanning
automation
    of attack tools, 110
    of incident handling, 135
availability, 116
Bach Khoa Internetwork Security Center, 28
Backbone Security, 157
Bank of Montreal InfoSec Incident Response Team, 32
BCP 55/RFC 3227, 115
benchmarking, 3, 130
benefits

CSIRT staff, 57, 60
of CSIRTs, 64
Best Current Practice, 115
best practices, 74, 75, 84, 85, 86, 130, 134, 137, 169
Best Practices for Seizing Electronic Evidence, 115
Biber, David, xiv
binary files, 91
BKIS, 28
Blaster worm, 111
BMO ISIRT, 32
bottom-up approach, 23
Bradley, Diane, xiv
Brazilian Federal Police, 32
Brazilian Internet Steering Committee, 31
Brazilian Research Network CSIRT, 30
breach of information, 61
break-in, 93
British Standards (BS), 4
BS EN ISO17799, 85
BS7799, 85
budgets, 56, 72, 129
Bunten, Andreas, xiii
burnout, 78
business
case, 56, 64
continuity plans, 64
hours, 102
intelligence, 12, 64
CAIF, 123
CAIS, 30, 31
California security law, 115
Canadian Computer Incident Response Coordination Centre, 32
Canadian CSIRTs, 32, 33
CanCERT, 55
Carnegie Mellon University, 19, 34
case laws, 114
case studies, 100, 130, 133
categorizing
incidents, 95
reports, 91
CdnCIRCC, 32
Center for Education and Research in Information Assurance and Security, 62
Centers of Academic Excellence in Information Assurance Education, 79
CEOs, 107
CERIAS Incident Response Database, 62, 95
CERNET Computer Emergency Response Team, 28
CERT, 19
CERT Coordination Center. *See* CERT/CC
CERT CSIRT Development Team, ix, 3, 6, 13, 15, 59
CERT Guide to System and Network Security Practices, 82, 131, 151
CERT/CC, ix, 8
AirCERT project, 125
annual CSIRT conference, 22
certification program, 80, 162
coordination with, 107
courses, 157
CSIRT course attendance, 46
Current Activity web page, 125
evolution, 51
FIRST membership, 21
funding, 55
incident reporting form, 92
influence on early European teams, 23
origin of, 19
Overview of Attack Trends, 110
response to WANK worm, 20
statistics, 112
CERT-BUND, 95
CERTCC-KR, 27, 28, 46
CERT-Certified Computer Security Incident Handler, 80
certification, 26, 77, 80, 134, 135, 137, 162
Certified Incident Handler, 80
Certified Information Systems Security Professional, 80
CERT-NL, 22, 55
CERT-RS, 32
CERTs in Europe task force, 24
challenges, 48, 56, 59, 91, 112, 128
checklists, 130, 137
Chief Information Officers (CIOs), 4, 52, 106
Chief Security Officers (CSOs), 4, 52
CHIHT, 127
child pornography, 116
Chilean Computer Emergency Response Team, 30
China Computer Emergency Response Team Coordination Center, 28
CIAC, 21

CIO, 84, 92
CIRC, 13
CIRT, 13
CISSP, 80
civil liability, 114
CLCERT, 30
clearances, 77
Clearinghouse for Incident Handling Tools, 119, 127
CNCERT/CC, 28
Code Red worm, 114
collaboration, 26, 119
collecting evidence, 178
Committee of Ministers of the Council of Europe, 116
Common Advisory Interchange Format, 123
Common Body of Knowledge, 80
common laws, 114
communication
    channels of, 112
    mechanisms, 18
    secure, 105
    skills, 76
    tools, 101
compliance
    department, 51
    requirements, 33
compromise, 58
CompTIA, 162
computer crime, 60, 62, 104, 114, 115, 118
computer crime laws, state, 118
Computer Emergency Response Team, 19
Computer Emergency Response Team Coordination Center-Korea. *See* CERTCC-KR
Computer Emergency Response Team for the German Research Network DFN. *See* DFN-CERT
computer forensics. *See* forensics
Computer Forensics, Incident Response Essentials, 151
Computer Fraud and Abuse Act, 118
Computer Incident Advisory Capability, 20, 21
Computer Incident Response Guidebook, 155
computer network attack, 82
Computer Network Defense Service Providers, 80
computer security, 49, 53, 60, 82, 133
    experts, 122
    incidents, 122
    terminology, 134
Computer Security Incident Handling Step by Step, 152
Computer Security Incident Response Planning, 97, 153
computer security incident response teams, ix
computer security incidents, 71, 109
Computer Security Institute (CSI), 157
Computer Security Institute/Federal Bureau of Investigation Computer Crime and Security Survey, 60
Computer Security Resource and Response Center, 21
CONCERT, 46
confidential information, 106
confidentiality, 116
configuration maintenance, 12
consortium sponsorship, 55
constituencies, 22, 49
contact information, 91, 92, 120
containment, 83, 86
Contingency Planning Guide for Information Technology Systems, 153
contract services, 55
Convention on Cybercrime, 116
coordination, 21
    function, 12
    issues, 129
    mechanisms, 119, 129, 135
    network, 20
    of teams, 24, 26, 35, 47
    with other external entities, 106
    with other teams, 106
coordination centers, 14, 53, 69, 89, 99, 107, 108
copyright
    law, 116, 171
    violations, 58
core team, 73, 74
Cormack, Andrew, xiii
Coroner's Toolkit, The, 100
corporate security, 73
correlating incident activity, 90
correspondence, capturing data from, 91
costs, 137
    computer crime, 62
    CSIRT, 54, 57

incident, 58, 59, 62, 91
of CSIRTs, 63
recovery, 11
staff, 54
start-up, 54
sustainment, 54
Council Framework Decision, 117
Council of Europe, 116, 165
Council of the European Union, 116
courses, 139, 157
court
cases, 76
evidence, 57, 90, 101, 114
testimony, 77
criminal
investigation, 90
investigative staff, 73
law, 116
liability, 114
Criminal Intellectual Property Laws, 170
Crisis Action Meeting, 106
crisis management, 5
critical
assets, 12, 65, 128
incident information, 90, 92
information, 131
infrastructure, 32, 33
services, 64, 112
cryptographic keys, 120
cryptography, 105
CSI/FBI Computer Crime and Security Survey, 103, 112
CSIRC, 13
CSIRT
agreements, 24
authority, 111
certification, 80
community, 26
composition, 8
constituencies, 5, 11, 49
coordination, 24, 28, 55
courses, 139
evolution, 51
framework, 86
growth, 133
infrastructure, 25
managers, 4, 49, 73, 74
models, 15, 69, 72, 89, 99, 107, 108, 137
organizational structure, 49
processes, 9, 133
projects, 118
propagation, 48
responsibilities, 8
sectors, 7, 16, 42, 46, 89, 103, 133, 137
support, 47
team leads, 74
CSIRT Basic Skills, 78
CSIRT FAQ, 82
CSIRT for the National Autonomous University of Mexico, 30
CSIRT Handbook of Legislative Procedures, 117
CSIRT Organizational Survey, 80, *See* survey
CSIRT Services, 12
CSIRT Task Force. *See* TF-CSIRT
CSIRTs
American, 33, 34, 40, 43
Asian, 27, 28, 29, 43
Australian, 23, 27
banking and finance sector, 7, 46, 69, 89, 99, 104, 105, 107
Canadian, 32, 33, 40, 43
centralized, 53, 69, 89, 105, 107, 108
combined, 53, 69, 72, 89, 99, 105, 107, 108
commercial sector, 7, 26, 27, 33, 42, 43, 54, 69, 89, 99, 105, 107, 108
communication and information sector, 7, 89
coordinating, 16, 53, 54, 69, 89, 99, 107, 108
critical infrastructure, 33, 46
defined, ix
described, 11
distributed dedicated, 70, 89, 99, 105, 107, 108
distributed part-time, 53, 70, 71, 89, 99, 105, 107, 108
education sector, 7, 33, 52, 57, 69, 89, 99, 102, 103, 104, 105, 108
establishing, 6, 49
European, 22, 23, 24, 25, 26, 27, 39, 40, 43
first, 19
government, 26, 27, 31, 33, 42, 46
growth of, 38, 39, 42
information and communication sector, 69, 99, 102, 105, 107, 108
insurance sector, 46

internal, 14, 92
internal centralized, 15
internal combined, 15
internal distributed, 15
ISP, 33, 43, 44, 47
Latin American, 30, 31, 32, 43
law enforcement, 7, 46
lists of, 38
military sector, 7, 33, 52, 54, 57, 69, 71, 102, 104, 105, 108
national, 28, 42, 43, 46, 51, 54
non-profit sector, 7, 31, 33, 54, 57, 69, 89, 99, 103, 104, 105, 108
number of, 38
operating, 6
placement in organization, 49, 51
power and energy sector, 46
proactive functions of, 11
public administration, 7
reactive functions of, 11
registered, 40, 45
research, 31, 32, 33, 42, 43, 54
research network, 104
security company, 47
size of, 71
state government, 33
telecommunications sector, 31, 32, 33
transportation sector, 46
types of, 14
university, 31, 32, 45, 47, 54, 59
CSIRTsectors, 99, 107
CSRC, 21
cultural differences, 23
Curry, D. A., 85
Curtis, Pamela, xiv
customer privacy policies, 64
customer service, 76
cyber
crime, 114, 117
crime laws, 114, 116, 118, 137, 165
forensics. *See* forensics
insurance, 64
security, 33
security laws, 34
space, 117
damage estimates, 59
DARPA, 18
data
archiving, 124
collection, 122, 124, 125
management, 134
privacy, 33
protection requirements, 11, 64, 118
repository, 75
synthesis, 125
database tools, 59
DECNET, 20
Defense Advanced Research Projects Agency. *See* DARPA
Defense Communication Agency, 21
Defense Data Network, 21
definitions, of computer incident terms, 82
Deloitte Touche Tohmatsu, 82
denial-of-service attacks, 58, 61, 93, 103, 110, 118
Department of Trade and Industry (U.K.), 61
detection, 83, 86, 133
DFN-CERT, 22, 51, 95
diagnostic procedures, 67
Digital Equipment Corporation, 20
disaster recovery, 73
disseminating information, 74
distributed attack tools, 110
Distributed Intrusion Detection System, 126
DITSCAP, 174
Dittrich, David, 59
DND CIRT, 32
DNS (Domain Name System), 111
DoD Directive 8530.1, 80
DoD Instruction 8530.2, 80
DShield.org, 126
eCSIRT, 84
eCSIRT.net, 72, 120
EISPP, 121
Electronic Crime Scene Investigation: A Guide for First Responders, 115
electronic records, 124
email relays, 17
EnCase, 100
encrypted information, 91
eradication, 83
establishing CSIRTs, 49
ETS no. 185, 116
ETS no. 189, 116
EU. *See* European Union
EuroCERT, 24, 27
European
constituencies, 23
coordination center, 24

CSIRTs, 21, 22, 24, 25, 26, 27, 39, 43, 119
directory of, 38
research networks, 22, 23
European Commission, 116
European Commission's Information Society Directorate-General, 117
European CSIRTs Directory, 46
European Data Protection regulations, 64
European Information Security Promotion Programme, 121
European Information Societies Technology, 120
European Parliament, 116
European Union, 26, 116, 166
evidence, 57, 90, 114
evidence collection tools, 101
EWA-Canada/CanCERT, 32
exchanging incident data, 25, 84, 94
Expectations for Computer Security Incident Response, 84, 124
expert staff, 58
expert testimony, 77
exploitation scripts, 109
extended team, 73
extranets, 105
facsimile, capturing data from, 91
FBI, 84
FedCIRC, 55
federal computer intrusion laws, 170
Federal Information Security Management Act, 118, 174
federal regulations, 118
fee-based services, 55
Fifth Framework Programme, 121
financial
fraud, 61
institutions, 64
loss, 60, 61, 85
financial services industry, 118
Financial Services Modernization Act of 1999, 64
fire department analogy, 11
firewall logs, 126
FIRST, 21, 27, 46, 158
conferences, 20, 27, 30, 48
creation of, 21
founding members, 21
growth of, 38
members, 27, 30, 31, 32, 33
regional distribution, 39
sponsorship, 47
Team Members List, 38
first responders, 73, 74
FISMA, 118
Fithen, Katherine, xiv
flowcharts, 130, 179
forensic
analysis, 9, 49, 67, 76, 101
evidence, 67, 99
evidence collection, 68, 76, 77, 100, 124
examinations, 101
services, 57
forensics, 9, 79, 100, 109, 157
formalization of procedures and formats, 135
formats for exchanging incident data, 119
forms, 137, 179
Forno, R., 92
Forum of Incident Response and Security Teams. *See* FIRST
Foundstone, 158
framework
accreditation, 26, 120
CSIRT, 86
European, 121
legal, 117
fraud, 103, 114, 116
Freeman Incident Tracking System, 95
full authority, 53
full-time staff, 72
funding, 54, 56, 128, 135
funding strategies, 55
G8. *See* Group of 8
Gartner, 57
German Research Network, 87
Global Information Assurance Certification (GIAC), 80, 162
Global Knowledge, 158
goals, 51, 84, 85
Goddard Space Flight Center, 21
GOVCERT.NL, 27
Government of Canada, 33
government sponsorship, 55
Gramm-Leach-Bliley Act, 64, 118, 174
grass-roots approach, 23
Green, John, xiii
Griffith University, 27, 63
GRIP, 34, 84
Group of 8, 117, 168
guidelines

incident handling, 84
reporting, 92
sample, 130, 179
Guidelines and Recommendations for Incident Processing, 34
Guidelines for Evidence Collection and Archiving, 115, 124
hacker attacks, 58, 103
hacker scanning tools, 61
Hacker's Challenge, 130
Handbook for CSIRTs, xiii, 5, 6, 48, 53, 72, 78, 87, 109, 139
Handlers Diary, 126
harassment, 103
harmful code, 58
Harvey, Christopher C., 20
HB-171-2003, 124
health care providers, 118
health insurance, 118
Health Insurance Portability and Accountability Act (HIPAA), 118
Heiser, J., 92
Helminthiasis of the Internet, The, 17
help desks, 55, 67, 73, 74, 88, 94, 102
high bandwidth, 112
high-stress positions, 79
high-tech crime, 117
hiring regulations, 77
HKCERT/CC, 29
Hoepers, Cristine, xiii
home users, 112
Honeynet Project, 128
Hong Kong Computer Emergency Response Team Coordination Center, 29
host systems, 17
hotline, 19, 68, 71, 73, 74, 88, 102
hours of operation, 102
human resources, 5, 73, 75
hurricane severity levels, 97
Hysert, Ronald H., 20
IAP, 116
ICAMP, 58, 59, 60
IDCERT, 29
IDMEF, 94, 121
IDS, 67, 68, 70, 88, 123, 125
IETF, 34, 84, 93, 121
IHT, 13
illegal software, 58
improvement, 86, 133
INCH, 25
INCH Working Group, 84, 122
incident
analysis, 13, 66, 71
analysts, 73
cost model, 59
costs, 58, 62
data, 67
data exchange, 135
definition of, 82
detection services, 12
handlers, 74, 114
level, 95
life cycle, 87
management, 85, 86
priority, 95
reporting forms, 89, 92, 125, 131
reporting procedures, 82
reports, 66, 95
scope, 93
severity, 95
statistics, 112, 120
tracking systems, 62, 75, 122
Incident Cost Analysis and Modeling Project. *See* ICAMP
incident handling
by early European teams, 23
by platform specialists, 75
definition of, 13
field, 78, 133
guidelines, 84
knowledge, sharing of, 49
methodologies, 134
procedures, 85
service, 65, 66
skills, 78
staff, 73, 128
time data, 59
tools, 122, 127
training, 79
Incident Handling Step-by-Step, 82, 101
Incident Handling Working Group. *See* INCH Working Group, *See* INCH
Incident Object Description and Exchange Format. *See* IODEF
incident response
activities, 86
capability, xi
checklist, 85
CSIRT authority for, 53
definition of, 13, 83
field, 2, 133

function, 66
in Asia Pacific region, 28
laws and regulations, 115
literature, 8
methodology, 131
planning, 109
plans, 9, 84, 112
processes, 83, 131
providers, 15
time data, 59
tools, 127
training, 79
Incident Response, 56, 151
Incident Response and Reporting Procedure for State Government, 154
Incident Response: A Strategic Guide to Handling System and Network Security Breaches, 151
Incident Response: Investigating Computer Crime, 151
incidents
number of, 104
prevention of, 21
types of, 58
Incidents.org, 126
indirect costs (of incidents), 60
Indonesia Computer Emergency Response Team, 29
information
assets, 11
assurance, 49, 79
disclosure, policies and practices, 75
exchange, 122
security, 56, 79, 85, 118, 157
sharing, 21, 26, 106, 122
systems, 117
Information Security, 100
Information Security Breaches Survey, 61, 103
information security programs, 160
Information Systems Security Incident Response, 152
Information Systems Security Officers (ISSOs), 4
InfoSecurity News, 109
infrastructure attacks, 111
Infrastructure Protection Coordination Centre, 33
insider abuse, 61
instant messaging, 110
Instituto Tecnológico y de Estudios Superiores, 30
insurance premiums, 64
intangible costs (of incidents), 60
integrity, 77, 116
intellectual property, 118, 170
interface standards, 134
international
cooperation, 116, 117
coordination, 55
cyber crime laws, 116, 165
International Association of Chiefs of Police, 115
International Information Systems Security Certifications Consortium, 80, 162
International Organization on Computer Evidence, 115
International Standards Organization, 4
Internet, 112, 125, 126
Internet Engineering Task Force. *See* IETF
Internet Glossary, 83
Internet Relay Chat, 110
Internet Security Systems, 57, 85
Internet Society, 115
Internet Worm. *See* Morris Worm
intranets, 92, 105
intruder
activity, 128
attacks, 87
trends, 12
Intrusion Detection Message Exchange Format, 94
intrusion detection systems. *See* IDS
Intrusion Detection Working Group, 123
investigations, 5
investigative process, 114
IOCE, 115
IODEF, 25, 91, 94, 119, 121, 122
IRC, 13
Ireland, Terry, xiv
IRF. *See* incident reporting forms
IRT, 13
ISO 17799, 85
ISPs, 43, 44, 54
ISS, 97
IT
department, 51, 65, 68, 70, 83, 100, 106
help desks, 102
managers, 4, 52

security, 56, 124
support staff, 73, 111
ITESM, 30, 31
Ito, Yurie, xiii
JANET-CERT, 60, 94
Japan Computer Emergency Response Team Coordination Center (JPCERT/CC), 14, 27, 28, 29
job descriptions, 75, 77, 78
judicial opinions, 114
judicial proceedings, 77, 124
justification to management, 6
key policies, 120
Kossakowski, Klaus-Peter, xiii
Kruse, W., 92
laptop theft, 61
Laswell, Barbara, xiii
Latin America, 30, 31, 32
law enforcement
agencies and organizations, 5, 13, 176
coordinating with, 105, 106
CSIRTs, 98
exchanging data with, 123
in extended CSIRTs, 76
interacting with, 74
involvement in forensic analysis, 101
involvement in incident reporting, 93
reporting incidents to, 104, 114
role in collecting evidence, 101
working relationships with, 115, 136
law resources, 177
Lawrence Livermore National Laboratory, 21
laws, 64, 75, 114
local, 11
national, 11
Learning Tree International, 163
legal
counsel, 115
department, 5, 75, 106
investigations, 68
issues, 114, 124, 137
precedents, 64
requirements, 93, 133
staff, 73, 74
legitimate services, 111
lessons learned, 24, 63, 76, 86, 87
level of service, 71
liability issues, 75
liaison, CSIRT as, 105
LionTech IT Ltd., 158
List of CSIRT Services, 65
local teams, 54
logging information, 94
Lopéz, Juan Carlos Guel, xiii
loss minimization, 12
loss of life, 85
Lotus Notes, 94
Love Letter worm, 114
Lyon Group, 117
major events, 73
Malaysian Computer Emergency Response Team, 29
malicious attacks, 112
managed security service providers. *See* MSSPs
management
buy-in, 5, 62
perspective, 67
requirements, 90
skills, 77
support, 128, 136
managers, CSIRT, 49, 73, 74
managing incident workload, 90
MCI WorldCom, 55
McMillan, Rob, xiii
media
department, 5
relations, 74, 75, 105
specialists, 73
Megamind, Institute for Advanced Technology Training, 158
Melissa virus, 114
membership fees, 27, 28, 55
mentoring, 74, 134, 137
message centers, 102
methodologies
data exchange, 84
incident handling, 14, 87, 134
Methodology of Incident Handling, The, 153
methods, intruder, 109
Mexican Computer Emergency Response Team, 30
Microsoft Access, 94
Microsoft Certified Systems Administrator, 81
Microsoft Windows, 101
military coordination centers, 67
military CSIRTs, 71
MIS Training Institute, 158, 163

mission, 51, 74, 77, 84, 90, 93, 98, 105, 124, 129
mission statement, 51
misuse of resources, 11
models, 15, 53, 69, 72, 89, 99, 107, 108, 137
monitoring
IDS, 68, 70
of network and system logs, 68
Morris Worm, 17
MSSPs, 16, 44, 46, 51, 55, 98
multi-layered security strategy, 1
mutual assistance, 117
Mx-CERT, 30, 31
MyCERT, 29, 55, 56
NASA, 19, 21
NASA ARC CNSRT, 21
National Autonomus University of Mexico, 31
National Computer Security Center, 18
National Cyber Security Division, 34
National Hurricane Preparedness Center, 97
National Institute of Justice, 115
National Institute of Standards and Technology. *See* NIST
national research networks, 22, 44
National Security Agency, 18, 79
Naval Computer Incident Response Team (NAVCIRT), 21
NBSO, 30, 31
Nebraska, State of, 85
network
activity, 125
administrators, 5
monitoring programs, 88
sensors, 88
services, 17
sniffer programs, 109
surveillance techniques, 130
New South Wales Police, 82
New Technologies Inc. (NTI), 159
NIC BR Security Office - Brazilian Computer Emergency Response Team, 30
Nimda worm, 114
NIST, 19, 20, 21, 83, 161, 163
NIST Contingency Planning Guide for Information Technology Systems, 131
NIST Special Publication 800-34, 153
NITC, 92
no authority, 53
non-disclosure agreements, 75, 77, 106
notification lists, 112
NT/2000, 101
number of incidents, 104
Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP), 33
off-the-shelf recording products, 94
OILZ, 20, 21
operational coordination, 135
operational guidance, 74
Oracle, 94
organizational models. *See* models
Organizational Models for CSIRTs, 5, 6, 16, 65
organizational structure, 49, 135
orientation, of new employees, 77
Ottawa, 33
outsourcing, 65, 75, 101
parent organization funding, 55
part-time staff, 72
penetration testing, 68, 75
perpetrators, 105
personnel. *See* staff
Pethia, Richard D., 20
PGP, 105
PH-CERT, 29
Philippine Computer Emergency Response Teams, 29
PHP, 125
pitfalls, 48
plan of action, 14
platform specialists, 73, 75
point of contact, 24, 28, 85, 117
policies and procedures, 47, 59, 75, 83, 84, 86, 98, 108, 112, 115, 124, 127, 134, 179
policy attributes, 109
policy design and implementation, 108
polymorphic tools, 111
postmortem, 83
post-secondary education institutions, 49
practices, 82
preparation/protection, 83, 86, 133
PRESECURE, 159
Presidential Decision Directive 63, 173
Pretty Good Privacy, 105
prioritizing
activities, 106, 129
incidents, 95

incoming information, 74
priority scales, 98
privacy issues, 118, 124
privacy laws, 101, 114, 173
proactive services, 65, 86, 114, 133
probes, 93, 103
procedural law, 116
procedures. *See* policies and procedures
process guidelines, 137
processes, 14, 86, 87, 88, 133, *See also* policies and procedures
product security teams, 44
productivity loss, 63
professional development, 78
project leaders, 4
projects, CSIRT, 118
protocol flaws, 109
public
outreach, 34
relations, 5, 73, 75
services, 55
public key cryptography, 105
Putting on the Gloves, 101
Queensland University of Technology, 27, 63
racist acts, 116
rapid response, 12
RARE CERT Task Force, 23
reactive services, 65, 86, 114
recording data, 89, 91, 94
recovery, 12, 18, 64, 99
Red Siren, 159
registered teams, 21, 32, 38, 40, 42, 43, 45
regulations, 11, 33, 64, 75, 93
Remedy HelpDesk and Action Request System, 94
repair costs, 64
repeatable process, 136
reporting
guidelines, 84
incidents, 85
structures, 49, 51, 52
reputation, 76, 85
Request Tracker for Incident Response, 94
requirements for establishing a CSIRT capability, 135
research, 128
networks, 26, 42, 45, 52
sponsorship, 55
Réseaux Associés pour la Recherche Européene, 23
Responding to Computer Security Incidents: Guidelines for Incident Handling, 153
response, 86, 133
and recovery, 12
capability, 56, 64
plans, 111
services, 90
strategies, 12, 98
response team network, 20
responsibilities, staff, 51, 74, 77
retaining information, 93
revenue loss, 64
Reynolds, J., 17
RFC
1135, 17
1244, 154
2196 Site Security Handbook, 154
2350, 34, 84, 124
2828, 83
3227, 124
risk, 11, 65, 66, 85
assessments, 76
data, 12
management, 5, 76
mitigation, 12
models, 64
Rogers, Stephanie, xiv
roles, staff, 51, 77
Rosenthal, Sheila, xiv
routers, 111
RTIR, 94
sabotage, 61
SafeBack, 100
Safer Internet Action Plan, 116
SAGE, 78, 108
salary costs, 56, 57, 60
SANS, 82, 92, 101, 126, 159
SANS Security Alert, 57
SC Magazine, 163
scanning, 11, 61, 93, 103, 109
scope
of CSIRT activity, 85
of incidents, 93
search and seizure, 101
Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, 115
secretarial staff, 73
Section 1030, 118

sectors, 7, 16, 42, 46, 89, 99, 103, 107, 133, 137
secure communications, 105
secure practices, 129
Securing Information Assets: Planning, Prevention and Response, 153
security
  awareness training, 12, 65, 68, 75, 77, 86, 128
  breaches, 64, 85, 115
  clearances, 77
  configuration, 68, 86
  consulting, 12
  department, 51
  experts, 15, 73
  flaws, 109
  managers, 52
  policies, 12
  policy development, 67
  practices, 64
  product development, 68
  teams, 15, 16, 68, *See also* ad hoc teams
  weaknesses, 88
Security Architecture and Incident Management for E-business, 153, 154
Security Emergency Response Team, 27
SecurityMap.Net CERT, 29
SEI, 18
Senior Experts Group on Transnational Organized Crime, 117
SERT, 13, 27, 63
servers, 17
service interruptions, 58
service level agreements, 75
service quality management services, 66
services, 55, 56, 65, 66, 73, 88, 98, 105, 124
severity scales, 98
shared authority, 53
sharing information, 106, 122
Siemens, 55
Singapore Computer Emergency Response Team (SingCERT), 27, 28, 29
SIRT, 13
size, of CSIRTs, 71
skills, 49, 76
Slammer worm, 111, 114
Snort, 125
Sobig.F, 111
Software Engineering Institute, 18
Sokol, M. S., 85
Solha, Liliana Velásquez, xiii
sophistication of attacks, 72
source code, 109
Space Physics Analysis Network (SPAN), 20, 21
spamming, 103
SPAN CERT, 21
SPAN-France, 21
speed of attacks, 111
sponsorship, 47
SQL, 94, 111
SQL/Slammer worm, 114
staff, 4, 49
  burnout, 78
  costs, 54, 57, 60
  full-time, 72
  number of, 71
  part-time, 72
  positions, 72
  responsibilities, 56, 74, 77, 84
  roles, 77
  skills, 76
  training, 26
staffing levels, 90
standards, 64, 119, 122, 134
  interface, 134
  professional, 134
start-up costs, 54
state computer crime laws, 118
State of the Practice
  structure, 6
  summary, 133
  uses, 5, 6
State of the Practice project, 3
State of Vermont Incident Handling Procedure, 154
Statement on Auditing Standards (SAS) No. 70, 175
statistics, incident, 90, 120
statutory laws, 114
Steinauer, Dennis, D., 20
Stikvoort, Don, xiii
strategic direction, 74
strategic plan, 5
stress, 76
SURFnet, 55
SURFnet Computer Security Incident Response Team, 22
surveillance techniques, 101

survey, xii, 5, 49, 52, 55, 67, 71, 81, 88, 94, 99, 129, 137
constituencies, 50
description of, 6
of organizational structures, 2
participants, 7
sectors, 7, 16
sustainment costs, 54
Symantec, 109
synthesizing incident data, 125
SysAdmin, Audit, Network, Security Institute. *See* SANS
system
administrators, 5, 78, 114
downtime, 63
owners, 107
penetration, 61
weaknesses, 66
System Security: A Management Perspective, 152
Taiwan Computer Emergency Response Team/Coordination Center, 29
Taiwan Computer Incident Response Coordination Center, 29
taxonomy, 82, 84, 134, 137
team leads, 73, 74
team size, 71
teamwork, 77
technical
advice, 67
advisories, 12
analysis, 67
documentation, 68, 75, 98, 99
perspective, 67
staff, 73, 77
writers, 75
techniques, intruder, 109
technology watch, 68, 69, 74
telecom eavesdropping, 61
telecommunications, 106
telecommunications fraud, 61
telephone calls, capturing data from, 91
TeliaCERTCC, 84
templates, 58, 92, 130, 134, 137, 179
TERENA, 24, 26, 119, 122, 127
terminology, 9, 13, 82, 134
testimony, 77
TF-CSIRT, 25, 48, 121, 122, 127
Thai Computer Emergency Response Team (ThaiCERT), 29
theft, 61, 75, 103, 114
TheTrainingCo., 159
third-party answering services, 102
threat metrics, 76
threats, 11, 65, 66, 67, 83, 87, 112, 126
TI. *See* Trusted Introducer
TI Review Board, 120
time zones, 93
Title 17 - Copyrights, 171
Title 18, 118
Title 18 – Crimes and Criminal Procedure, 171
Title 35 - Patents, 172
toolkits, 109
tools, 119, 127, 130
evidence gathering, 127
evidence investigation, 127
intruder, 109
proactive, 127
remote access, 127
system recovery, 127
tools of the trade, 101
tracking and tracing, 67, 68, 89, 91, 94
training
department, 65
forensics, 100
materials, 74
of CSIRTs, 25, 28, 29, 47, 49, 54, 57, 79, 81, 135, 137, 139, 157
programs (college and university), 160
security awareness, 12, 65, 68, 75, 77, 86
Training of Network Security Incident Teams Staff, 25
Trans-European Research and Networking Association. *See* TERENA
TRANSITS, 25, 159
transnational organized crime, 117
trap and trace, 101
trends, 45, 52, 70, 71, 89, 90, 99, 112, 119
triage, 71, 74
Trojan horses, 61, 103
TruSecure, 162
trust, 26, 85, 106, 136
trusted
contacts, 72
experts, 106
introducers, 26, 135
Trusted Introducer, 26, 39, 40, 120
trustworthiness, 76
tutorials, 49

TWCERT, 29
TW-CIRC, 29
types of incidents, 102
UNAM-CERT, 30, 31
unauthorized access, 11, 61, 103, 109, 118
United Kingdom, 103
United Nations, 169
United Nations Convention Against Transnational Organized Crime, 117
United Nations General Assembly, 117
United States
    Army, 79
    Computer Emergency Response Team, 34
    CSIRTs, 19, 33
    cyber crime laws, 118
    Department of Defense, 80
    Department of Defense Information Technology Security Certification and Accreditation Process, 174
    Department of Energy, 19, 21
    Department of Homeland Security, 34
    Department of Justice, 115
    Department of Justice, Computer Crime and Intellectual Property Section, 118
    Department of National Defence CIRT, 32
    Department of the Army Response Team, 21
    Department of the Navy, 82
    federal laws, 169
    federal requirements, 173
    Secret Service, 84, 92, 115
    state laws, 175
university networks, 52
University of Queensland, The, 27, 63
UNIX, 101
US-CERT, 34
user compromises, 103
van Wyk, K., 92
VBS, 95
Vermont, State of, 82, 85
victims, 105, 130
viruses, 61, 68, 93, 102, 103
Vorfallsbearbeitungssystem, 95
vulnerabilities, 110, 113
vulnerability
    analysts, 73
    assessments, 12, 68
    disclosure, 135
    handlers, 75
    handling, 68, 75
    scanning, 68
walk-in reports, 89
WANK, 20, 21
war stories, 130
web defacement, 60
West-Brown, Moira, xiii
Williams, Pam, xiv
wiretapping, 61
workflows, 134
working groups, 25, 28, 29
workload, 90, 91, 129
worms, 17, 20, 61, 103
xenophobic acts, 116
XML, 25, 122, 123

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY (Leave Blank)	2. REPORT DATE October 2003	3. REPORT TYPE AND DATES COVERED Final
4. TITLE AND SUBTITLE State of the Practice of Computer Security Incident Response Teams (CSIRTs)		5. FUNDING NUMBERS F19628-00-C-0003
6. AUTHOR(S) Georgia Killcrece, Klaus-Peter Kossakowski, Robin Ruefle, Mark Zajicek		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213		8. PERFORMING ORGANIZATION REPORT NUMBER CMU/SEI-2003-TR-001
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) HQ ESC/XPK 5 Eglin Street Hanscom AFB, MA 01731-2116		10. SPONSORING/MONITORING AGENCY REPORT NUMBER ESC-TR-2003-001
11. SUPPLEMENTARY NOTES		
12A DISTRIBUTION/AVAILABILITY STATEMENT Unclassified/Unlimited, DTIC, NTIS		12B DISTRIBUTION CODE

13. ABSTRACT (MAXIMUM 200 WORDS)

Keeping organizational information assets secure in today's interconnected computing environment is a challenge that becomes more difficult with each new "e" product and each new intruder tool. There is no one solution for securing information assets; instead a multi-layered security strategy is required. One of the layers that many organizations are including in their strategy today is a computer security incident response team, or CSIRT. This report provides an objective study of the state of the practice of incident response, based on information about how CSIRTs around the world are operating. It covers CSIRT services, projects, processes, structures, and literature, as well as training, legal, and operational issues. The report can serve as a resource both to new teams that are setting up their operations and to existing CSIRTs that are interested in benchmarking their operations.

14. SUBJECT TERMS CSIRT, computer security incident response team, incident handling, incident response, computer emergency response team, incident management, incident response management, CERT/CC, CERT Coordination Center	15. NUMBER OF PAGES 290
16. PRICE CODE	

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL