



Cybersecurity Fundamentals

STUDY GUIDE

ISACA®

With more than 115,000 constituents in 180 countries, ISACA (www.isaca.org) helps business and IT leaders build trust in, and value from, information and information systems. Established in 1969, ISACA is the trusted source of knowledge, standards, networking, and career development for information systems audit, assurance, security, risk, privacy and governance professionals. ISACA offers the Cybersecurity Nexus™, a comprehensive set of resources for cybersecurity professionals, and COBIT®, a business framework that helps enterprises govern and manage their information and technology. ISACA also advances and validates business-critical skills and knowledge through the globally respected Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) and Certified in Risk and Information Systems Control™ (CRISC™) credentials. The association has more than 200 chapters worldwide.

Disclaimer

ISACA has designed and created *Cybersecurity Fundamentals Study Guide* primarily as an educational resource for cybersecurity professionals. ISACA makes no claim, representation or warranty that use of any of this study guide will assure a successful outcome or result in any certificate or certification. The study guide was produced independently from the Cybersecurity Fundamentals exam. Copies of current or past exams are not released to the public and were not used in the preparation of this publication.

Reservation of Rights

© 2015 ISACA. All rights reserved. No part of this publication may be used, copied, reproduced, modified, distributed, displayed, stored in a retrieval system or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise), without the prior written authorization of ISACA.

ISACA

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
Email: info@isaca.org
Web site: www.isaca.org

Provide Feedback: www.isaca.org/cyber-fundamentals-study-guide
Participate in the ISACA Knowledge Center: www.isaca.org/knowledge-center
Follow ISACA on Twitter: <https://twitter.com/ISACANews>
Join ISACA on LinkedIn: ISACA (Official), <http://linkd.in/ISACAOfficial>
Like ISACA on Facebook: www.facebook.com/ISACAHQ

ACKNOWLEDGMENTS

The *Cybersecurity Fundamentals Study Guide* development is the result of the collective efforts of many volunteers. ISACA members from throughout the world participated, generously offering their talent and expertise.

Expert Reviewers

Orestes Balderas Zamora, CISA, Nielsen, Mexico

Matthiew Morin, Analyst, Stroz Friedberg, United States

Ignacio Paredes, CISA, CISM, CRISC, Industrial Cybersecurity Center, Spain

Jeffrey L. Roth, CISA, CGEIT, Nova Technologies, United States

John Tannahill, CISM, CGEIT, CRISC, J. Tannahill & Associates, Canada

Shay Zandani, CISA, CISM, CRISC, Cytegit, Israel

Page intentionally left blank

CONTENTS

EXECUTIVE SUMMARY.....	1
SECTION 1: CYBERSECURITY INTRODUCTION AND OVERVIEW	3
Topic 1—Introduction to Cybersecurity	5
Topic 2—Difference Between Information Security and Cybersecurity	9
Topic 3—Cybersecurity Objectives	11
Topic 4—Cybersecurity Roles	13
Topic 5—Cybersecurity Domains.....	17
Section 1—Knowledge Check	19
SECTION 2: CYBERSECURITY CONCEPTS.....	21
Topic 1—Risk.....	23
Topic 2—Common Attack Types and Vectors	27
Topic 3—Policies and Procedures.....	33
Topic 4—Cybersecurity Controls	37
Section 2—Knowledge Check	40
SECTION 3: SECURITY ARCHITECTURE PRINCIPLES.....	41
Topic 1—Overview of Security Architecture	43
Topic 2—The OSI Model.....	47
Topic 3—Defense in Depth.....	51
Topic 4—Firewalls	53
Topic 5—Isolation and Segmentation.....	59
Topic 6—Monitoring, Detection and Logging	61
Topic 7A—Encryption Fundamentals	65
Topic 7B—Encryption Techniques	67
Topic 7C—Encryption Applications.....	73
Section 3—Knowledge Check	75
SECTION 4: SECURITY OF NETWORKS, SYSTEMS, APPLICATIONS AND DATA.....	77
Topic 1—Process Controls—Risk Assessments.....	79
Topic 2—Process Controls—Vulnerability Management	83
Topic 3—Process Controls—Penetration Testing.....	85
Topic 4—Network Security.....	87
Topic 5—Operating System Security	95
Topic 6—Application Security	101
Topic 7—Data Security	107
Section 4—Knowledge Check	111
SECTION 5: INCIDENT RESPONSE.....	113
Topic 1—Event vs. Incident.....	115
Topic 2—Security Incident Response.....	117
Topic 3—Investigations, Legal Holds and Preservation.....	121
Topic 4—Forensics.....	123
Topic 5—Disaster Recovery and Business Continuity Plans.....	127
Section 5—Knowledge Check	131

SECTION 6: SECURITY IMPLICATIONS AND ADOPTION OF EVOLVING TECHNOLOGY	133
Topic 1—Current Threat Landscape.....	135
Topic 2—Advanced Persistent Threats	137
Topic 3—Mobile Technology—Vulnerabilities, Threats and Risk	141
Topic 4—Consumerization of IT and Mobile Devices	147
Topic 5—Cloud and Digital Collaboration.....	149
Section 6—Knowledge Check	153
APPENDICES	155
Appendix A—Knowledge Statements	157
Appendix B—Glossary	159
Appendix C—Knowledge Check Answers.....	183
Appendix D—Additional Resources	189

EXECUTIVE SUMMARY

CYBERSECURITY FUNDAMENTALS STUDY GUIDE

Why become a cybersecurity professional? The protection of information is a critical function for all enterprises. Cybersecurity is a growing and rapidly changing field, and it is crucial that the central concepts that frame and define this increasingly pervasive field are understood by professionals who are involved and concerned with the security implications of information technology (IT). The Cybersecurity Fundamentals Study Guide is designed for this purpose, as well as to provide insight into the importance of cybersecurity, and the integral role of cybersecurity professionals. This guide will also cover five key areas of cybersecurity: 1) cybersecurity concepts, 2) security architecture principles, 3) security of networks, systems, applications and data, 4) incident response and 5) the security implications of the adoption of emerging technologies.

This guide covers the following learning objectives:

- Understand basic cybersecurity concepts and definitions
- Understand basic risk management and risk assessment principles relating to cybersecurity threats
- Apply security architecture principles
- Identify components of a security architecture
- Define network security architecture concepts
- Understand malware analysis concepts and methodology
- Recognize the methodologies and techniques for detecting host- and network-based intrusions via intrusion detection technologies
- Identify vulnerability assessment tools, including open source tools and their capabilities
- Understand system hardening
- Understand penetration testing principles, tools and techniques
- Define network systems management principles, models, methods and tools
- Understand remote access technology and systems administration concepts
- Distinguish system and application security threats and vulnerabilities
- Recognize system life cycle management principles, including software security and usability
- Define types of incidents (categories, responses and time lines for responses)
- Outline disaster recovery and business continuity planning
- Understand incident response and handling methodologies
- Understand security event correlation tools, and how different file types can be used for atypical behavior
- Recognize investigative implications of hardware, operating systems and network technologies
- Be aware of the basic concepts, practices, tools, tactics, techniques and procedures for processing digital forensic data
- Identify network traffic analysis methods
- Recognize new and emerging information technology and information

Page intentionally left blank



Section 1:

Cybersecurity Introduction and Overview

Topics covered in this section include:

1. Cybersecurity definition
2. Objectives of cybersecurity
3. Key business and technology factors
4. Cybersecurity roles and governance
5. Domains of cybersecurity

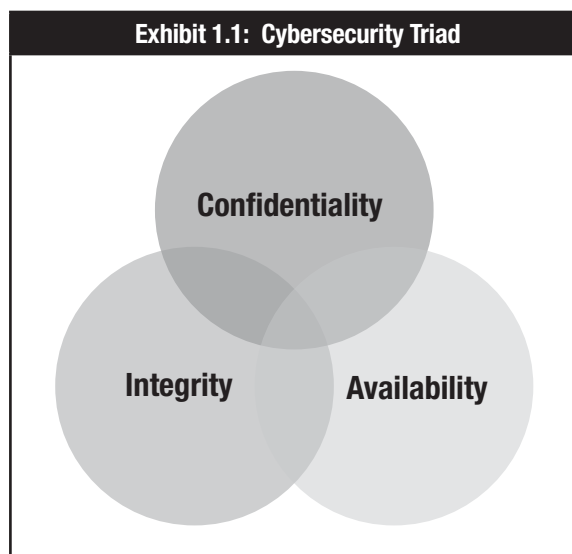
Page intentionally left blank

TOPIC 1—INTRODUCTION TO CYBERSECURITY

THE EVOLUTION OF CYBERSECURITY

Computer security. Network security. Information security. Cybersecurity. All of these terms are used to describe the protection of information assets. Why have there been so many changes in the way we refer to security?

Safeguarding information has been a priority for as long as people have needed to keep information secure and private. Even simple encryption techniques such as Caesar ciphers were created to ensure confidentiality. But as time and technology move forward, so do the demands of security. Today, the objective of information security is threefold, involving the critical components of confidentiality, integrity and availability (see **exhibit 1.1**). All three components are concerned with the protection of information. **Confidentiality** means protection from unauthorized access, while **integrity** means protection from unauthorized modification, and **availability** means protection from disruptions in access.



In current discussions of security, there are references to both “cybersecurity” and “information security.” The terms are often used interchangeably, but in reality cybersecurity is a part of information security. Marketing, vendors and analysts often use the term “cyber” too broadly, due to the increasingly complex nature of information in the digital age. Additionally, the interconnected nature of critical infrastructure systems has introduced a host of new vulnerabilities with far-reaching implications. All of these factors have influenced the shift from information security to cybersecurity. Generally, cybersecurity refers to anything intended to protect enterprises and individuals from intentional attacks, breaches, incidents and consequences. More specifically, **cybersecurity** can be defined as “the protection of information assets by addressing threats to information processed, stored and transported by internetworked information systems.”

CYBERSECURITY AND SITUATIONAL AWARENESS

Cybersecurity plays a significant role in today’s ever-evolving cyberlandscape. New trends in mobility and connectivity present a broader range of challenges than ever before as new attacks continue to develop along with emerging technologies. Cybersecurity professionals must be informed and flexible to identify and manage potential new threats, such as advanced persistent threats (APTs), effectively. APTs are attacks by an adversary who possesses sophisticated levels of expertise and significant resources, which allow the attacker to create opportunities to achieve its objectives using multiple attack vectors.

In order to successfully protect their systems and information, cybersecurity professionals must demonstrate a high degree of situational awareness. This type of awareness takes time to cultivate, because it usually develops through experience within a specific organization. Each organization has its own distinct culture, which means that conditions vary widely from one organization to another. Therefore, it is critical for cybersecurity professionals to have an awareness of the environment in which they operate.

Central to this awareness is an understanding of key business and technology factors that affect information security. Numerous factors, both internal and external, can directly impact an organization and its security needs, including:

- Business plans and business environment
- Available information technology, security process or systems in particular

Both of these factors tend to be situational in nature, as every organization faces its own unique challenges and risk based on the nature of its business. Business environment in particular tends to drive risk decisions. For example, a small start-up company may be much more tolerant of risk than a large, well-established corporation. Therefore, it can be helpful to reference these broad criteria when evaluating the drivers affecting the security of a specific organization.

With respect to technology, there are many factors that can impact security, such as:

- Platforms and tools used
- Network connectivity (internal, third-party, public)
- Level of IT complexity
- Operational support for security
- User community and capabilities
- New or emerging security tools

When evaluating business plans and the general business environment, consider drivers, such as:

- Nature of business
- Risk tolerance
- Security profile
- Industry trends for security
- Mergers, acquisitions and partnerships
 - Consider type, frequency and resulting level of integration
- Outsourcing services or providers

Although business and technology drivers cannot all be predicted with certainty, they should be anticipated reasonably and handled as efficiently as possible. Failure to anticipate key security drivers reflects an inability to effectively react to changing business circumstances, which in turn results in diminished security and missed opportunities for improvement.

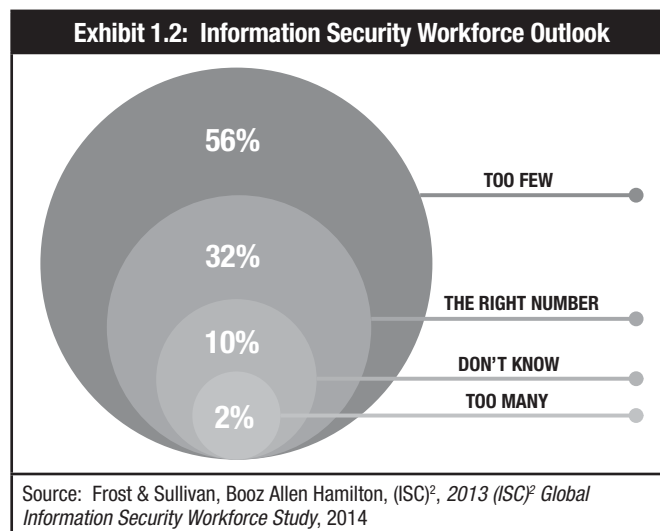
THE CYBERSECURITY SKILLS GAP

Cybersecurity is a field that demands skilled professionals who possess the foundational knowledge, education and thought leadership necessary to confront the difficulties that accompany constant technological change. Advanced threat vectors, emerging technologies and myriad regulations require cybersecurity professionals to be skilled in technology as well as business and communications.

Cybersecurity addresses both internal and external threats to an organization's digital information assets by focusing on critical electronic data processes, signal processing, risk analytics and information system security engineering.

There are an estimated 410,000 to 510,000 information security professionals worldwide, and jobs are expected to increase 53 percent by 2018 with over 4.2 million jobs available. However, recent studies and reports suggest that there are simply not enough skilled professionals to fill them.

While the cybersecurity landscape has evolved, the skill set among existing and potential cybersecurity professionals has not kept pace. The 2013 (ISC)² *Global Information Security Workforce Study* sponsored by Frost & Sullivan, Booz Allen Hamilton and (ISC)² concludes that there is a dangerous shortage of skilled professionals in the cybersecurity profession.¹ The study indicates that the shortage negatively impacts organizations and their customers, leading to more frequent and costly data breaches. The United Kingdom's National Audit Office states that there are not enough existing or upcoming professionals with appropriate skills, as shown in **exhibit 1.2**. Likewise, the EU's digital agenda commissioner believes that the growing cybersecurity skills gap is threatening the EU's competitiveness. Skills gaps are seen in both technical and business aspects of security. This guide provides an overview of these business and technical practices, along with various other methodologies and procedures related to cybersecurity.



¹ Frost & Sullivan, Booz Allen Hamilton, (ISC)², 2013 (ISC)² *Global Information Security Workforce Study*, 2014, www.isc2cares.org/Workforcestudy

Page intentionally left blank

TOPIC 2—DIFFERENCE BETWEEN INFORMATION SECURITY AND CYBERSECURITY

The terms “cybersecurity” and “information security” are often used interchangeably. Some use the term cybersecurity as a synonym for information security, IT security and information risk management. Others, particularly in government circles, have adopted more technical definitions related to national defense, including cyber warfare and protection of critical infrastructure. Although different groups tend to adapt terminology for their own purposes, there are some important distinctions between cybersecurity and information security.

Information security deals with information, regardless of its format—it encompasses paper documents, digital and intellectual property in people’s minds, and verbal or visual communications. **Cybersecurity**, on the other hand, is concerned with protecting digital assets—everything from networks to hardware and information that is processed, stored or transported by internetworked information systems. Additionally, concepts such as nation-state-sponsored attacks and advanced persistent threats (APTs) belong almost exclusively to cybersecurity. It is helpful to think of cybersecurity as a component of information security.

Therefore, to eliminate confusion, the term cybersecurity will be defined in this guide as protecting information assets by addressing threats to information processed, stored and transported by internetworked information systems.

PROTECTING DIGITAL ASSETS

In their cybersecurity frameworks, both the National Institute of Standards and Technology (NIST) and the European Union Agency for Network and Information Security (ENISA) have identified five key functions necessary for the protection of digital assets. These functions coincide with incident management methodologies and include the following activities:

- **Identify:** Use organizational understanding to minimize risk to systems, assets, data and capabilities.
- **Protect:** Design safeguards to limit the impact of potential events on critical services and infrastructure.
- **Detect:** Implement activities to identify the occurrence of a cybersecurity event.
- **Respond:** Take appropriate action after learning of a security event.
- **Recover:** Plan for resilience and the timely repair of compromised capabilities and services.

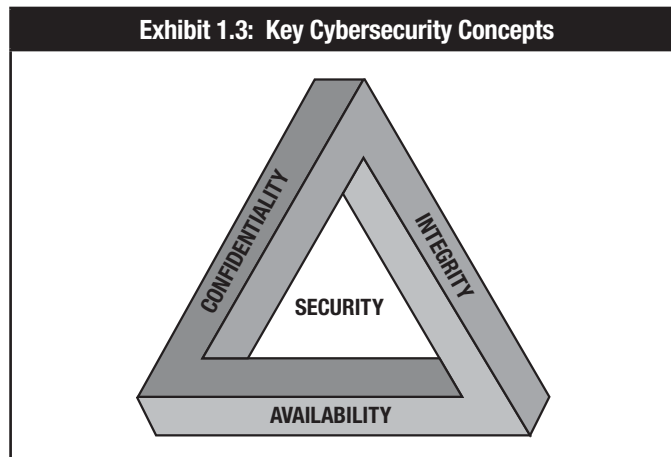
Page intentionally left blank

TOPIC 3—CYBERSECURITY OBJECTIVES

CONFIDENTIALITY, INTEGRITY AND AVAILABILITY

To better understand cybersecurity and the protection of cyberassets, it is helpful to consider three key concepts that are used to guide security policies, as shown in **exhibit 1.3**. The concepts are:

- Confidentiality
- Integrity
- Availability



Confidentiality is the protection of information from unauthorized access or disclosure. Different types of information require different levels of confidentiality, and the need for confidentiality can change over time. Personal, financial and medical information require a higher degree of confidentiality than the minutes of a staff meeting, for example. Similarly, some companies need to protect information on competitive future products before their release but may need to make the same information public afterwards.

Data must be protected from improper disclosure according to its sensitivity and applicable legal requirements. The confidentiality of digital information can be maintained using several different means, including access controls, file permissions and encryption.

Integrity is the protection of information from unauthorized modification. For example, if a bank transfers US \$10,000 to another financial institution, it is important that the amount does not change to US \$100,000 during the exchange. The concept of integrity also applies to software and configurations.

Any violation of integrity is significant because it may be the first step in a successful attack against system availability or confidentiality. Contaminated systems and corrupted data must be dealt with immediately to assess the potential for further violation or damage. The integrity of digital assets can be controlled by logging, digital signatures, hashes, encryption and access controls.

Availability ensures the timely and reliable access to and use of information and systems. This would include safeguards to make sure data are not accidentally or maliciously deleted. This is particularly important with a mission-critical system, because any interruptions in its availability can result in a loss of productivity and revenue. Similarly, the loss of data can impact management's ability to make effective decisions and responses. Availability can be protected by the use of redundancy, backups and access control.

The impacts, potential consequences and methods of control of confidentiality, integrity and availability are shown in exhibit 1.4.

Exhibit 1.4: Confidentiality, Integrity and Availability Model and Related Impacts		
Requirement	Impact and Potential Consequences	Methods of Control
Confidentiality: the protection of information from unauthorized disclosure	Loss of confidentiality can result in the following consequences: <ul style="list-style-type: none"> • Disclosure of information protected by privacy laws • Loss of public confidence • Loss of competitive advantage • Legal action against the enterprise • Interference with national security 	Confidentiality can be preserved using the following methods: <ul style="list-style-type: none"> • Access Controls • File Permissions • Encryption
Integrity: the accuracy and completeness of information in accordance with business values and expectations	Loss of integrity can result in the following consequences: <ul style="list-style-type: none"> • Inaccuracy • Erroneous decisions • Fraud 	Integrity can be preserved using the following methods: <ul style="list-style-type: none"> • Access controls • Logging • Digital Signatures • Hashes • Encryptions
Availability: the ability to access information and resources required by the business process following consequences:	Loss of availability can result in the following consequences: <ul style="list-style-type: none"> • Loss of functionality and operational effectiveness • Loss of productive time • Interference with enterprise's Objectives 	Availability can be preserved using the following methods: <ul style="list-style-type: none"> • Redundancy • Backups • Access Controls

NONREPUDIATION

Confidentiality, integrity and availability are equally important factors in the process of ensuring nonrepudiation. In a digital context, nonrepudiation refers to the concept that a message or other piece of information is genuine. It assures that the data's integrity has been protected and that the party sending or receiving it cannot deny or repudiate that they sent or received it. Nonrepudiation is important in transactions that require trust, such as financial transactions and legal matters. Nonrepudiation is implemented through transactional logs and digital signatures.

TOPIC 4—CYBERSECURITY ROLES

GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE

The structure and governance of every organization is different and varies based on the type of organization. Each organization has its own mission (business), size, industry, culture and legal regulations. However, all organizations have a responsibility and duty to protect their assets and operations, including their IT infrastructure and information. At the highest level, this is generally referred to as governance, risk management and compliance (GRC). Some entities implement these three areas in an integrated manner, while others may have less comprehensive approaches. Regardless of the actual implementation, every organization needs a plan to manage these three elements.

Governance is the responsibility of the board of directors and senior management of the organization. A governance program has several goals:

- Provide strategic direction
- Ensure that objectives are achieved
- Ascertain whether risk is being managed appropriately
- Verify that the organization's resources are being used responsibly

Risk management is the process by which an organization manages risk to acceptable levels. Risk management requires the development and implementation of internal controls to manage and mitigate risk throughout the organization, including financial and investment risk, physical risk and cyberrisk.²

Compliance is the act of adhering to, and the ability to demonstrate adherence to, mandated requirements defined by laws and regulations. It also includes voluntary requirements resulting from contractual obligations and internal policies.

Cybersecurity is the responsibility of the entire organization at every level. The next section outlines some of the specific roles in managing cyberrisk within most organizations.

WHAT DOES A CYBERSECURITY PROFESSIONAL DO?

The cybersecurity professional's duties include analysis of policy, trends and intelligence. Using problem-solving and detection skills, they strive to better understand how an adversary may think or behave. The inherent complexity of their work requires the cybersecurity workforce to possess not only a wide array of technical IT skills, but also advanced analytical capabilities. A cybersecurity professional may be a practitioner or part of senior management.

INFORMATION SECURITY ROLES

Because cybersecurity is part of information security, there is occasional overlap between the terms and how they are applied to management structures and titles. For the purposes of this discussion, assume that the term information security encompasses cybersecurity roles and functions.

BOARD OF DIRECTORS

Cybersecurity governance requires strategic direction and impetus. It depends on commitment, resources and responsibility for cybersecurity management and it requires a means for the board to determine whether its intent has been met. Effective governance can be accomplished only by senior management involvement in approving policy and by appropriate monitoring and metrics coupled with reporting and trend analysis.

Members of the board need to be aware of the organization's information assets and their criticality to ongoing business operations. The board should periodically be provided with the high-level results of comprehensive risk assessments and business impact analyses (BIAs), which identify how quickly essential business unit and processes have to return to full operation following a disaster event. A result of these activities should include board members identifying the key assets they want protected and verifying that protection levels and priorities are appropriate to a standard of due care.

² ISACA, *CISM Review Manual 2014*, USA

The tone at the top must be conducive to effective security governance. It is up to senior management to set a positive example in this regard, as lower-level personnel are much more likely to abide by security measures when they see their superiors respecting the same measures as well. Executive management's endorsement of security requirements ensures that security expectations are met at all levels of the enterprise. Penalties for noncompliance must be defined, communicated and enforced from the board level down.

Beyond these requirements, the board has an ongoing obligation to provide oversight for activities related to cybersecurity. Senior management has the legal and ethical responsibility of exercising due care in protecting the organization's key assets, including its confidential and critical information. Therefore, their involvement and oversight is required.

EXECUTIVE MANAGEMENT

An organization's executive management team is responsible for ensuring that needed organizational functions, resources, and supporting infrastructure are available and properly utilized to fulfill the directives of the board, regulatory compliance and other demands.

Generally, executive management looks to the chief information security officer (CISO) or other senior cybersecurity manager to define the information security program and its subsequent management. Often, the cybersecurity manager is also expected to provide education and guidance to the executive management team. As opposed to being the decision maker, the manager's role in this situation is often constrained to presentation of options and key decision support information. In other words, the cybersecurity manager acts as an advisor.

Executive management sets the tone for cybersecurity management within the organization. The level of visible involvement and the inclusion of information risk management in key business activities and decisions indicate to other managers the level of importance that they are also expected to apply to risk management for activities within their organizations.

SENIOR INFORMATION SECURITY MANAGEMENT

The exact title for the individual who oversees information security and cybersecurity varies from organization to organization. One of the most common titles is chief information security officer (CISO), but some organizations prefer the term chief security officer (CSO) to denote responsibility for all security matters, both physical and digital. Likewise, the responsibilities and authority of information security managers vary dramatically between organizations.

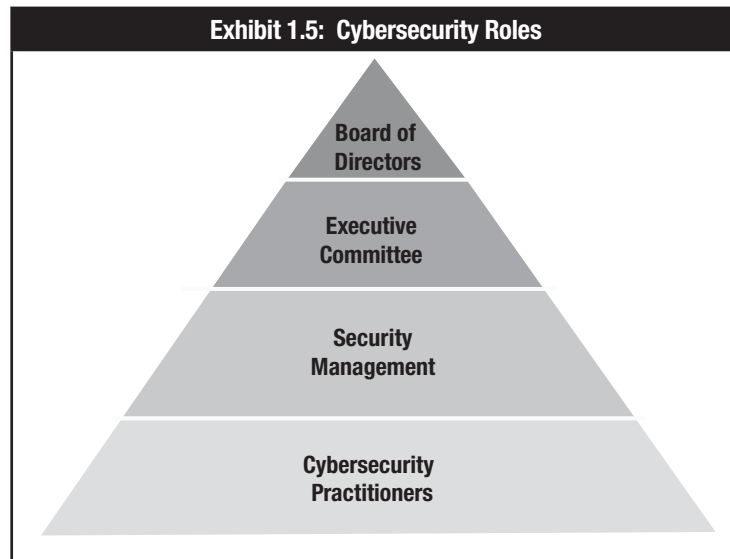
Generally, the cybersecurity manager will be responsible for:

- Developing the security strategy
- Overseeing the security program and initiatives
- Coordinating with business process owners for ongoing alignment
- Ensuring that risk and business impact assessments are conducted
- Developing risk mitigation strategies
- Enforcing policy and regulatory compliance
- Monitoring the utilization and effectiveness of security resources
- Developing and implementing monitoring and metrics
- Directing and monitoring security activities
- Managing cybersecurity incidents and their remediation, as well as incorporating lessons learned

CYBERSECURITY PRACTITIONERS

In most organizations, cybersecurity is managed by a team of subject matter experts and cybersecurity practitioners, including security architects, administrators, digital forensics and network security specialists. Together they design, implement and manage processes and technical controls and respond to events and incidents.

These practitioners work within the direction, policies, guidelines, mandates and regulations set by the board of directors, executives and cybersecurity management. Cybersecurity roles are shown in **exhibit 1.5**.



Page intentionally left blank

TOPIC 5—CYBERSECURITY DOMAINS

The cybersecurity domains covered in this guide are as follows:

- Cybersecurity Concepts
- Security Architecture Principles
- Security of Networks, Systems, Applications and Data
- Incident Response
- Security Implications and Adoption of Evolving Technology

CYBERSECURITY CONCEPTS

This domain provides discussion of critical concepts such as:

- Basic risk management
- Common attack vectors and threat agents
- Patterns and types of attacks
- Types of security policies and procedures
- Cybersecurity control processes

All of these concepts are addressed in light of how they influence security policies and procedures relating to cybersecurity threats. Each topic considers various approaches with a focus on security best practices.

SECURITY ARCHITECTURE PRINCIPLES

This domain provides information that helps security professionals identify and apply the principles of security architecture. It discusses a variety of topics, including:

- Common security architectures and frameworks
- System topology and perimeter concepts
- Firewalls and encryption
- Isolation and segmentation
- Methods for monitoring, detection and logging

These topics are presented with a focus on best security practice. Various types of security architectures are discussed to illustrate the importance of layering controls to achieve defense in depth.

SECURITY OF NETWORKS, SYSTEMS, APPLICATIONS AND DATA

This domain addresses basic system hardening techniques and security measures, including:

- Process controls
 - Risk assessments
 - Vulnerability management
 - Penetration testing
- Best practices for securing networks, systems, applications and data
 - System and application security threats and vulnerabilities
 - Effective controls for managing vulnerabilities

These discussions aim to help cybersecurity professionals assess their risk tolerance and respond appropriately to vulnerabilities.

INCIDENT RESPONSE

This domain articulates the critical distinction between an event and an incident. More importantly, it outlines the steps necessary when responding to a cybersecurity incident. In doing so, it covers the following topics:

- Incident categories
- Disaster recovery and business continuity plans
- Steps of incident response
- Forensics and preservation of evidence

These discussions aim to provide entry-level professionals with the level of knowledge necessary to respond to cybersecurity incidents competently.

SECURITY IMPLICATIONS AND ADOPTION OF EVOLVING TECHNOLOGY

This domain outlines the current threat landscape, including a discussion of vulnerabilities associated with the following emerging technologies:

- Mobile devices
- Cloud computing and storage
- Digital collaboration

Although the current threat landscape continues to evolve, this section highlights the recent developments most likely to impact cybersecurity professionals. For example, it discusses the implications of bring your own device (BYOD) environments and addresses the risk introduced by mobile and web applications. There is also an extended discussion of APTs and their most frequent targets.

SECTION 1—KNOWLEDGE CHECK

1. Three common controls used to protect the availability of information are:
 - a. Redundancy, backups and access controls.
 - b. Encryption, file permissions and access controls.
 - c. Access controls, logging and digital signatures.
 - d. Hashes, logging and backups.
2. Select all that apply. Governance has several goals, including:
 - a. Providing strategic direction.
 - b. Ensuring that objectives are achieved.
 - c. Verifying that organizational resources are being used appropriately.
 - d. Directing and monitoring security activities.
 - e. Ascertaining whether risk is being managed properly.
3. Choose three. According to the NIST framework, which of the following are considered key functions necessary for the protection of digital assets?
 - a. Encrypt
 - b. Protect
 - c. Investigate
 - d. Recover
 - e. Identify
4. Which of the following is the best definition for cybersecurity?
 - a. The process by which an organization manages cybersecurity risk to an acceptable level
 - b. The protection of information from unauthorized access or disclosure
 - c. The protection of paper documents, digital and intellectual property, and verbal or visual communications
 - d. Protecting information assets by addressing threats to information that is processed, stored or transported by interworked information systems
5. Which of the following cybersecurity roles is charged with the duty of managing incidents and remediation?
 - a. Board of directors
 - b. Executive committee
 - c. Security management
 - d. Cybersecurity practitioners

Page intentionally left blank



CYBERSECURITY NEXUS

Section 2:

Cybersecurity Concepts

Topics covered in this section include:

1. Risk management terms, concepts and frameworks
2. Common attack types and vectors
3. General process and attributes of cyberattacks
4. Malware
5. Policies and procedures framework and guidelines
6. Cybersecurity control processes

Page intentionally left blank

TOPIC 1—RISK

The core duty of cybersecurity is to identify, mitigate and manage cyberrisk to an organization's digital assets. While most people have an inherent understanding of risk in their day-to-day lives, it is important to understand risk in the context of cybersecurity, which means knowing how to determine, measure and reduce risk effectively.

Assessing risk is one of the most critical functions of a cybersecurity organization. Effective policies, security implementations, resource allocation and incident response preparedness are all dependent on understanding the risk and threats an organization faces. Using a risk-based approach to cybersecurity allows more informed decision-making to protect the organization and to apply limited budgets and resources effectively. If controls are not implemented based on awareness of actual risk, then valuable organizational assets will not be adequately protected while other assets will be wastefully overprotected.³

Yet, too often, cybersecurity controls are implemented with little or no assessment of risk. ISACA's recent worldwide survey of IT management, auditors and security managers consistently shows that over 80 percent of companies believe "information security risks are either not known or are only partially assessed" and that "IT risk illiteracy and lack of awareness" are major challenges in managing risk.⁴ Therefore, understanding risk and risk assessments are critical requirements for any security practitioner.

APPROACHES TO CYBERSECURITY

Generally, there are three different approaches to implementing cybersecurity. Each approach is described briefly below.

- **Compliance-based**—Also known as standards-based security, this approach relies on regulations or standards to determine security implementations. Controls are implemented regardless of their applicability or necessity, which often leads to a "checklist" attitude toward security.
- **Risk-based**—Risk-based security relies on identifying the unique risk a particular organization faces and designing and implementing security controls to address that risk above and beyond the entity's risk tolerance and business needs.
- **Ad hoc**—An *ad hoc* approach simply implements security with no particular rationale or criteria. Ad hoc implementations may be driven by vendor marketing, or they may reflect insufficient subject matter expertise, knowledge or training when designing and implementing safeguards.

In reality, most organizations with mature security programs use a combination of risk-based and compliance-based approaches. In fact, most standards or regulations such as the Payment Card Industry Data Security Standard (PCIDSS) or the US Health Insurance Portability and Accountability Act (HIPAA) require risk assessments to drive the particular implementation of the required controls.

KEY TERMS AND DEFINITIONS

There are many potential definitions of risk—some general and others more technical. Additionally, it is important to distinguish between a risk and a threat. Although many people use the words threat and risk synonymously, they have two very different meanings. As with any key concept, there is some variation in definition from one organization to another. For the purposes of this guide, we will define terms as follows:

Risk—The combination of the probability of an event and its consequence (International Organization for Standardization/International Electrotechnical Commission [ISO/IEC] 73). Risk is mitigated through the use of controls or safeguards.

³ Anderson, Kent, "A Business Model for Information Security," ISACA® *Journal*, Vol. 3, 2008

⁴ ISACA, "Top Business/Security Issues Survey Results," USA, 2011

Threat—Anything (e.g., object, substance, human) that is capable of acting against an asset in a manner that can result in harm. ISO/IEC 13335 defines a threat broadly as a potential cause of an unwanted incident. Some organizations make a further distinction between a threat source and a threat event, classifying a threat source as the actual process or agent attempting to cause harm, and a threat event as the result or outcome of a threat agent's malicious activity.

Asset—Something of either tangible or intangible value that is worth protecting, including people, information, infrastructure, finances and reputation

Vulnerability—A weakness in the design, implementation, operation or internal control of a process that could expose the system to adverse threats from threat events

Although much of cybersecurity is focused on the design, implementation and management of controls to mitigate risk, it is critical for security practitioners to understand that risk can never be completely eliminated. Beyond the general definition of risk provided above, there are other, more specific types of risk that apply to cybersecurity.

Residual risk—Even after safeguards are in place, there will always be residual risk, defined as the remaining risk after management has implemented a risk response.

Inherent risk—The risk level or exposure without taking into account the actions that management has taken or might take (e.g., implementing controls)

LIKELIHOOD AND IMPACT

When assessing a threat, cybersecurity professionals often analyze the threat's likelihood and impact in order to rank and prioritize it among other existing threats.

In some cases where clear, statistically sound data are available, likelihood can be a matter of mathematical probability. This is true with situations such as weather events or natural disasters. However, sometimes accurate data are simply not available, as is often the case when analyzing human threat agents in cybersecurity environments. There will also be factors that create situations where the likelihood of certain threats is more or less prevalent for a given organization. For example, a connection to the Internet will predispose a system to port scanning. Typically, qualitative rankings such as "High, Medium, Low" or "Certain, Very Likely, Unlikely, Impossible" can be used to rank and prioritize threats stemming from human activity. When using qualitative rankings, however, the most important step is to rigorously define the meaning of each category and use definitions consistently throughout the assessment process.

For each identified threat, the impact or magnitude of harm expected to result should also be determined. The impact of a threat can take many forms, but it often has an operational consequence of some sort, whether financial, reputational or legal. Impacts can be described either qualitatively or quantitatively, but as with likelihoods, qualitative rankings are most often used in cybersecurity risk assessment. Likewise, each ranking should be well-defined and consistently used. In cybersecurity, impacts are also evaluated in terms of confidentiality, integrity and availability.

APPROACHES TO RISK

There are a number of methodologies available to measure risk. Different industries and professions have adopted various tactics based upon the following criteria:

- Risk tolerance
- Size and scope of the environment in question
- Amount of data available

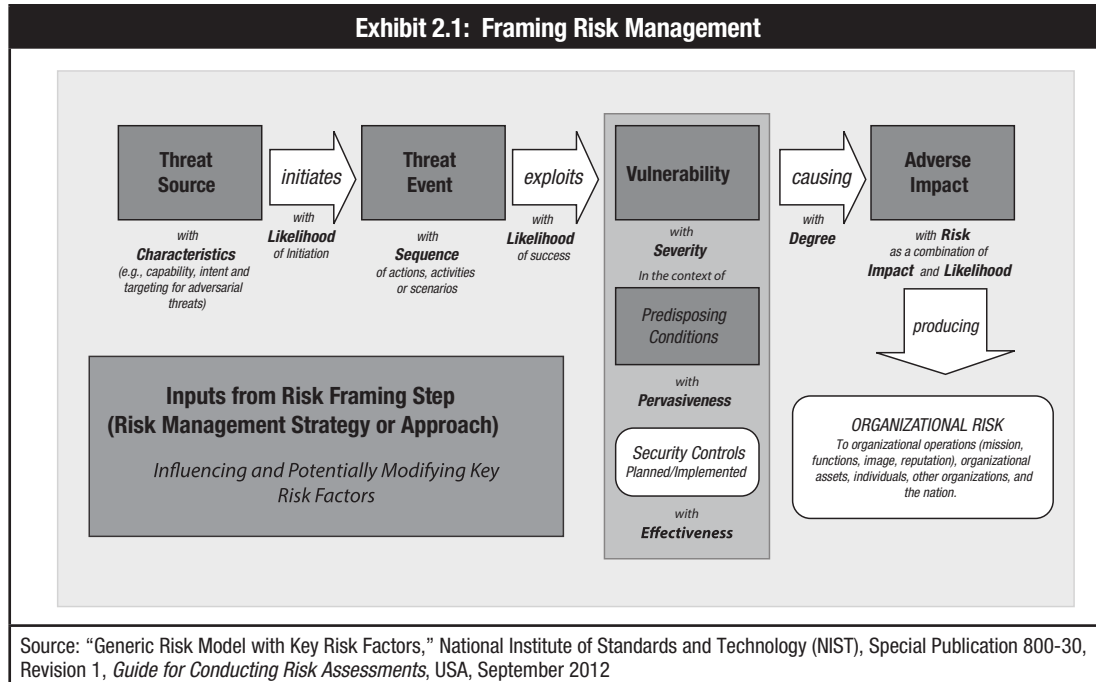
It is particularly important to understand an organization's risk tolerance when considering how to measure risk. For example, a general approach to measuring risk is typically sufficient for risk-tolerant organizations such as academic institutions or small businesses. However, more rigorous and in-depth risk assessment is required for entities with a low tolerance for risk. This is especially relevant for any heavily regulated entity, like a financial institution or an airline reservation system, where any down time would have a significant operational impact.

THIRD-PARTY RISK

Cybersecurity can be more difficult to control when third parties are involved, especially when different entities have different security cultures and risk tolerances. No organization exists in a vacuum, and information must be shared with other individuals or organizations, often referred to as third parties. It is important to understand third-party risk, such as information sharing and network access, as it relates to cybersecurity.

RISK MANAGEMENT

Exhibit 2.1 illustrates how many of these key terms come into play when framing an approach to risk management.



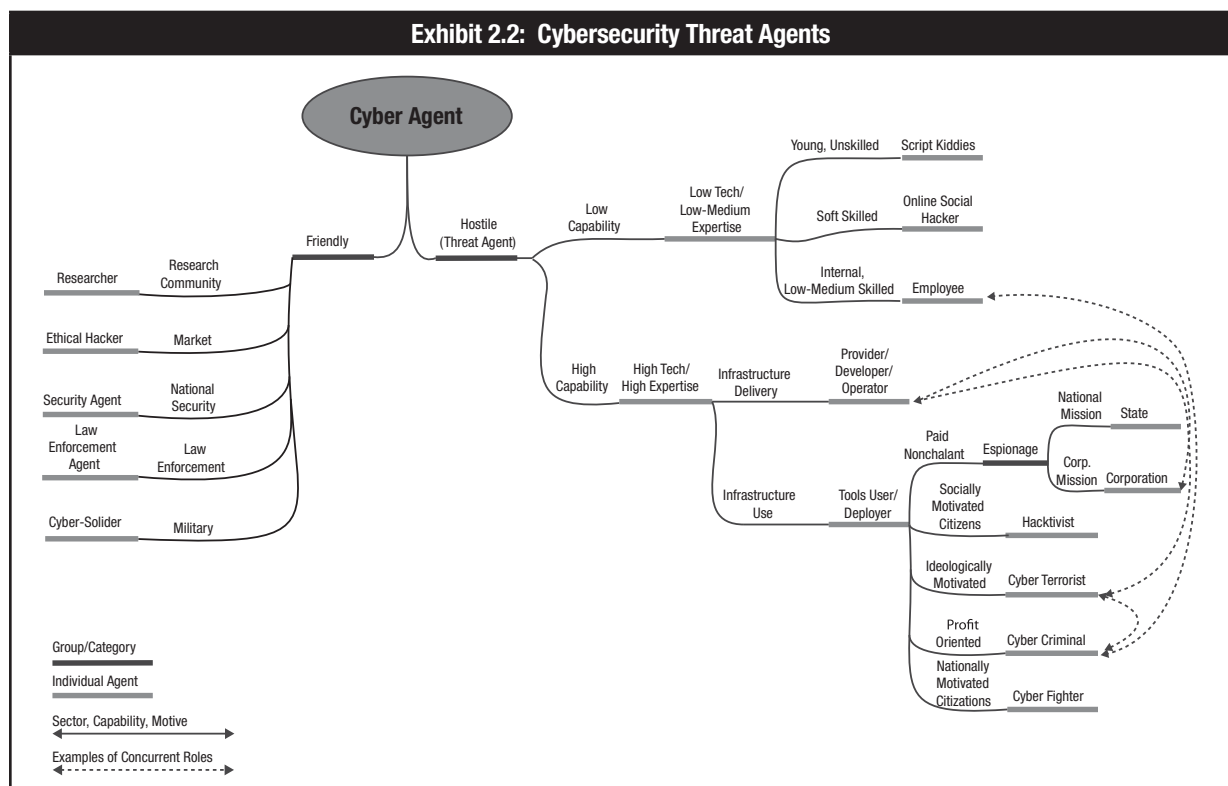
Page intentionally left blank

TOPIC 2—COMMON ATTACK TYPES AND VECTORS

As attack vectors and methodologies continue to evolve, they represent a significant threat on the client side. Although some attacks are made at random with no particular target in mind, there are also targeted attacks against recipients who have been researched and identified as useful by attackers. Phishing attacks are often directed toward recipients who have access to data or systems to which the attacker wishes to gain access. In other cases, malware is deployed in widespread attacks with the hope that it will hit as many vulnerable systems as possible, though these situations are not likened to “cyberattacks.” Rather, a cyberattack is a well-defined, advanced, targeted attack that is stealthy and has a mission that it will not stop attempting to achieve until it is identified and mitigated or succeeds. In today’s threat landscape, a number of distinct threat agents and attack patterns have emerged. It is essential for cybersecurity professionals to be able to identify these threats in order to manage them appropriately.

THREAT AGENTS

Not surprisingly, there are many types of attackers in today’s threat landscape. ENISA has identified threat agents, shown in **exhibit 2.2**.



Corporations—Corporations have been known to breach security boundaries and perform malicious acts to gain a competitive advantage.

Nation States—Nation states often target government and private entities with a high level of sophistication to obtain intelligence or carry out other destructive activities.

Hacktivists—Although they often act independently, politically motivated hackers may target specific individuals or organizations to achieve various ideological ends.

Cyberterrorists—Characterized by their willingness to use violence to achieve their goals, cyberterrorists frequently target critical infrastructures and government groups.

Cybercriminals—Motivated by the desire for profit, these individuals are involved in fraudulent financial transactions.

Cyberwarriors—Often likened to hacktivists, cyberwarriors, also referred to as cyberfighters, are nationally motivated citizens who may act on behalf of a political party or against another political party that threatens them.

Script Kiddies—Script kiddies are young individuals who are learning to hack; they may work alone or with others and are primarily involved in code injections and distributed denial-of-service (DDoS) attacks.

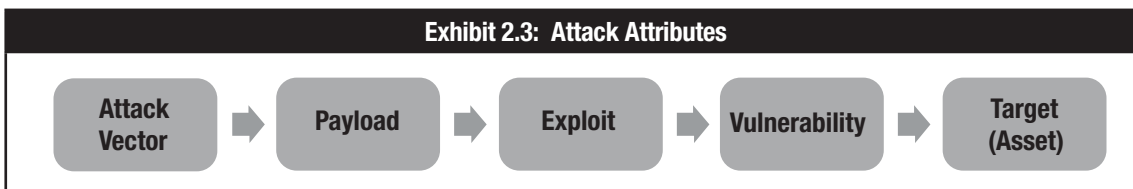
Online Social Hackers—Skilled in social engineering, these attackers are frequently involved in cyberbullying, identity theft and collection of other confidential information or credentials.

Employees—Although they typically have fairly low-tech methods and tools, dissatisfied current or former employees represent a clear cybersecurity risk. All of these attacks are adversarial, but some are not related to APT cyberattacks.

ATTACK ATTRIBUTES

While risk is measured by potential activity, an **attack** is the actual occurrence of a threat. More specifically, an attack is an activity by a threat agent (or adversary) against an asset. From an attacker's point of view, the asset is a **target**, and the path or route used to gain access to the target (asset) is known as an **attack vector**. There are two types of attack vectors: ingress and egress (also known as data exfiltration). While most attack analysis concentrates on ingress, or intrusion, into systems, some attacks are designed to remove data from systems and networks. Therefore, it is important to consider both types of attack vectors.

The attacker must defeat any controls in place and/or use an **exploit** to take advantage of a vulnerability. Another attribute of an attack is the **attack mechanism**, or the method used to deliver the exploit. Unless the attacker is personally performing the attack, the attack mechanism may involve a **payload**, or container, that delivers the exploit to the target. The attributes of an attack are shown in **exhibit 2.3**.



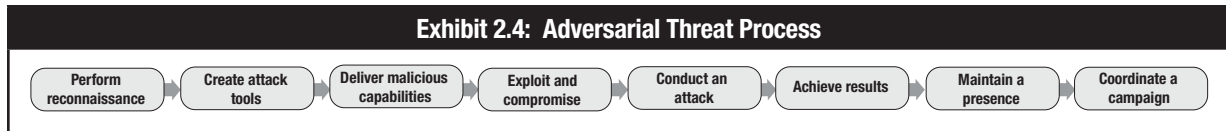
Detailed analysis of cyberattacks requires significant technical and subject matter expertise and is an important part of cybersecurity. Each of the attack attributes (attack vector, payload, exploit, vulnerability, target and, if applicable, egress) provides unique points where controls to prevent or detect the attack can be placed. It is also essential to understand each of these attributes when analyzing and investigating an actual attack. For example, the payload used to deliver the exploit often leaves artifacts or evidence that can be used by technical analysts and investigators to understand the attack and potentially identify the perpetrators. Analysis of the data exfiltration path may identify additional opportunities to prevent or detect the removal of data or obtain evidence, even if the attack was able to gain access to the target.

Attacks can be analyzed and categorized based on their type and patterns of use. From these characteristics, it is possible to make generalizations that facilitate better design and controls. There are two broad categories for threat events: adversarial and nonadversarial. An **adversarial threat event** is made by a human threat agent (or adversary), while a **nonadversarial threat event** is usually the result of an error, malfunction or mishap of some sort.⁵

⁵ MITRE, *Common Attack Pattern Enumeration and Classification (CAPEC)*, February 2014, <http://capec.mitre.org/>

GENERALIZED ATTACK PROCESS

While each attack is different, most adversarial threat events follow a common process, as shown in **exhibit 2.4** and described below.



1. Perform reconnaissance: The adversary gathers information using a variety of techniques, which may include:

- Sniffing or scanning the network perimeter
- Using open source discovery of organizational information
- Running malware to identify potential targets

2. Create attack tools: The adversary crafts the tools needed to carry out a future attack, which may include:

- Phishing or spear phishing attacks
- Crafting counterfeit web sites or certificates
- Creating and operating false front organizations to inject malicious components into the supply chain

3. Deliver malicious capabilities: The adversary inserts or installs whatever is needed to carry out the attack, which may include the following tactics:

- Introducing malware into organizational information systems
- Placing subverted individuals into privileged positions within the organization
- Installing sniffers or scanning devices on targeted networks and systems
- Inserting tampered hardware or critical components into organizational systems or supply chains

4. Exploit and compromise: The adversary takes advantage of information and systems in order to compromise them, which may involve the following actions:

- Split tunneling or gaining physical access to organizational facilities
- Exfiltrating data or sensitive information
- Exploiting multitenancy in a cloud environment
- Launching zero-day exploits

5. Conduct an attack: The adversary coordinates attack tools or performs activities that interfere with organizational functions. Potential methods of attack include:

- Communication interception or wireless jamming attacks
- Denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks
- Remote interference with or physical attacks on organizational facilities or infrastructures
- Session-hijacking or man-in-the-middle attacks

6. Achieve results: The adversary causes an adverse impact, which may include:

- Obtaining unauthorized access to systems and/or sensitive information
- Degrading organizational services or capabilities
- Creating, corrupting or deleting critical data

7. Maintain a presence or set of capabilities: The adversary continues to exploit and compromise the system using the following techniques:

- Obfuscating adversary actions or interfering with intrusion detection systems (IDSs)
- Adapting cyberattacks in response to organizational security measures

8. Coordinate a campaign: The adversary coordinates a campaign against the organization that may involve the following measures:

- Multi-staged attacks
- Internal and external attacks
- Widespread and adaptive attacks

NONADVERSARIAL THREAT EVENTS

Although most attacks are the result of a coordinated effort, there are other events that can pose various risk to an organization. Some of the most common nonadversarial threat events are:

- Mishandling of critical or sensitive information by authorized users
- Incorrect privilege settings
- Fire, flood, hurricane, windstorm or earthquake at primary or backup facilities
- Introduction of vulnerabilities into software products
- Pervasive disk errors or other problems caused by aging equipment

MALWARE AND ATTACK TYPES⁶

Malware, also called malicious code, is software designed to gain access to targeted computer systems, steal information or disrupt computer operations. There are several types of malware, the most important being computer viruses, network worms and Trojan horses, which are differentiated by the way in which they operate or spread.

A recent example of malware's ability to function as a tool for cyberespionage is Flame, also known as Flamer and Skywiper. Discovered in 2012, it can record keyboard activity and network traffic as well as screenshots, audio and video communications such as Skype. Once collected, the recorded information is sent to various control servers, and a "kill command" is launched to wipe all traces of the malware from the computer.

The computer worm known as Stuxnet highlights malware's potential to disrupt supervisory control and data acquisition (SCADA) systems and programmable logic controllers (PLCs), typically used to automate mechanical processes in factory settings or power plants. Discovered in 2010, Stuxnet was used to compromise Iranian nuclear systems and software. It has three components:

1. A **worm** that carries out routines related to the payload
2. A **link file** that propagates copies of the worm
3. A **rootkit** that hides malicious processes to prevent detection

Other common types of malware include:

Viruses—A computer virus is a piece of code that can replicate itself and spread from one computer to another. It requires intervention or execution to replicate and/or cause damage.

Network worm—A variant of the computer virus, which is essentially a piece of self-replicating code designed to spread itself across computer networks. It does not require intervention or execution to replicate.

Trojan horses—A further category of malware is the Trojan horse, which is a piece of malware that gains access to a targeted system by hiding within a genuine application. Trojan horses are often broken down into categories reflecting their purposes.

Botnets—A botnet (a term derived from "robot network") is a large, automated and distributed network of previously compromised computers that can be simultaneously controlled to launch large-scale attacks such as denial-of-service (DoS).

A number of further terms are also used to describe more specific types of malware, characterized by their purposes. They include:

Spyware—A class of malware that gathers information about a person or organization without the knowledge of that person or organization.

Adware—Designed to present advertisements (generally unwanted) to users.

Ransomware—A class of extortive malware that locks or encrypts data or functions and demands a payment to unlock them.

⁶ ISACA, *Advanced Persistent Threats: How to Manage the Risk to Your Business*, USA, 2013

Keylogger—A class of malware that secretly records user keystrokes and, in some cases, screen content.

Rootkit—A class of malware that hides the existence of other malware by modifying the underlying operating system.

OTHER ATTACK TYPES

In addition to malware, there are many other types of attacks. The MITRE Corporation publishes a catalogue of attack patterns known as Common Attack Pattern Enumeration and Classification (CAPEC) as “an abstraction mechanism for helping describe how an attack against vulnerable systems or networks is executed.” Some of the most common attack patterns are listed below.

Advanced persistent threats—Complex and coordinated attacks directed at a specific entity or organization. They require an enormous amount of research and time, often taking months or even years to fully execute.

Backdoor—A means of regaining access to a compromised system by installing software or configuring existing software to enable remote access under attacker-defined conditions.

Brute force attack—An attack made by trying all possible combinations of passwords or encryption keys until the correct one is found.

Buffer overflow—Occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information—which has to go somewhere—can overflow into adjacent buffers, corrupting or overwriting the valid data held in them.

Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity. In buffer overflow attacks, the extra data may contain codes type of security attack on data integrity.

Cross-site scripting (XSS)—A type of injection in which malicious scripts are injected into otherwise benign and trusted web sites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.

Denial-of-service (DoS) attack—An assault on a service from a single source that floods it with so many requests that it becomes overwhelmed and is either stopped completely or operates at a significantly reduced rate.

Man-in-the-middle attack—An attack strategy in which the attacker intercepts the communication stream between two parts of the victim system and then replaces the traffic between the two components with the intruder’s own, eventually assuming control of the communication.

Social engineering—Any attempt to exploit social vulnerabilities to gain access to information and/or systems. It involves a “con game” that tricks others into divulging information or opening malicious software or programs.

Phishing—A type of electronic mail (email) attack that attempts to convince a user that the originator is genuine, but with the intention of obtaining information for use in social engineering.

Spear phishing—An attack where social engineering techniques are used to masquerade as a trusted party to obtain important information such as passwords from the victim.

Spoofing—Faking the sending address of a transmission in order to gain illegal entry into a secure system.

Structure Query Language (SQL) injection—According to MITRE, SQL injection results from failure of the application to appropriately validate input. When specially crafted user-controlled input consisting of SQL syntax is used without proper validation as part of SQL queries, it is possible to glean information from the database in ways not envisaged during application design.

Zero-day exploit—A vulnerability that is exploited before the software creator/vendor is even aware of its existence.

TOPIC 3—POLICIES AND PROCEDURES

PURPOSE OF POLICIES AND PROCEDURES

Information security policies are a primary element of cybersecurity and governance. They specify requirements and define the roles and responsibilities of everyone in the organization, along with expected behaviors in various situations. Therefore, they must be properly created, accepted and validated by the board and executive management before being communicated throughout the organization. During this process, there may be occasions where other documents must be created to address unique situations separate from the bulk of the organization. This may be necessary when part of the organization has a specific regulatory requirement to protect certain types of information.

POLICY LIFE CYCLE

In addition to a policy framework, another important aspect of information security policies is their lifecycle of development, maintenance, approval and exception.

Every compliance document should have a formal process of being created, reviewed, updated and approved. Additionally, there may be legitimate need for an exception to a policy; therefore, a clear process of how an exception is approved and monitored is necessary.

GUIDELINES

There are several attributes of good policies that should be considered:

- Security policies should be an articulation of a well-defined information security strategy that captures the intent, expectations and direction of management.
- Policies must be clear and easily understood by all affected parties.
- Policies should be short and concise, written in plain language.

Most organizations should create security policies prior to developing a security strategy. Although many organizations tend to follow an ad hoc approach to developing security strategy, there are also instances, especially in smaller organizations, where effective practices have been developed that may not be reflected in written policies. Existing practices that adequately address security requirements may usefully serve as the basis for policy and standards development. This approach minimizes organizational disruptions, communications of new policies and resistance to new or unfamiliar constraints.

COMPLIANCE DOCUMENTS AND POLICY FRAMEWORKS

Compliance documents, such as policies, standards and procedures, outline the actions that are required or prohibited. Violations may be subject to disciplinary actions.

POLICY FRAMEWORKS

The way that compliance documents relate to and support each other is called a policy framework. A framework defines different types of documents and what is contained in each. Organizations may have simple or relatively complex policy frameworks depending on their unique needs.

Some common compliance document types are shown in **exhibit 2.5**.

Exhibit 2.5: Compliance Document Types	
Type	Description
Policies	Communicate required and prohibited activities and behaviors
Standards	Interpret policies in specific situations
Procedures	Provide details on how to comply with policies and standards
Guidelines	Provide general guidance on issues such as “what to do in particular circumstances.” These are not requirements to be met, but are strongly recommended.

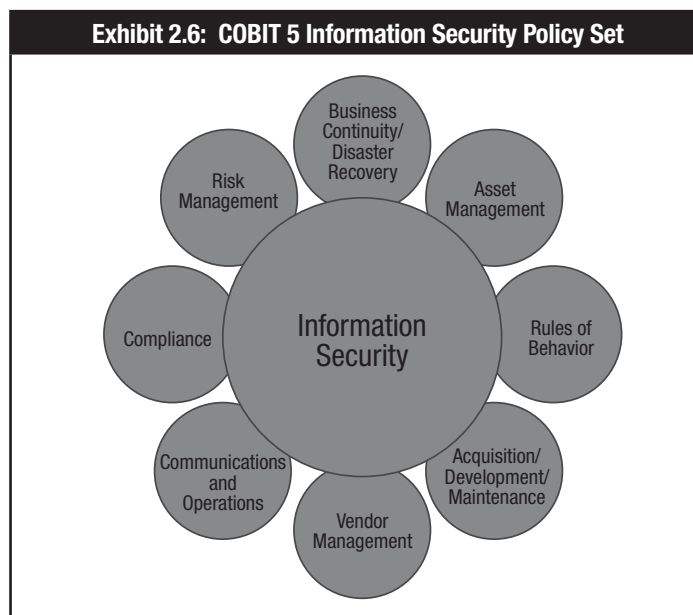
Some organizations may not implement all of these types of documents. For example, smaller organizations may simply have policies and procedures; others may have policies, standards and procedures, but not guidelines.

TYPES OF INFORMATION SECURITY POLICIES

The number and type of policies an organization chooses to implement varies based on the organization’s size, culture, risk, regulatory requirements and complexity of operations. However, some common examples are provided below with the type of information they might contain.⁷

GENERAL INFORMATION SECURITY POLICY

Most organizations have a general, high-level information security policy that may stand alone as a single policy or serve as a foundation for other compliance documents. For larger enterprises, it is common practice to subdivide policies by topic to address all of the information security. The COBIT 5 Information Security policy set is shown in **exhibit 2.6**.



The appearance and length of an information security policy varies greatly among enterprises. Some enterprises consider a one-page overview to be a sufficient information security policy. In these cases, the policy could be considered a directive statement, and it should clearly describe links to other specific policies. In other enterprises, the information security policy is fully developed, containing nearly all the detailed guidance needed to put the principles into practice. It is important to understand what the information stakeholders expect in terms of coverage and to adapt to this expectation.

⁷ ISACA, *COBIT 5 for Information Security*, USA, 2013

Regardless of its size or degree of detail, the information security policy needs a clearly defined scope. This involves:

- The enterprise's definition of information security
- The responsibilities associated with information security
- The vision for information security, accompanied by appropriate goals, metrics and rationale of how the vision is supported by the information security culture and awareness
- Explanation of how the information security policy aligns with other high-level policies
- Elaboration on specific information security topics such as data management, information risk assessment, and compliance with legal, regulatory and contractual obligations

In addition to the elements discussed above, a policy may potentially affect the security life cycle budget and cost management. Information security strategic plans and portfolio management can be added as well.

The policy should be actively communicated to the entire enterprise and distributed to all employees, contractors, temporary employees and third-party vendors. Stakeholders need to know the information principles, high-level requirements, and roles and responsibilities for information security. The responsibility for updating and revalidating the information security policy lies with the cybersecurity function.

Other possible security policies or procedures may include access control, personnel information and security incidents.

ACCESS CONTROL POLICY

The access control policy provides proper access to internal and external stakeholders to accomplish business goals. This can be measured by metrics such as the:

- Number of access violations that exceed the amount allowed
- Amount of work disruption due to insufficient access rights
- Number of segregation of duties incidents or audit findings

Additionally, the access control policy should ensure that emergency access is appropriately permitted and revoked in a timely manner. Metrics related to this goal include the number of emergency access requests and the number of active emergency accounts in excess of approved time limits.

The access control policy should cover the following topics, among others:

- Physical and logical access provisioning life cycle
- Least privilege/need to know
- Segregation of duties
- Emergency access

This policy is meant for all corresponding business units, vendors and third parties. Updates and revalidation should involve HR, data and system owners, and information security. A new or updated policy should be distributed to all corresponding business units, vendors and third parties.

PERSONNEL INFORMATION SECURITY POLICY

The personnel information security policy objective includes, but is not limited to, the following goals:

- Execute regular background checks of all employees and people at key positions. This goal can be measured by counting the number of completed background checks for key personnel. This can be amplified with the number of overdue background check renewals based on a predetermined frequency.
- Acquire information about key personnel in information security positions. This can be followed up by counting the number of personnel in key positions that have not rotated according to a predefined frequency.
- Develop a succession plan for all key information security positions. A starting point is to list all the critical information security positions that lack backup personnel.
- Define and implement appropriate procedures for termination. This should include details about revoking account privileges and access.

This policy is meant for all corresponding business units, vendors and third parties. Updates and revalidation should involve HR, the privacy officer, the legal department, information security and facility security. A new or updated policy needs to be distributed to employees, contract personnel, vendors under contract and temporary employees.

SECURITY INCIDENT RESPONSE POLICY

This policy addresses the need to respond to incidents in a timely manner in order to recover business activities. The policy should include:

- A definition of an information security incident
- A statement of how incidents will be handled
- Requirements for the establishment of the incident response team, with organizational roles and responsibilities
- Requirements for the creation of a tested incident response plan, which will provide documented procedures and guidelines for:
 - Criticality of incidents
 - Reporting and escalation processes
 - Recovery (including):
 - Investigation and preservation of process
 - Testing and training
 - Post incident meetings to document root cause analysis and enhancements of information security practices that prevent similar future events
- Incident documentation and closing

This policy is meant for all corresponding business units and key employees. Updates and revalidation should involve the information security function. A new or updated policy should be distributed to key employees.

TOPIC 4—CYBERSECURITY CONTROLS

Cybersecurity is a dynamic and ever-changing environment and therefore requires continuous monitoring, updating, testing, patching and changing as technology and business evolve. These controls are critical to maintaining security within any organization's IT infrastructure. Failure to address these processes is one of the top causes of vulnerabilities.

IDENTITY MANAGEMENT

Cybersecurity relies upon the establishment and maintenance of user profiles that define the authentication, authorization and access controls for each user. Today, organizations have a variety of *ad hoc* processes and tools to manage and provision user identity information. Identity management focuses on streamlining various business processes needed to manage all forms of identities in an organization—from enrollment to retirement.

The ability to integrate business processes and technology is critically important in the emerging model because it links people to systems and services. A key objective of identity management is to centralize and standardize this process so that it becomes a consistent and common service across the organization.

Identity management is comprised of many components that provide a collective and common infrastructure, including directory services, authentication services (validating who the user is) and authorization services (ensuring the user has appropriate privileges to access systems based on a personalized profile). It also includes user-management capabilities, such as user provisioning and deprovisioning.

PROVISIONING AND DEPROVISIONING

User provisioning is part of the organization's hiring process where user accounts are created. Passwords and access control rights are generally assigned based on the job duties of the users. This can be a complicated process, as users may need access to many different resources such as systems, databases, email, applications and remote services, each of which has its own access control, passwords, encryption keys or other authorization and authentication requirements. Additionally, access control rights often change based on shifting job requirements, so it is frequently necessary to update access controls and remove access that is no longer needed. Likewise, when a user leaves an organization, their accounts need to be deprovisioned—meaning that all accounts and accesses must be suspended or deleted in a timely manner.

AUTHORIZATION⁸

The authorization process used for access control requires that the system be able to identify and differentiate among users. Access rules (authorizations) specify who can access what. For example, access control is often based on least privilege, which means granting users only those accesses required to perform their duties.

Access should be on a documented need-to-know and need-to-do basis by type.

Computer access can be set for various levels, e.g., files, tables, data items etc. When IS auditors review computer accessibility, they need to know what can be done with the access and what is restricted. For example, access restrictions at the file level generally include the following:

- Read, inquiry or copy only
- Write, create, update or delete only
- Execute only
- A combination of the above

The least dangerous type of access is read-only, as long as the information being accessed is not sensitive or confidential. This is because the user cannot alter or use the computerized file beyond basic viewing or printing.

⁸ ISACA, *CISA Review Manual 2014*, USA

ACCESS CONTROL LISTS⁹

To provide security authorizations for the files and facilities listed previously, logical access control mechanisms utilize access authorization tables, also referred to as access control lists (ACLs) or access control tables. ACLs refer to a register of users (including groups, machines and processes) who have permission to use a particular system resource.

The types of access permitted by ACLs vary considerably in their capability and flexibility. Some only allow specifications for certain preset groups (e.g., owner, group or world), while more advanced ACLs allow much more flexibility (e.g., user-defined groups), and they can also be used to explicitly deny access to a particular individual or group. With more advanced ACLs, access is at the discretion of the policy maker and implemented by the security administrator or individual user, depending upon how the controls are technically implemented. When a user changes job roles within an organization, often their old access rights are not removed before adding their new required accesses. Without removing the old access rights, there could be a potential segregation of duties issue.

ACCESS LISTS^{10, 11}

Access lists filter traffic at router interfaces based on specified criteria, thus affording basic network security. Without access lists, routers pass all packets. Conversely, after an access list is created and applied to an interface, it then only passes traffic permitted by rules due to an implied “deny all” statement automatically appended to the list. Understanding the placement and impact of an access list is essential because errors can halt network traffic entirely.

PRIVILEGED USER MANAGEMENT

Privileged access permits authorized users to maintain and protect systems and networks. Privileged users can often access any information stored within a system, which means they can modify or circumvent existing safeguards such as access controls and logging.

Because of this elevated access, organizations need to think carefully about privileged users and accounts and apply additional controls to them. Common controls include:

- Limiting privileged access to only those who require it to perform their job functions
- Performing background checks on individuals with elevated access
- Implementing additional logging of activity associated with privileged accounts
- Maintaining accountability by never sharing privileged accounts
- Using stronger passwords or other authentication controls to protect privileged accounts from unauthorized access
- Regularly reviewing accounts for privileges and removing those no longer required

CHANGE MANAGEMENT

Change management is essential to the IT infrastructure. Its purpose is to ensure that changes to processes, systems, software, applications, platforms and configuration are introduced in an orderly, controlled manner. Controls are implemented in the form of a structured review process intended to evaluate and minimize the potential for disruption that a proposed change, maintenance activity or patch may introduce. Effective controls ensure that all changes are categorized, prioritized and authorized. The process generally includes mechanisms for tracking and documenting changes to demonstrate accountability and compliance with best practices.

It is important to note that change management is not a standalone process; it draws upon a number of other processes and controls. Therefore, it requires a comprehensive knowledge of enterprise operations and infrastructure to be implemented effectively.

⁹ ISACA, *CISA Review Manual 2013*, USA

¹⁰ Wilson, Tracey; *Basics of Access Control Lists: How to Secure ACLs*, 16 May 2012, <http://blog.pluralsight.com/access-control-list-concepts>

¹¹ Cisco; *Access Control Lists: Overview and Guidelines*, *Cisco IOS Security Configuration Guide*, www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfacs.html

CONFIGURATION MANAGEMENT

Maintaining the security configurations of network devices, systems, applications and other IT resources is critically important to ensure security controls are properly installed and maintained. As organizations grow and evolve, so does the potential for change and dysfunction. In order to manage such changes and minimize their potential to disrupt operations, efficiency and profits, it is necessary to develop formal processes. These processes of configuration management can be quite complex, as they support many other activities within the enterprise.

Implementing a configuration management process has several benefits for security including:¹²

- Verification of the impact on related items
- Assessment of a proposed change's risk
- Ability to inspect different lines of defense for potential weaknesses
- Tracking of configuration items against approved secure configuration baselines
- Insights into investigations after a security breach or operations disruption
- Version control and production authorization of hardware and software components

PATCH MANAGEMENT

Patches are solutions to software programming errors. In many cases, security vulnerabilities are introduced by coding errors. Therefore, it is vital that software bugs that are identified as security vulnerabilities be patched as soon as possible. Most software vendors release regular software updates and patches as the vulnerabilities are identified and fixed.

Failure to apply patches to known security vulnerabilities is the most common cause of security breaches. Patching is therefore an important part of vulnerability management, and organizations must set up processes to identify patches that are relevant to their IT infrastructure. Once a necessary patch is identified, it should be tested to ensure it does not negatively impact operations. After the patch has been verified, it can be scheduled and installed where appropriate.

¹² ISACA, *Configuration Management Using COBIT 5*, USA, 2013

SECTION 2—KNOWLEDGE CHECK

Directions: Select the correct answer to complete each statement below. Use each word only once.

WORD BANK

Standards	Vulnerability	Guidelines
Attack Vector	Policies	Risk
Threat	Asset	Patches
Identity Management	Malware	Rootkit
Payload	Procedure	

1. The core duty of cybersecurity is to identify, respond to and manage _____ to an organization's digital assets.
2. A(n) _____ is anything capable of acting against an asset in a manner that can cause harm.
3. A(n) _____ is something of value worth protecting.
4. A(n) _____ is a weakness in the design, implementation, operation or internal controls in a process that could be exploited to violate the system security.
5. The path or route used to gain access to the target asset is known as a(n) _____.
6. In an attack, the container that delivers the exploit to the target is called a(n) _____.
7. _____ communicate required and prohibited activities and behaviors.
8. _____ is a class of malware that hides the existence of other malware by modifying the underlying operating system.
9. _____ provide details on how to comply with policies and standards.
10. _____ provide general guidance and recommendations on what to do in particular circumstances.
11. _____, also called malicious code, is software designed to gain access to targeted computer systems, steal information or disrupt computer operations.
12. _____ are used to interpret policies in specific situations.
13. _____ are solutions to software programming and coding errors.
14. _____ includes many components such as directory services, authentication and authorization services, and user management capabilities such as provisioning and deprovisioning.

Security Architecture Principles

Topics covered in this section include:

1. Perimeter security concepts
2. Security architectures and frameworks
3. The OSI model and TCP/IP communication protocol
4. Defense in depth
5. Firewall concepts and implementations
6. Isolation and segmentation
7. Intrusion detection and prevention systems
8. Antivirus and anti-malware
9. Encryption fundamentals, techniques and applications

Page intentionally left blank

TOPIC 1—OVERVIEW OF SECURITY ARCHITECTURE

Security architecture describes the structure, components, connections and layout of security controls within an organization's IT infrastructure. Organizations have different types of security architectures that determine the particulars of various subsystems, products and applications. These particulars will in turn influence an organization's approach to **defense in depth**, or the practice of layering defenses to provide added protection.

Security architecture shows how defense in depth is implemented, as well as how layers of control are linked. It is therefore essential to designing and implementing security controls in any complex environment.

Each component of a given system poses its own security risk. Because the topology of security architecture varies from one organization to another, there are a number of different variables and risk to consider when addressing the topology of a particular organization. This section will discuss those variables individually, along with best practices for successfully managing their related risk.

THE VIRTUAL ORGANIZATION

Outsourcing, both onshore and offshore, is increasingly common as companies focus on core competencies and ways to cut costs. From an information security point of view, these arrangements can present risk that may be difficult to quantify and potentially difficult to mitigate. Typically, both the resources and skills of the outsourced functions are lost to the organization, which itself will present a set of risk. Providers may operate on different standards and can be difficult to control. The security strategy should consider outsourced security services carefully to ensure either that they are not a critical single point of failure or that there is a viable backup plan in the event of service provider failure.¹³

Much of the risk posed by outsourcing can also materialize as the result of mergers and acquisitions. Typically, significant differences in culture, systems, technology and operations between the parties present a host of security challenges that must be identified and addressed. Often, in these situations, security is an afterthought and the security manager must strive to gain a presence in these activities and assess the risk for management consideration.¹⁴

THE SECURITY PERIMETER

Many current security controls and architectures were developed with the concept of a perimeter—a well-defined (if mostly virtual) boundary between the organization and the outside world. In these models of cybersecurity, the focus is **network-** or **system-centric**. In the system-centric model, the emphasis is on placing controls at the network and system levels to protect the information stored within. An alternative model is **data-centric**, which emphasizes the protection of data regardless of its location.

With the advent of the Internet, outsourcing, mobile devices, cloud and other hosted services, the perimeter has expanded considerably. Consequently, there are significant new risk and vulnerabilities to confront in this hyper-connected and extended environment. The perimeter, then, is an important line of defense that protects the enterprise against external threats, and its design should reflect a proactive stance toward preventing potential risk.

An important component of the security perimeter is the Internet perimeter. This perimeter ensures secure access to the Internet for enterprise employees and guest users residing at all locations, including those involved in telecommuting or remote work. In order to provide security of email, front-end mobile and web apps, domain name system (DNS), etc., the Internet perimeter should:

- Route traffic between the enterprise and the Internet
- Prevent executable files from being transferred through email attachments or HTTP responses
- Monitor network ports for rogue activity
- Detect and block traffic from infected internal end points

¹³ ISACA, *CISM Review Manual 2015*, USA

¹⁴ *Ibid.*

- Control user traffic bound toward the Internet
- Identify and block anomalous traffic and malicious packets recognized as potential attacks
- Eliminate threats such as email spam, viruses and worms
- Enforce filtering policies to block access to web sites containing malware or questionable content

The perimeter should also provide protection for virtual private networks (VPNs), wide area networks (WANs) and wireless local area networks (WLANs).

For VPNs, this protection should be threefold:

1. Terminate VPN traffic from remote users
2. Provide a hub for terminating VPN traffic from remote sites
3. Terminate traditional dial-in users

VPN traffic is first filtered at the egress point to the specific IP addresses and protocols that are part of the VPN service. A remote user can only gain access after being authenticated.

For WANs, security is provided by input/output system (IOS) features. Unwanted traffic can be blocked from the remote branch using input access lists, and IP spoofing can be mitigated through L3 filtering. Organizations that are very concerned about privacy may choose to encrypt traffic on their WAN links.

INTERDEPENDENCIES

As previously discussed, modern IT architectures are usually decentralized and deperimeterized. This includes a growing number of cloud-based platforms and services, as well as a shift in computing power and utilization patterns toward intelligent mobile devices such as tablet PCs or smartphones. As a consequence, both the number of potential attack targets outside the organizational boundary and the number of attack vectors have grown. Conversely, the degree of control over deperimeterized environments has been significantly reduced, especially in enterprises permitting partial or full integration of user-owned mobile devices (i.e., bring your own device [BYOD]). These changes have important ramifications for security architecture.

In distributed and decentralized IT architectures, the third-party risk is likely to increase, often as a function of moving critical applications, platforms and infrastructure elements into the cloud. For platforms, storage infrastructure and cloud-based data repositories, the focus of cybersecurity is shifting toward contracts and service level agreements (SLAs). Simultaneously, third-party cloud providers are facing an increased risk of attacks and breaches due to the agglomeration and clustering of sensitive data and information. In addition to concerns about third-party services, there is significant legal risk. Enterprises experiencing a loss of sensitive data may not be in a position to bring an action against the perpetrators because the cloud provider often has to initiate legal action.

Regardless of the generic information security arrangements made by an enterprise, there are often exposed areas within IT architectures. Cybercrime and cyberwarfare perpetrators continue to aim at “weak spots” in architectural elements and systems. In contrast to indiscriminate and opportunistic attacks, APTs and cybercrime always rely on preparatory research and insight into the target enterprise. This, in turn, raises the level of exposure for weak or unsecured parts of the overall architecture. These vulnerable spots include legacy systems, unpatched parts of the architecture, “dual persona” use of mobile devices and many others.

SECURITY ARCHITECTURES AND FRAMEWORKS

A great number of architectural approaches currently exist, and many of them have evolved from the development of enterprise architecture. Although their specific details may differ, they all generally aim to articulate what processes a business performs and how those processes are executed and secured. They articulate the organization, roles, entities and relationships that exist or should exist to perform a set of business processes.

Similarly, models of security architecture typically fall into two categories: process models and framework models. Frameworks allow a great deal of flexibility in how each element of the architecture is developed. The essence of a framework is to describe the elements of architecture and how they relate to one another, while a process model is more directive in its approach to the processes used for the various elements.

SABSA AND THE ZACHMAN FRAMEWORK

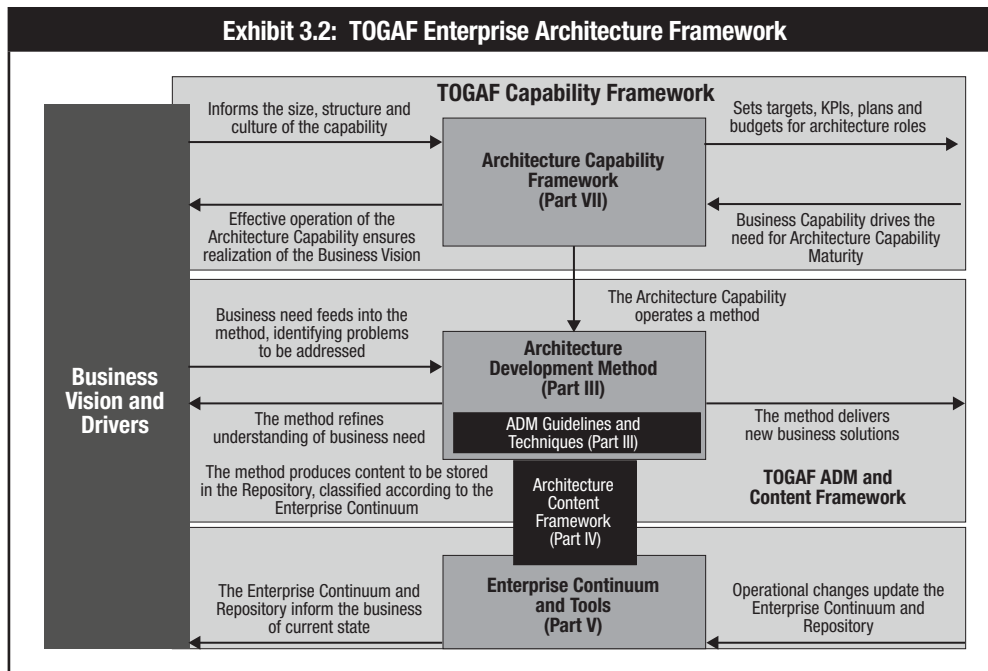
Just as there are many different types of business enterprises, there are many different approaches to security architecture. For example, the Zachman framework approach of developing a who, what, why, where, when and how matrix (shown in **exhibit 3.1**) is shared by Sherwood Applied Business Security Architecture (SABSA). The matrix contains columns showing aspects of the enterprise that can be described or modeled, while the rows represent various viewpoints from which those aspects can be considered. This approach provides a logical structure for classifying and organizing design elements, which improves the completeness of security architecture.

Exhibit 3.1: SABSA Security Architecture Matrix						
	Assets (What)	Motivation (Why)	Process (How)	People (Who)	Location (Where)	Time (When)
Contextual	The Business	Business Risk Model	Business Process Model	Business Organization and Relationships	Business Geography	Business Time Dependencies
Conceptual	Business Attributes Profile	Control Objectives	Security Strategies and Architectural Layering	Security Entity Model and Trust Framework	Security Domain Model	Security-related Lifetimes and Deadlines
Logical	Business Information Model	Security Policies	Security Services	Entity Schema and Privilege Profiles	Security Domain Definitions and Associations	Security Processing Cycle
Physical	Business Data Model	Security Rules, Practices and Procedures	Security Mechanisms	Users, Applications and the User Interface	Platform and Network Infrastructure	Control Structure Execution
Component	Detailed Data Structures	Security Standards	Security Products and Tools	Identities, Functions, Actions and ACLs	Processes, Nodes, Addresses and Protocols	Security Step Timing and Sequencing
Operational	Assurance of Operational Continuity	Operational Risk Management	Security Service Management and Support	Application and User Management and Support	Security of Sites, Networks and Platforms	Security Operations Schedule

Source: Sherwood Applied Business Security Architecture (SABSA), 1995-2008. All rights reserved. Used with permission.
www.sabsa.org.

THE OPEN GROUP ARCHITECTURE FRAMEWORK (TOGAF)

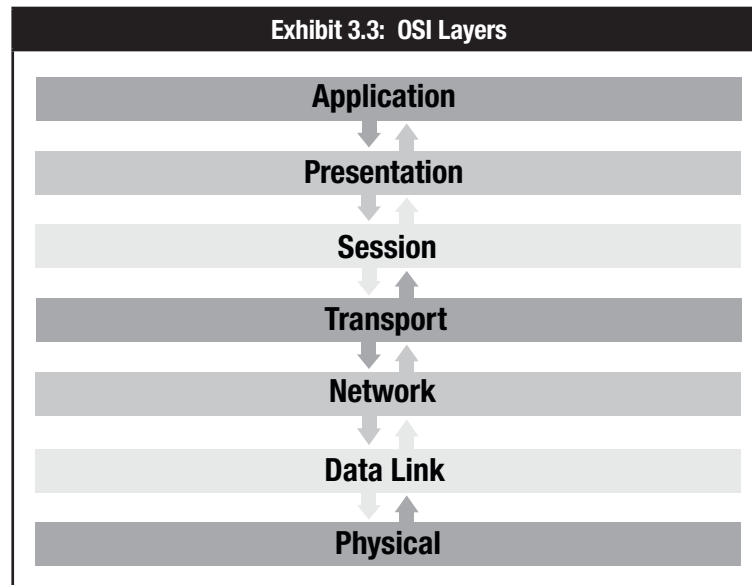
Another architecture framework is The Open Group Architecture Framework (TOGAF). Developed by The Open Group in the 1990s, this high-level and holistic approach addresses security as an essential component of the overall enterprise design. TOGAF's objective is to ensure that architectural development projects meet business objectives, that they are systematic and that their results are repeatable. **Exhibit 3.2** depicts the TOGAF architectural process and its relationship to businesses operations.



TOPIC 2—THE OSI MODEL

The Open Systems Interconnect (OSI) model is used to describe networking protocols. Because it is rarely implemented in actual networks, it is considered a reference to standardize the development of actual networks. OSI was the first nonproprietary open definition for networking.

The OSI model defines groups of functionality required for network computers into layers, with each layer implementing a standard protocol for its functionality. There are seven layers in the OSI model, shown in **exhibit 3.3**.



Each OSI layer performs a specific function for the network:

Physical Layer—Manages signals among network systems

Data Link Layer—Divides data into frames that can be transmitted by the physical layer

Network Layer—Translates network addresses and routes data from sender to receiver

Transport Layer—Ensures that data are transferred reliably in the correct sequence

Session Layer—Coordinates and manages user connections

Presentation Layer—Formats, encrypts and compresses data

Application Layer—Mediates between software applications and other layers of network services

TCP/IP

The protocol suite used as the de facto standard for the Internet is known as the Transmission Control Protocol/Internet Protocol (TCP/IP). The TCP/IP suite includes both network-oriented protocols and application support protocols. **Exhibit 3.4** shows some of the standards associated with the TCP/IP suite and where these fit within the OSI model. It is interesting to note that the TCP/IP set of protocols was developed before the OSI framework; therefore, there is no direct match between the TCP/IP standards and the layers of the framework.

Exhibit 3.4: OSI Association with the TCP/IP Suite

	OSI Model	TCP/IP Conceptual Layers	Protocol Data Unit (PDU)	TCP/IP Protocols	Equipment	Layer Functions	Layer Functions
7	Application	Application	Data	HTTP File Transport Protocol (FTP) Simple Mail Transport Protocol (SMTP) TFTP NFS Name Server Protocol (NSP) Simple Network Management Protocol (SNMP) Remote Terminal Control Protocol (Telnet) LPD X Windows DNS DHCP/BootP	Gateway	Provides user interface	File, print, message, database, and application services
6	Presentation					Presents data	Data encryption, compression and translation services
5	Session					Keeps separate the data of different applications	Dialog control
4	Transport	Transport	Segment	Transmission Control Protocol (TCP) User Datagram Protocol (UDP)	Layer 4 switch	Provide reliable or unreliable delivery	End-to-end connection
3	Network	Network interface	Packet	ICMP ARP RARP Internet Protocol (IP)	Router Layer 3 switch	Provides logical addressing which routers use for path determination	Routing
2	Data link	LAN or WAN interface	Frame	Ethernet Fast Ethernet FDDI Token Ring Point-to-point Protocol (PPP)	Layer 2 switch Bridge Wireless AP NIC	Combines packets into bytes and bytes into frames Provides access to media using MAC address Performs error detection, not error correction	Framing
1	Physical		Bits		Hub Repeater NIC	Moves bits between devices Specifies voltage, wire speed and pin-out of cables	Physical topology

Source: ISACA, *CISA Review Manual 2015*, USA, 2015, exhibit 4.18

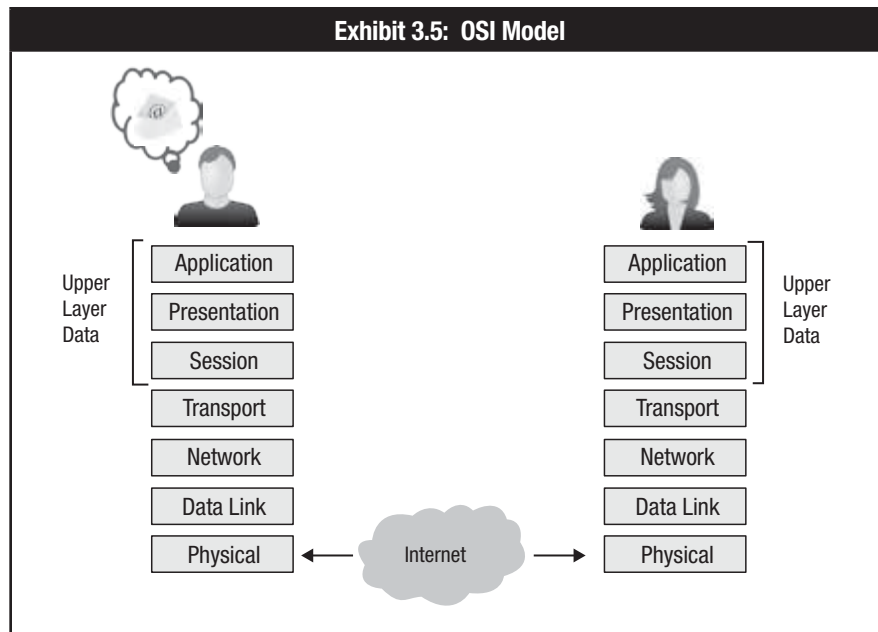
ENCAPSULATION

Encapsulation is the process of adding addressing information to data as it is transmitted down the OSI stack. Each layer relies on the services provided by the layer below. Each layer of the OSI model only communicates with its destination peer. It does so using datagrams or Protocol Data Units (PDUs). Refer to the previous **exhibit 3.4** for PDU names.

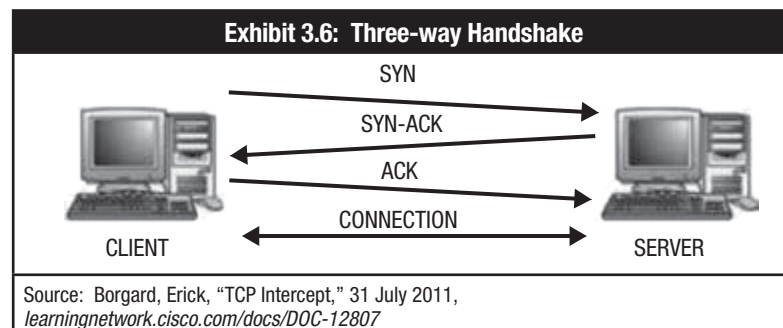
The OSI model is shown in **exhibit 3.5**. Upper layer data are passed down to the transport layer as segments and are “wrapped” with a header for identification.

These segments are passed down to the network layer as packets again with a header. Data are broken down to frames at the data link layer and also have control information appended. At the physical layer, data take the form of bits (1s and 0s) for delivery to destination network.

Once at the destination—each layer on the receiving end strips off the appropriate addressing information and passes it up the OSI stack until the message is delivered. This process is called decapsulation.



Communication services at layer 4 are categorized as either connection-oriented or connectionless. TCP provides reliable, sequenced delivery with error-checking. Connections are established using a three-way handshake, and thus are connection-oriented, as shown in **exhibit 3.6**. User Datagram Protocol (UDP) is a connectionless protocol used where speed is more important than error-checking and guaranteed delivery. UDP does use checksums for data integrity.



Page intentionally left blank

TOPIC 3—DEFENSE IN DEPTH

Because no single control or countermeasure can eliminate risk, it is often important to use several controls to protect an asset. This process of layering defenses is known as **defense in depth**, but it may also be called protection in depth and security in depth. It forces an adversary to defeat or avoid more than one control to gain access to an asset.

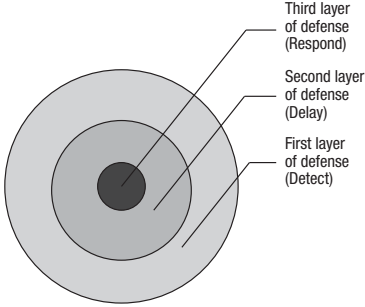
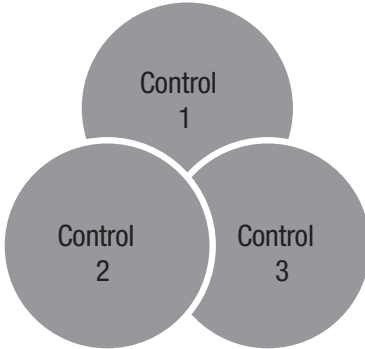

Defense in depth is an important concept in designing an effective information security strategy or architecture. When designed and implemented correctly, multiple control layers provide multiple opportunities for monitoring to detect the attack. Adding additional controls to overcome also creates a delay so that the attack may be interrupted and prevented.

The number and types of layers needed is a function of asset value, criticality, the reliability of each control and the degree of exposure. Excessive reliance on a single control is likely to create a false sense of confidence. For example, a company that depends solely on a firewall can still be subject to numerous attack methodologies. A further defense may be to use education and awareness to create a “human firewall,” which can constitute a critical layer of defense. Segmenting the network can constitute yet another defensive layer.

Using a defense in depth strategy for implementing controls has several advantages, including increasing the effort required for a successful attack and creating additional opportunities to detect or delay an attacker. There are several ways defense in depth can be implemented, as shown in **exhibit 3.7**.¹⁵

¹⁵ Encurve, LLC, *Risk Management Concepts Presentation*, 2013

Exhibit 3.7: Types of Defense in Depth Implementations

Type of Defense	Graphical Representation	Description
Concentric Rings (or nested layering)	 <p>Third layer of defense (Respond) Second layer of defense (Delay) First layer of defense (Detect)</p>	<p>Creates a series of nested layers that must be bypassed in order to complete an attack.</p> <p>Each layer delays the attacker and provides opportunities to detect the attack.</p>
Overlapping redundancy		<p>Two or more controls that work in parallel to protect an asset.</p> <p>Provides multiple, overlapping points of detection. This is most effective when each control is different.</p>
Segregation or compartmentalization		<p>Compartmentalizes access to an asset, requiring two or more processes, controls or individuals to access or use the asset.</p> <p>This is effective in protecting very high value assets or in environments where trust is an issue.</p>

Another way to think about defense in depth is from an architectural perspective of:

- **Horizontal defense in depth**, where controls are placed in various places in the path of access for an asset, which is functionally equivalent to concentric ring model above
- **Vertical defense in depth**, where controls are placed at different system layers—hardware, operating system, application, database or user levels

Using defense in depth techniques does require effective planning and understanding of each type's strengths and weaknesses as well as how the controls interact. It is easy to create an overly complex system of controls, and too many layers can be as bad as too few. When developing defense in depth implementations, consider the following questions:

- What vulnerabilities are addressed by each layer or control?
- How does the layer mitigate the vulnerability?
- How does each control interact with or depend on the other controls?

TOPIC 4—FIREWALLS

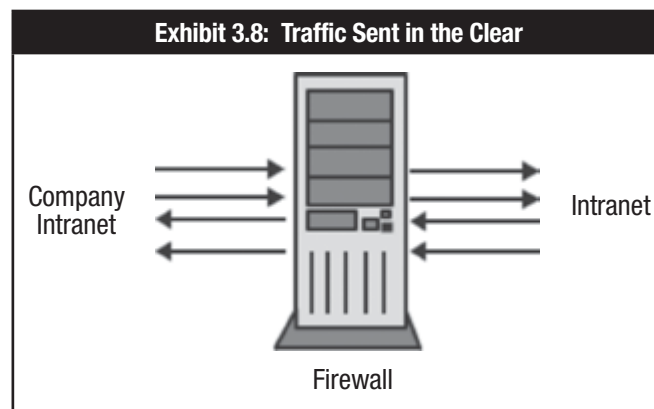
The Internet's openness makes every corporate network connected to it vulnerable to attack. Hackers on the Internet could theoretically break into a corporate network and do harm in a number of ways—by stealing or damaging important data, by damaging individual computers or the entire network, by using the corporate computer's resources or by using the corporate network and resources to pose as a corporate employee. Companies should build firewalls as one means of perimeter security for their networks.

A **firewall** is defined as a system or combination of systems that enforces a boundary between two or more networks, typically forming a barrier between a secure and an open environment such as the Internet. It applies rules to control the type of networking traffic flowing in and out. Most commercial firewalls are built to handle commonly used Internet protocols.

Effective firewalls should allow individuals on the corporate network to access the Internet and simultaneously prevent others on the Internet from gaining access to the corporate network to cause damage. Most organizations follow a deny-all philosophy, which means that access to a given resource will be denied unless a user can provide a specific business reason or need for access to the information resource. The converse of this access philosophy—which is not widely accepted—is the accept-all philosophy, under which everyone is allowed access unless someone can provide areas for denying access.

FIREWALL GENERAL FEATURES

Firewalls separate networks from one another and screen the traffic between them. See **exhibit 3.8**.



Thus, along with other types of security, firewalls control the most vulnerable point between a corporate network and the Internet, and they can be as simple or complex as the corporate information security policy demands.

There are many different types of firewalls, but most of them enable organizations to:

- Block access to particular sites on the Internet.
- Limit traffic on an organization's public services segment to relevant addresses and ports.
- Prevent certain users from accessing certain servers or services.
- Monitor and record communications between an internal and an external network.
- Monitor and record communications between an internal network and the outside world to investigate network penetrations or detect internal subversion.
- Encrypt packets that are sent between different physical locations within an organization by creating a VPN over the Internet (e.g., IP security [IPSec], VPN tunnels). The capabilities of some firewalls can be extended so they can also provide for protection against viruses and attacks directed to exploit known operating system vulnerabilities.

NETWORK FIREWALL TYPES

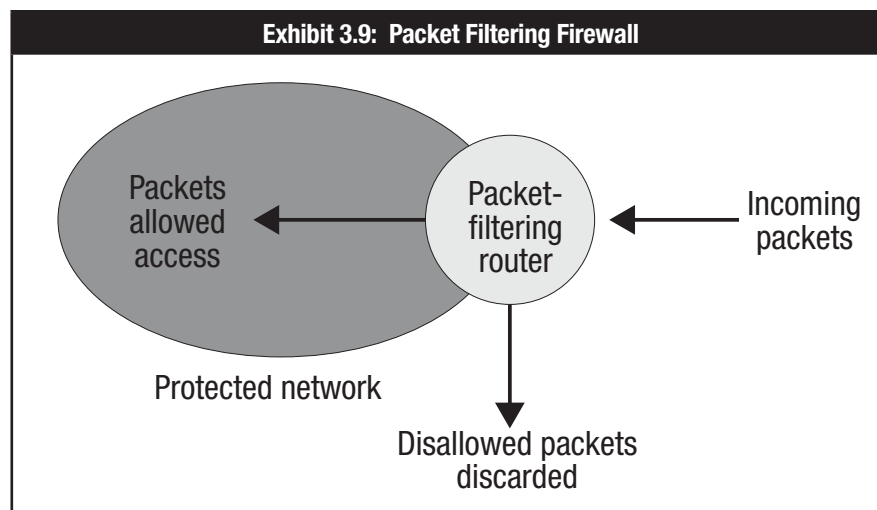
Generally, the types of network firewalls available today fall into three categories:

- Packet filtering
- Application firewall systems
- Stateful inspection
- Next generation firewall (NGFW)

Each type of firewall is discussed in the following sections.

PACKET FILTERING FIREWALLS

First generation firewalls were packet filtering-based firewalls deployed between the private network and the Internet. In **packet filtering**, a screening router examines the header of every packet of data traveling between the Internet and the corporate network. Packet headers contain information, including the IP address of the sender and receiver, along with the port numbers (application or service) authorized to use the information transmitted. Based on that information, the router knows what kind of Internet service (e.g., web-based service or FTP) is being used to send the data as well as the identities of the sender and receiver of the data. Then, the router can prevent certain packets from being sent between the Internet and the corporate network. For example, the router could block any traffic to and from suspicious destinations. See **exhibit 3.9**.



Because the direct exchange of packets is permitted between outside systems and inside systems, the potential for an attack is determined by the total number of hosts and services to which the packet filtering router permits traffic. Packet filtering firewalls are therefore best suited for smaller networks. Organizations with many routers may face difficulties in designing, coding and maintaining the rule base.

Because their filtering rules are performed at the network layer, packet filtering firewalls are generally stable and simple. This simplicity has both advantages and disadvantages, as shown in **exhibit 3.10**.

Exhibit 3.10: Packet Filtering Firewalls	
Advantages	Disadvantages
Simplicity of one network “choke point”	Vulnerable to attacks from improperly configured filters
Minimal impact on network performance	Vulnerable to attacks tunneled over permitted services
Inexpensive or free	All private network systems vulnerable when a single packet filtering router is compromised

In light of these advantages and disadvantages, packet filtering is most effective when implemented with basic security and monitoring in mind.

Some of the more common attacks against packet filter firewalls are:

- **IP spoofing**—In this type of attack, the attacker fakes the IP address of either an internal network host or a trusted network host. This enables the packet being sent to pass the rule base of the firewall and penetrate the system perimeter. If the spoofing uses an internal IP address, the firewall can be configured to drop the packet on the basis of packet flow direction analysis. However, attackers with access to a secure or trusted external IP address can spoof on that address, leaving the firewall architecture defenseless.
- **Source routing specification**—This type of attack centers around the routing that an IP packet must take when it traverses the Internet from the source host to the destination host. In this process, it is possible to define the route so it bypasses the firewall. However, the attacker must know the IP address, subnet mask and default gateway settings to accomplish this. A clear defense against this attack is to examine each packet and drop packets whose source routing specification is enabled. Note that this countermeasure will not be effective if the topology permits a route that skips the choke point.
- **Miniature fragment attack**—Using this method, an attacker fragments the IP packet into smaller ones and pushes it through the firewall. This is done with the hope that only the first sequence of fragmented packets will be examined, allowing the others to pass without review. This is possible only if the default setting is to pass residual packets. Miniature fragment attacks can be countered by configuring the firewall to drop all packets where IP fragmentation is enabled.

APPLICATION FIREWALL SYSTEMS

Packet filtering routers allow the direct flow of packets between internal and external systems. The primary risk of allowing packet exchange between internal and external systems is that the host applications residing on the protected network's systems must be secure against any threat posed by the allowed packets.

In contrast to packet filtering routers, application- and circuit-level gateways allow information to flow between systems but do not allow the direct exchange of packets. Therefore, application firewall systems provide greater protection capabilities than packet filtering routers.

The two types of application firewall systems sit atop hardened (i.e., tightly secured) operating systems such as Windows NT and UNIX®. They work at the application level of the OSI model.

There are two types of application firewall systems:

- **Application-level gateways**—Application-level gateways are systems that analyze packets through a set of proxies—one for each service (e.g., Hypertext Transmission Protocol [HTTP] proxy for web traffic, FTP proxy). The implementation of multiple proxies, however, impacts network performance. When network performance is a concern, a circuit-level gateway may be a better choice.
- **Circuit-level gateways**—Commercially, circuit-level gateways are quite rare. Because they use one proxy server for all services, they are more efficient and also operate at the application level. There, TCP and UDP sessions are validated, typically through a single, general-purpose proxy before opening a connection. This differs from application-level gateways, which require a special proxy for each application-level service.

Both application firewall systems employ the concept of bastion hosting in that they handle all incoming requests from the Internet to the corporate network, such as FTP or web requests. Bastion hosts are heavily fortified against attack. When there is only one host handling incoming requests, it is easier to maintain security and track attacks. In the event of a break-in, only the firewall system is compromised, not the entire network.

This way, none of the computers or hosts on the corporate network can be contacted directly for requests from the Internet, providing an effective level or layer of security.

Additionally, application-based firewall systems are set up as proxy servers to act on the behalf of someone inside an organization's private network. Rather than relying on a generic packet filtering tool to manage the flow of Internet services through the firewall, a special-purpose code called a proxy server is incorporated into the firewall system. For example, when someone inside the corporate network wants to access a server on the Internet, a request from the computer is sent to the proxy server. The proxy server contacts the Internet server, and the proxy server then sends the information from the Internet server to the computer inside the corporate network. By acting as a go-between, proxy servers can maintain security by examining the program code of a given service (e.g., FTP, Telnet). It then modifies and secures it to eliminate known vulnerabilities. The proxy server can also log all traffic between the Internet and the network.

One feature available on both types of firewall systems is the network address translation (NAT) capability. This capability takes private internal network addresses, which are unusable on the Internet, and maps them to a table of public IP addresses assigned to the organization, which can be used across the Internet.

Application firewalls have advantages and disadvantages, as shown in **exhibit 3.11**.

Exhibit 3.11: Application Firewalls	
Advantages	Disadvantages
Provide security for commonly used protocols	Poor performance and scalability as Internet usage grows
Generally hide the network from outside untrusted networks	
Ability to protect the entire network by limiting break-ins to the firewall itself	
Ability to examine and secure program code	

STATEFUL INSPECTION FIREWALLS

A stateful inspection firewall, also referred to as dynamic packet filtering, tracks the destination IP address of each packet that leaves the organization's internal network. Whenever a response to a packet is received, its record is referenced to ascertain whether the incoming message was made in response to a request that the organization sent out. This is done by mapping the source IP address of an incoming packet with the list of destination IP addresses that is maintained and updated. This approach prevents any attack initiated and originated by an outsider.

In contrast to application firewalls, stateful inspection firewalls provide control over the flow of IP traffic. They do this by matching information contained in the headers of connection-oriented or connectionless IP packets at the transport layer against a set of rules authorized by the organization. Consequently, they have advantages and disadvantages, as shown in **exhibit 3.12**.

Exhibit 3.12: Stateful Inspection Firewalls	
Advantages	Disadvantages
Provide greater control over the flow of IP traffic	Complex to administer
Greater efficiency in comparison to CPU-intensive, full-time application firewall systems	

STATELESS VS. STATEFUL

Stateless filtering does not keep the state of ongoing TCP connection sessions. In other words, it has no memory of what source port numbers the sessions' client selected. Stateful firewalls keep track of TCP connections. The firewall keeps an entry in a cache for each open TCP connection. Stateless firewalls perform more quickly than stateful firewalls, but they are not as sophisticated.

EXAMPLES OF FIREWALL IMPLEMENTATIONS

Firewall implementations can take advantage of the functionality available in a variety of firewall designs to provide a robust layered approach in protecting an organization's information assets. Commonly used implementations available today include:

- **Screened-host firewall**—Utilizing a packet filtering router and a bastion host, this approach implements basic network layer security (packet filtering) and application server security (proxy services). An intruder in this configuration must penetrate two separate systems before the security of the private network can be compromised. This firewall system is configured with the bastion host connected to the private network with a packet filtering router between the Internet and the bastion host. Router filtering rules allow inbound traffic to access only the bastion host, which blocks access to internal systems. Since the inside hosts reside on the same network as the bastion host, the security policy of the organization determines whether inside systems are permitted direct access to the Internet, or whether they are required to use the proxy services on the bastion host.
- **Dual-homed firewall**—This is a firewall system that has two or more network interfaces, each of which is connected to a different network. A dual-homed firewall usually acts to block or filter some or all of the traffic trying to pass between the networks. A dual-homed firewall system is a more restrictive form of a screened-host firewall system in which a dual-homed bastion host is configured with one interface established for information servers and another for private network host computers.
- **Demilitarized zone (DMZ) or screened-subnet firewall**—This is a small, isolated network for an organization's public servers, bastion host information servers and modem pools. The DMZ connects the untrusted network to the trusted network, but it exists in its own independent space to limit access and availability of resources. As a result, external systems can access only the bastion host and possibly information servers in the DMZ. The inside router manages access to the private network, accepting only traffic originating from the bastion host. The filtering rules on the outside router require the use of proxy services by accepting only outbound traffic on the bastion host. The key benefits of this system are that an intruder must penetrate three separate devices, private network addresses are not disclosed to the Internet, and internal systems do not have direct access to the Internet.

FIREWALL ISSUES

Problems faced by organizations that have implemented firewalls include the following:

- **Configuration errors**—Misconfigured firewalls may allow unknown and dangerous services to pass through freely.
- **Monitoring demands**—It is necessary to apply and review log settings appropriately, but monitoring activities may not always occur on a regular basis.
- **Policy maintenance**—Firewall policies may not be maintained regularly.
- **Vulnerability to application- and input-based attacks**—Most firewalls operate at the network layer; therefore, they do not stop any application-based or input-based attacks, such as SQL injection and buffer-overflow attacks. Newer-generation firewalls are able to inspect traffic at the application layer and stop some of these attacks.

FIREWALL PLATFORMS

Firewalls may be implemented using hardware or software platforms. Implementing hardware will provide performance with minimal system overhead. Although hardware-based firewall platforms are faster, they are not as flexible or scalable as software-based firewalls. Software-based firewalls are generally slower with significant systems overhead. However, they are flexible with additional services; for example, they may include content and virus checking before traffic is passed to users.

It is generally better to use appliances, rather than normal servers, for the firewall. Appliances are normally installed with hardened operating systems. When server-based firewalls are used, operating systems in servers are often vulnerable to attacks. When attacks on operating systems succeed, the firewall can be compromised. In general, appliance-type firewalls are significantly faster to set up and recover.

NEXT GENERATION FIREWALLS^{16, 17, 18, 19}

Next Generation Firewalls (NGFWs) are the newest type of firewall to enter the marketplace aimed at addressing two key limitations of earlier variants: 1) the inability to inspect packet payload and 2) the inability to distinguish between types of web traffic.

An **NGFW** is an adaptive network security system capable of detecting and blocking sophisticated attacks.

NGFWs typically perform traditional functions such as packet filtering, stateful inspection and network address translation (NAT), but introduce application awareness, incorporate deep packet inspection (DPI) technology and offer varying degrees of integrated threat protection, such as data loss prevention (DLP), intrusion prevention system (IPS), SSL/SSH inspection and web filtering.

Application awareness is “the capacity of a system to maintain information about connected applications to optimize their operation and that of any subsystems that they run or control.”²⁰ This is important because discriminating between legitimate and malicious traffic has become increasingly difficult amid the upsurge in web-based services. The ability of an NGFW to differentiate between types of web traffic such as an authorized business web application and a streaming media site aids enforcement of corporate policies—regardless of port or protocol—and similarly offers insight to user activities and behavior.

DPI allows for payload interrogation against signatures for known exploits, malware, etc. DPI affords a great deal of information about your traffic, which aids in determination of normal traffic making anomaly detection more effective, especially in more complex networks.

Depending on your particular organization, you may be asked to review, recommend or specify vendor solutions. Bear in mind that while many next generation solutions advertise similar functions, how they do so is often decided by their interpretation of concepts and implementation of proprietary technology. As sophisticated as NGFWs may be today, it should not be your only line of defense.

¹⁶ Ohlhorst, Frank, “Next-Generation Firewalls 101,” Network Computing, 1 March 2013, www.networkcomputing.com/careers-and-certifications/next-generation-firewalls-101/a/d-id/1234097

¹⁷ Miller, Lawrence C.; *Next-Generation Firewalls for Dummies*, Wiley Publishing, Inc., USA, 2011 www.paloaltonetworks.com/content/dam/paloaltonetworks-com/en_US/assets/pdf/education/NGFW_dummies.pdf

¹⁸ Rouse, Margaret; *Next-generation firewall*, January 2014. <http://searchsecurity.techtarget.com/definition/next-generation-firewall-NGFW>

¹⁹ My Digital Shield; “Firewalls Don’t Cut It Anymore – Why You Need Next Generation Firewalls,” 28 August 2014, www.mydigitalshield.com/firewalls-dont-cut-anymore-need-next-generation-firewalls

²⁰ TechTarget, Wigmore, Ivy; *Application Awareness*, January 2013, <http://whatis.techtarget.com/definition/application-awareness>

TOPIC 5—ISOLATION AND SEGMENTATION

VLANS

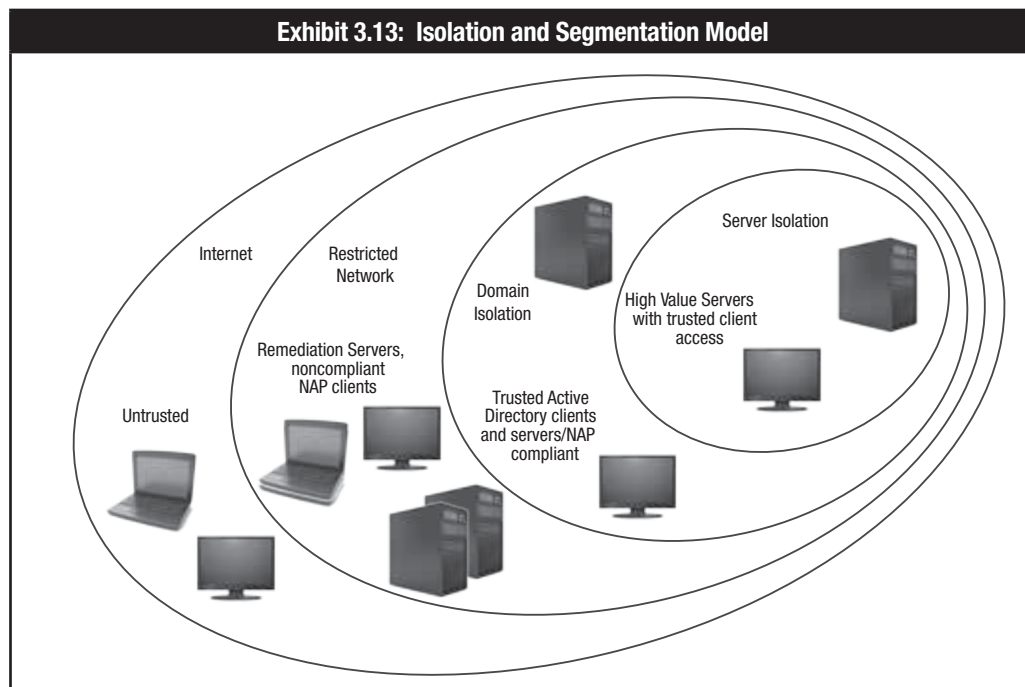
A common technique for implementing network security is to segment an organization's network so that each segment can be separately controlled, monitored and protected. **Virtual local area networks (VLANs)** are groups of devices on one or more logically segmented LAN.

A VLAN is set up by configuring ports on a switch, so devices attached to these ports may communicate as if they were attached to the same physical network segment, although the devices are actually located on different LAN segments. Segmenting network traffic in this way enables an organization to keep different types of data separate from one another.

A VLAN is based on logical rather than physical connections and, thus, it allows great flexibility. This flexibility enables administrators to segment network resources for optimal performance by restricting users' access of network resources to the necessary individuals only. In Layer 4 switching (transport layer), some application information is taken into account along with Layer 3 addresses. For IP, this information includes the port numbers from protocols such as UDP and TCP. These devices, unlike Layer 3 switches, are more resource intensive because they have to store application-based protocol information. Only address information is stored at the Layer 2 and Layer 3 levels.

SECURITY ZONES AND DMZS

By creating separate zones, controls can be applied at a more granular level based on the systems, information and applications in each area. Separate zones can create defense in depth where additional layers of authentication, access control and monitoring can take place. Isolation and segmentation is shown in **exhibit 3.13**.



Most organizations separate their internal systems from the Internet using a firewall. However, some systems and services, such as web servers, need to be available outside the internal network. This can be accomplished with a network segment called a **demilitarized zone (DMZ)**, which places limited systems, applications and data in a public-facing segment. Servers located in a DMZ minimize the exposure to attacks. Utilizing two packet filtering routers and a bastion host, this approach creates the most secure firewall system because it supports network- and application-level security while defining a separate DMZ network.

The DMZ functions as a small, isolated network for an organization's public servers, bastion host information servers and modem pools. Typically, DMZs are configured to limit access from the Internet and the organization's private network. Incoming traffic access is restricted into the DMZ network by the outside router, protecting the organization against certain attacks by limiting the services available for use. Consequently, external systems can access only the bastion host (along with its proxying service capabilities to internal systems) and possibly information servers in the DMZ. The inside router provides a second line of defense, managing DMZ access to the private network, while accepting only traffic originating from the bastion host. For outbound traffic, the inside router manages private network access to the DMZ network. It permits internal systems to access only the bastion host and information servers in the DMZ. The filtering rules on the outside router require the use of proxy services by accepting only outbound traffic on the bastion host. The key benefits of this system are:

- An intruder must penetrate three separate devices
- Private network addresses are not disclosed to the Internet
- Internal systems do not have direct access to the Internet

TOPIC 6—MONITORING, DETECTION AND LOGGING

Monitoring, detection and logging are integral parts of cybersecurity. With potential for attacks and data loss on both sides, it is necessary to monitor data and information flowing into and out of an organization. As this topic will illustrate, there are a number of methods and tools an organization can use to detect and log potential problems. Most of these methods revolve around the central concepts of ingress, egress, and data loss prevention.

INGRESS, EGRESS AND DATA LOSS PREVENTION (DLP)

Although often overlooked, there are two types of attack vectors: ingress and egress (also known as data exfiltration). **Ingress** refers to network communications coming in, while **egress** refers to network communications going out. While most attack analysis concentrates on the ingress or intrusion into systems, if the adversary's goal is theft of information or data, then it is important to consider the vector or path used to remove the data from the owner's systems and networks. Data loss prevention software is helpful in this regard. A successful data loss prevention program helps an organization protect its information and prevent the exfiltration of sensitive data.

Strong DLP solutions cover three primary states of information. **Data at rest** refers to stored data. DLP solutions must be able to log where various file types are stored. Crawler applications then explore the information on these files searching for sensitive data like social security or credit card information. These crawlers determine whether the storage location follows predefined rules.

Data in motion refers to data traveling through the network. Deep packet inspection (DPI) is used to analyze the data for sensitive content. DLP solutions can alert management and even block, quarantine or encrypt controlled information based on controls.

Finally, good DLP solutions manage **data in use**, which is data movement at the user workstation level. This includes sending information to printers, thumb drives or even the copy-and-paste clipboard. DLP solutions use agent software to set rules for data use. All three information types, data at rest, data in motion and data in use, must be addressed to create a full DLP solution.

ANTIVIRUS AND ANTI-MALWARE

Malicious software is one of the most common attack vectors used by adversaries to compromise systems. Therefore, controls are required for its detection and prevention.

Historically, anti-malware controls, often referred to as virus checkers, were host-based applications that scanned incoming traffic such as email and looked for patterns (signatures) that identified known problems. While this can be effective for known threats, it cannot detect malicious code that has yet to be identified.

Heuristic-based methods of detecting unknown malware use specific techniques to identify common malicious code behaviors and flag them as suspicious.

Anti-malware can be controlled through many different mechanisms, including:

- Restriction of outbound traffic to prevent malware from exfiltrating data or communicating with control systems used by the adversary
- Policies and awareness that train users to avoid opening suspect emails or attachments and to recognize
- URLs that may introduce malicious code
- Multiple layers of anti-malware software using a combination of signature identification and heuristic analysis to identify possible malicious code

INTRUSION DETECTION SYSTEMS²¹

Another element to securing networks complementing firewall implementation is an intrusion detection system (IDS). An IDS works in conjunction with routers and firewalls by monitoring network usage anomalies. It protects a company's IS resources from external as well as internal misuse. An IDS operates continuously on the system, running in the background and notifying administrators when it detects a perceived threat.

Broad categories of IDSs include:

- **Network-based IDSs**—These identify attacks within the monitored network and issue a warning to the operator. If a network-based IDS is placed between the Internet and the firewall, it will detect all the attack attempts, regardless of whether they enter the firewall. If the IDS is placed between a firewall and the corporate network, it will detect those attacks that enter the firewall (i.e., it will detect intruders). The IDS is not a substitute for a firewall, but rather it complements the function of a firewall.
- **Host-based IDSs**—These are configured for a specific environment and will monitor various internal resources of the operating system to warn of a possible attack. They can detect the modification of executable programs, detect the deletion of files and issue a warning when an attempt is made to use a privileged command.

Components of an IDS are:

- Sensors responsible for collecting data in the form of network packets, log files, system call traces, etc.
- Analyzers that receive input from sensors and determine intrusive activity
- An administration console
- A user interface

Types of IDSs include:

- **Signature-based**—These IDS systems protect against detected intrusion patterns. The intrusive patterns they can identify are stored in the form of signatures.
- **Statistical-based**—These systems need a comprehensive definition of the known and expected behavior of systems.
- **Neural networks**—An IDS with this feature monitors the general patterns of activity and traffic on the network and creates a database. It is similar to the statistical model but with added self-learning functionality.

Signature-based IDSs are not able to detect all types of intrusions due to the limitations of their detection rules. On the other hand, statistical-based systems may report many events outside of the defined normal activity that are still normal activities on the network. A combination of signature- and statistical-based models provides better protection.

IDS FEATURES

The features available in an IDS include:

- Intrusion detection
- Ability to gather evidence on intrusive activity
- Automated response (e.g., termination of connection, alarm messaging)
- Security policy
- Interface with system tools
- Security policy management

IDS LIMITATIONS

An IDS cannot help with the following weaknesses:

- Weaknesses in the policy definition (see Policy section)
- Application-level vulnerabilities
- Back doors into applications
- Weaknesses in identification and authentication schemes

²¹ ISACA, *CISA Review Manual 2014*, USA

In contrast to IDSs, which rely on signature files to identify an attack as (or after) it happens, an intrusion prevention system (IPS) predicts an attack before it occurs. It does this by monitoring key areas of a computer system and looking for “bad behavior,” such as worms, Trojans, spyware, malware and hackers. It complements firewall, antivirus and antispyware tools to provide complete protection from emerging threats. It is able to block new (zero-day) threats that bypass traditional security measures since it does not rely on identifying and distributing threat signatures or patches.

IDS POLICY

An IDS policy should establish the action to be taken by security personnel in the event that an intruder is detected.

Actions may include:

- **Terminate the access:** If there is a significant risk to the organization’s data or systems, immediate termination is the usual procedure.
- **Trace the access:** If the risk to the data is low, the activity is not immediately threatening, or analysis of the entry point and attack method is desirable, the IDS can be used to trace the origin of the intrusion. This can be used to determine and correct any system weaknesses and to collect evidence of the attack that may be used in a subsequent court action.

In either case, the action required should be determined by management in advance and incorporated into a policy. This will save time when an intrusion is detected, which may impact the possible data loss.

INTRUSION PREVENTION SYSTEMS

Intrusion prevention systems (IPSs) are closely related to IDSs; in fact, it is quite common for an IPS to be an extension of an IDS. In fact, an IDS and IPS can be directly integrated so that one product sends alert data to another. IPSs are designed to not only detect attacks, but also to prevent the intended victim hosts from being affected by the attacks. An IPS should prevent malicious programs from causing a system to delete all the files in a system directory. The intrusion prevention approach appears to be effective in limiting damage or disruption to systems that are attacked.

Some advantages of IPSs include:

- Protection at the application layer
- Prevention of attacks rather than simply reacting to them
- Defense in depth
- Real-time event correlation

However, as with an IDS, the IPS must be properly configured and tuned to be effective. Threshold settings that are too high or low will lead to limited effectiveness of the IPS. Additionally, some concerns have been raised that IPSs may in themselves constitute a threat, because a clever attacker could send commands to a large number of hosts protected by an IPS in order to cause them to become dysfunctional. Such a situation could have a potentially catastrophic outcome in today’s typical corporate computing environment where continuity of service is so critical. In addition, IPSs can generate false positives that can create serious problems if automated responses are used.

Page intentionally left blank

TOPIC 7A—ENCRYPTION FUNDAMENTALS

Encryption is the process of converting a plaintext message into a secure-coded form of text, called ciphertext. The ciphertext cannot be understood without converting back, via decryption—the reverse process—to plaintext. This is done via a mathematical function and a special encryption/decryption password called the key. In many countries, encryption is subject to governmental laws and regulations that limit the key size or define what may not be encrypted.

Encryption is part of a broader science of secret languages called cryptography, which is generally used to:

- Protect information stored on computers from unauthorized viewing and manipulation
- Protect data in transit over networks from unauthorized interception and manipulation
- Deter and detect accidental or intentional alterations of data
- Verify authenticity of a transaction or document

Encryption is limited in that it cannot prevent the loss of data. It is possible to compromise encryption programs if encryption keys are not protected adequately. Therefore, encryption should be regarded as an essential, but incomplete, form of access control that should be incorporated into an organization's overall computer security program.

KEY ELEMENTS OF CRYPTOGRAPHIC SYSTEMS

Key elements of cryptographic systems include:

- **Encryption algorithm**—Mathematically based function or calculation that encrypts or decrypts data.
- **Encryption key**—Piece of information similar to a password that makes the encryption or decryption process unique. A user needs the correct key to access or decipher a message, as the wrong key converts the message into an unreadable form.
- **Key length**—Predetermined length for the key. The longer the key, the more difficult it is to compromise in a brute force attack where all possible key combinations are tried.

Effective cryptographic systems depend upon a variety of factors including:

- Algorithm strength
- Secrecy and difficulty of compromising a key
- Nonexistence of back doors by which an encrypted file can be decrypted without knowing the key
- Inability to decrypt parts of a ciphertext message and prevent known plaintext attacks
- Properties of the plaintext known by a perpetrator

KEY SYSTEMS

There are two types of cryptographic systems:

- **Symmetric Key Systems**—These use single, secret, bidirectional keys that encrypt and decrypt.
- **Asymmetric Key Systems**—These use pairs of unidirectional, complementary keys that only encrypt or decrypt. Typically, one of these keys is secret, and the other is publicly known.

Public key systems are asymmetric cryptographic systems. Most encrypted transactions over the Internet use a combination of private/public keys, secret keys, hash functions (fixed values derived mathematically from a text message) and digital certificates (that prove ownership of a public encryption key) to achieve confidentiality, message integrity, authentication and nonrepudiation by either sender or recipient (also known as a public key infrastructure [PKI]). Essentially, keys and hash values are used to transform a string of characters into a shorter or fixed-length value or key that represents the original string. This encryption process allows data to be stored and transported with reduced exposure so data remains secure as it moves across the Internet or other networks.

Page intentionally left blank

TOPIC 7B—ENCRYPTION TECHNIQUES

SYMMETRIC (PRIVATE) KEY ENCRYPTION

Symmetric key cryptographic systems are based on a symmetric encryption algorithm, which uses a secret key to encrypt the plaintext to the ciphertext and the same key to decrypt the ciphertext to the corresponding plaintext. In this case, the key is said to be symmetric because the encryption key is the same as the decryption key.

The most common symmetric key cryptographic system is the Data Encryption Standard (DES). DES is based on a public algorithm that operates on plaintext in blocks (strings or groups) of bits. This type of algorithm is known as a block cipher. DES uses blocks of 64 bits.

DES is no longer considered a strong cryptographic solution because its entire key space can be forced when every key is tried by large computer systems within a relatively short period of time. In this regard, private key cryptographic spaces of symmetric keys are susceptible to compromise. DES is being replaced with AES, a public algorithm that supports keys from 128 bits to 256 bits.

There are two main advantages to symmetric key cryptosystems such as DES or AES:

- The user only has to remember/know one key for both encryption and decryption.
- Symmetric key cryptosystems are generally less complicated and, therefore, use up less processing power than asymmetric techniques. They are ideally suited for bulk data encryption.

The disadvantages of this approach include:

- Difficulty distributing keys—Getting the keys into the hands of those with whom you want to exchange data can be a challenge, particularly in e-commerce environments where customers are unknown, untrusted entities.
- Limitations of shared secret—A symmetric key cannot be used to sign electronic documents or messages due to the fact that the mechanism is based on a shared secret.

One form of advanced encryption algorithm is known as Triple DES or 3DES. Triple DES provides a relatively simple method of increasing the key size of DES to protect information without the need to design a completely new block cipher algorithm.

ASYMMETRIC (PRIVATE) KEY ENCRYPTION

Public key cryptographic systems developed for key distribution solve the problem of getting single symmetric keys into the hands of two people who do not know each other but who want to exchange information securely. Based on an asymmetric encryption process, two keys work together as a pair. One key is used to encrypt data; the other is used to decrypt data. Either key can be used to encrypt or decrypt, but once the key has been used to encrypt data, only its partner can be used to decrypt the data. The key that was used to encrypt the data cannot be used to decrypt it. Thus, the keys are asymmetric in that they are inversely related to each other.

Based on mathematical integer factorization, asymmetric keys generate a single product from two large prime numbers, making it impractical to factor the number and recover the two factors. This integer factorization process forms the basis for public key cryptography, a function that is easy to compute in one direction but very difficult or impractical in the other. The system involves modular arithmetic, exponentiation and large prime numbers thousands of bits long.

Asymmetric keys are often used for short messages such as encrypting DES symmetric keys or creating digital signatures. If asymmetric keys were used to encrypt bulk data (long messages), the process would be very slow; this is the reason they are used to encrypt short messages such as digests or signatures.

With asymmetric encryption, one key—the secret or private key—is known only to one person. The other key—the public key—is known by many people. In other words, a message that has been sent encrypted by the secret (private) key of the sender can be deciphered by anyone with the corresponding public key. In this way, if the public key deciphers the message satisfactorily, one can be sure of the origin of the message because only the sender (owner of the correspondent private key) could have encrypted the message. This forms the basis of authentication and nonrepudiation, as the sender cannot later claim that he or she did not generate the message.

A message that has been sent encrypted using the public key of the receiver can be generated by anyone, but can only be read by the receiver. This is one basis of confidentiality. In theory, a message that has been encrypted twice, first by the sender's secret key, and second by the receiver's public key, achieves both authentication and confidentiality objectives, but it is not commonly used because it could generate performance issues.

ELLIPTICAL CURVE CRYPTOGRAPHY

Although public key cryptography ensures message security, the long keys and mathematical problems it uses tend to be inefficient. A variant and more efficient form of public key cryptography is elliptical curve cryptography (ECC), which is gaining prominence as a method for increasing security while using minimum resources. It is believed that ECC demands less computational power and therefore offers more security per bit. For example, an ECC with a 160-bit key offers the same security as an RSA-based system with a 1,024-bit key.

ECC works well on networked computers requiring strong cryptography. However, it has some limitations such as bandwidth and processing power.

QUANTUM CRYPTOGRAPHY

Quantum cryptography is the next generation of cryptography that may solve some of the existing problems associated with current cryptographic systems, specifically the random generation and secure distribution of symmetric cryptographic keys. It is based on a practical application of the characteristics of the smallest "grains" of light (photons) and the physical laws governing their generation, propagation and detection. Initial commercial usage has already started now that the laboratory research phase has been completed.

ADVANCED ENCRYPTION STANDARD

AES has replaced the DES as the cryptographic algorithm standard. It originated in 1997, when NIST announced the initiation of the AES development effort and made a formal call for algorithms. In October 2000, NIST announced that it had selected Rijndael as the algorithm for the AES. This algorithm was developed by Dr. Joan Daemen and Dr. Vincent Rijmen.

Rijndael is a symmetric block cipher with variable block and key length. For AES the block length was fixed to 128 bits, and three different key sizes (128, 192 and 256 bits) were specified. Therefore, AES-128, AES-192 and AES-256 are three different versions of AES. The cipher is based on substitution bytes, shifting rows, mixing columns and adding round keys that are repeated for 10 rounds. Each round has a 128-bit round key and the result of the previous round as input. The round keys can be precomputed or generated out of the input key. Due to its regular structure, it can be implemented efficiently in hardware.

Decryption is computed by applying inverse functions of the round operations. The sequence of operations for the round function differs from encryption, which often results in separated encryption and decryption circuits. Computational performance of software implementations often differs between encryption and decryption because the inverse operations in the round function are more complex than the respective operation for encryption.

DIGITAL SIGNATURE

A **digital signature** is an electronic identification of a person or entity created by using a public key algorithm. It serves as a way for the recipient to verify the integrity of the data and the identity of the sender. To verify the integrity of the data, a cryptographic hashing algorithm, called a checksum, is computed against the entire message or electronic document, which generates a small fixed string message, usually about 128 bits in length. This process, also referred to as a digital signature algorithm, creates a message digest (i.e., smaller extrapolated version of the original message).

Common types of message digest algorithms are SHA1, SHA2, MD2, MD4 and MD5. These algorithms are one-way functions, unlike private and public key encryption algorithms. The process of creating message digests cannot be reversed. They are meant for digital signature applications where a large electronic document or string of characters, such as word processor text, a spreadsheet, a database record, the content of a hard disk or a JPEG image has to be compressed in a secure manner before being signed with the private key. All digest algorithms take a message of

arbitrary length and produce a 128-bit message digest. While the structures of these algorithms are somewhat similar, the design of MD2 is quite different from that of MD4 and MD5. MD2 was optimized for 8-bit machines, whereas MD4 and MD5 were created for 32-bit machines.

The next step, which verifies the identity of the sender, is to encrypt the message digest using the sender's private key, which "signs" the document with the sender's digital signature for message authenticity. To decipher, the receiver would use the sender's public key, proving that the message could only have come from the sender. This process of sender authentication is known as nonrepudiation because the sender cannot later claim that they did not generate the message.

Once decrypted, the receiver will recompute the hash using the same hashing algorithm on the electronic document and compare the results with what was sent, to ensure the integrity of the message. Therefore, digital signature is a cryptographic method that ensures:

- **Data integrity**—Any change to the plaintext message would result in the recipient failing to compute the same message hash.
- **Authentication**—The recipient can ensure that the message has been sent by the claimed sender since only the claimed sender has the secret key.
- **Nonrepudiation**—The claimed sender cannot later deny generating and sending the message.

Digital signatures and public key encryption are vulnerable to man-in-the-middle attacks wherein the sender's digital signature private key and public key may be faked. To protect against such attacks, an independent sender authentication authority has been designed. The PKI performs the function of independently authenticating the validity of senders' digital signatures and public keys.

VIRTUAL PRIVATE NETWORK

A VPN is an example of applied cryptography that typically exchanges secure data over the Internet. Encryption is needed to make the connection virtually private. A popular VPN technology is IPSec, which commonly uses the DES, Triple DES or AES encryption algorithms. DES uses 56-bit keys, and Triple DES applies the key three times to achieve an effective key length of 168 bits. AES is a new standard adopted in 2001 that uses keys that can be 128, 192 or 256 bits long and a block size of 128 bits (vs. 64-bit blocks used in DES).

WIRELESS NETWORK PROTECTIONS

Wireless data transmission is subject to a higher risk of interception than wired traffic, in the same way that it is easier to intercept calls made from cell phones than calls from landline telephones. There is no need to manually tap into the connection, but rather remote tools can be used to intercept the connection covertly. Wireless transmission of confidential information should be protected with strong encryption. An insecure wireless connection exposes users to eavesdropping, which can lead to the exposure of confidential information, intercepted messages or abused connections. Here are some examples:

- Email can be intercepted and read or changed.
- Hackers can replace a user's credential with false information that leads to the destination server rejecting the user's access attempts, thereby causing denial-of-service (DoS).
- An unauthorized person can log on to a wireless network that is not secure and use its resources, including free connectivity to the Internet.

Wireless security standards are evolving. The most commonly used method for wireless local area networks is Wired Equivalency Protocol (WEP). An increasing number of organizations and vendors are replacing this with 802.11i (WPA2) and Wi-Fi Protected Access (WPA), which uses dynamic keys and an authentication server with credentials to increase protection against hackers.

WEP and WPA comply with the evolving versions of the 802.11 wireless standard specified by the Institute of Electrical and Electronics Engineers (IEEE), with WPA being compatible with more advanced versions of 802.11, even WPA has shortcomings. The key is protected with a passphrase that does not have a rigorously enforced length. WPA is a subset of the developing 802.11i standard. The full standard will call for enhanced security by implementing AES.

WEP and WPA are applicable to most wireless networks and commonly used in networks that involve PCs. Messages transmitted using portable wireless devices should also be protected with encryption. For example, the Blackberry enterprise server model integrates the device with corporate email and uses Triple DES to encrypt information between the Blackberry unit and a corporate mail server.

Public keys are also used in mobile devices. ECC is widely used on smart cards and is increasingly deployed for cell phones. ECC is suited for small devices because the algorithm, by combining plane geometry with algebra, can achieve stronger authentication with smaller keys compared to traditional methods, such as RSA, which primarily use algebraic factoring. Smaller keys are more suitable to mobile devices; however, some would argue that ECC is not as rigorous as traditional public key algorithms because it has a shorter history than algorithms like RSA. With increasing computing power, the length of keys is becoming a less important issue for PC-based applications.

STORED DATA

Encryption is an effective and increasingly practical way to restrict access to confidential information while in storage. The traditional protection method—a password—has inherent weaknesses and, in many cases, is easily guessable. ACLs that define who has access are also effective, but they often have to be used in conjunction with operating systems or applications. Further, ACLs cannot prevent improper use of information by systems administrators, as the latter can have total control of a computer. Encryption can fill the security gap, and it can also protect data from hackers who, by means of malicious software, can obtain systems administration rights. Encryption also helps to protect data when a computer or a disk falls into the wrong hands. Many email encryption programs can also be applied to stored data. There are also some encryption products that focus on file protection for computers and PDAs.

PUBLIC KEY INFRASTRUCTURE

If an individual wants to send messages or electronic documents and sign them with a digital signature using a public key cryptographic system, how does the individual distribute the public key in a secure way? If the public key is distributed electronically, it could be intercepted and changed. To prevent this from occurring, a framework known as a public key infrastructure (PKI) is used. PKI allows a trusted party to issue, maintain and revoke public key certificates.

PKI allows users to interact with other users and applications to obtain and verify identities and keys from trusted sources. The actual implementation of PKI varies according to specific requirements. Key elements of the infrastructure are as follows:

- **Digital certificates**—A digital credential is composed of a public key and identifying information about the owner of the public key. The purpose of digital certificates is to associate a public key with the individual's identity in order to prove the sender's authenticity. These certificates are electronic documents, digitally signed by some trusted entity with its private key (transparent to users) that contains information about the individual and his or her public key. The process requires the sender to "sign" a document by attaching a digital certificate issued by a trusted entity. The receiver of the message and accompanying digital certificate relies on the public key of the trusted third-party certificate authority (CA) (that is included with the digital certificate or obtained separately) to authenticate the message. The receiver can link the message to a person, not simply to a public key, because of their trust in this third party. The status and values of a current user's certificate should include:
 - A distinguishing username
 - An actual public key
 - The algorithm used to compute the digital signature inside the certificate
 - A certificate validity period
- **Certificate authority**—A certificate authority (CA) is an authority in a network that issues and manages security credentials and public keys for message signature verification or encryption. The CA attests to the authenticity of the owner of a public key. The process involves a CA who makes a decision to issue a certificate based on evidence or knowledge obtained in verifying the identity of the recipient. As part of a PKI, a CA checks with a registration authority (RA) to verify information provided by the requestor of a digital certificate. If the RA verifies the requestor's information, the CA can then issue a certificate. Upon verifying the identity of the recipient, the CA signs the certificate with its private key for distribution to the user. Upon receipt, the user will verify the certificate signature with the CA's public key (e.g., commercial CAs such as VeriSign™ issue certificates through web browsers). The ideal CA is

authoritative (someone that the user trusts) for the name or key space it represents. A certificate always includes the owner's public key, expiration date and the owner's information. Types of CAs may include:

- Organizationally empowered, which have authoritative control over those individuals in their name space
- Liability empowered, for example, choosing commercially available options (such as VeriSign) in obtaining a digital certificate

The CA is responsible for managing the certificate throughout its life cycle. Key elements or subcomponents of the CA structure include the certification practice statement (CPS), RAs and certificate revocation lists (CRLs).

- **Registration authority**—An RA is an authority in a network that verifies user requests for a digital certificate and tells the CA to issue it. An optional entity separate from a CA, an RA would be used by a CA with a very large customer base. CAs use RAs to delegate some of the administrative functions associated with recording or verifying some or all of the information needed by a CA to issue certificates or CRLs and to perform other certificate management functions. However, with this arrangement, the CA still retains sole responsibility for signing either digital certificates or CRLs. RAs are part of a PKI. The digital certificate contains a public key that is used to encrypt messages and verify digital signatures. If an RA is not present in the PKI structure established, the CA is assumed to have the same set of capabilities as those defined for an RA. The administrative functions that a particular RA implements will vary based on the needs of the CA, but must support the principle of establishing or verifying the identity of the subscriber. These functions may include the following:
 - Verifying information supplied by the subject (personal authentication functions)
 - Verifying the right of the subject to requested certificate attributes
 - Verifying that the subject actually possesses the private key being registered and that it matches the public key requested for a certificate (generally referred to as proof of possession [POP])
 - Reporting key compromise or termination cases where revocation is required
 - Assigning names for identification purposes
 - Generating shared secrets for use during the initialization and certificate pick-up phases of registration
 - Initiating the registration process with the CA on behalf of the subject end entity
 - Initiating the key recovery processing
 - Distributing the physical tokens (such as smart cards) containing the private keys
- Certificate revocation list—The CRL is an instrument for checking the continued validity of the certificates for which the CA has responsibility. The CRL details digital certificates that are no longer valid because they were revoked by the CA. The time gap between two updates is critical and is also a risk in digital certificates verification.
- Certification practice statement—CPS is a detailed set of rules governing the CA's operations. It provides an understanding of the value and trustworthiness of certificates issued by a given CA in terms of the following:
 - The controls that an organization observes
 - The method it uses to validate the authenticity of certificate applicants
 - The CA's expectations of how its certificates may be used

Page intentionally left blank

TOPIC 7C—ENCRYPTION APPLICATIONS

APPLICATIONS OF CRYPTOGRAPHIC SYSTEMS

The use of cryptosystems by applications, for example in email and Internet transactions, generally involves a combination of private/public key pairs, secret keys, hash functions and digital certificates. The purpose of applying these combinations is to achieve confidentiality, message integrity or nonrepudiation by either the sender or recipient. The process generally involves the sender hashing the message into a message digest or pre-hash code for message integrity, which is encrypted using the sender's private key for authenticity, integrity and non-repudiation (i.e., digital signature).

Using his/her secret key, the sender then will encrypt the message. Afterward, the secret key is encrypted with the recipient's public key, which has been validated through the recipient's digital certificate and provides message confidentiality. The process on the receiving end reverses what has been done by the sender. The recipient uses his/her private key to decrypt the sender's secret key. He/she uses this secret key to decrypt the message, to expose it. If the pre-hash code has been encrypted with the sender's private key, the recipient verifies its authenticity using the public key contained in the sender's digital certificate and decrypts the pre-hash code, which provides the nonrepudiation to the recipient of the sender's message. For integrity purposes, the recipient calculates a post-hash code, which should equal the pre-hash code. Specific examples of this method or related variants are described below.

Secure Sockets Layer (SSL) and Transport Layer Security (TLS)—These are cryptographic protocols that provide secure communications on the Internet. There are only slight differences between SSL 3.0 (the latest version) and TLS 1.0, but they are not interchangeable. For general concepts, both are called SSL.

SSL is a session- or connection-layered protocol widely used on the Internet for communication between browsers and web servers, in which any amount of data is securely transmitted while a session is established. SSL provides end-point authentication and communications privacy over the Internet using cryptography. In typical use, only the server is authenticated while the client remains unauthenticated.

Mutual authentication requires PKI deployment to clients. The protocols allow client-server applications to communicate in a way designed to prevent eavesdropping, tampering and message forgery. SSL involves a number of basic phases:

- Peer negotiation for algorithm support
- Public key, encryption-based key exchange and certificate-based authentication
- Symmetric cipher-based traffic encryption

While SSL can add security to any protocol that uses TCP, it is most commonly used with HTTP to form Hypertext Transmission Protocol Secure (HTTPS). HTTPS serves to secure World Wide Web pages for applications such as electronic commerce.

HTTPS uses public key certificates to verify the identity of end points. SSL uses a hybrid of hashed, private and public key cryptographic processes to secure transactions over the Internet through PKI. This provides the necessary confidentiality, integrity, authenticity and nonrepudiation features needed for e-commerce transactions over the Internet. SSL can be characterized as a two-way SSL process, such as in B-to-B e-commerce activities. It also is commonly associated as a one-way consumer process, whereby a retail customer in an Internet retail virtual store can verify, through a CA, the authenticity of an e-store's public key, which can then be used to negotiate a secure transaction.

The SSL provides for:

- Confidentiality
- Integrity
- Authentication (e.g., between client and server)

The SSL handshake protocol is based on the application layer but also provides for the security of the communication sessions. It negotiates the security parameters for each communication section. Multiple connections can belong to one SSL session and the parties participating in one session can take part in multiple simultaneous sessions.

Secure Hypertext Transfer Protocol (S/HTTP)—As an application layer protocol, S/HTTP transmits individual messages or pages securely between a web client and server by establishing an SSL-type connection. Using the https://designation in the URL instead of the standard http://, S/HTTP directs the message to a secure port number rather than the default web port address. This protocol utilizes SSL secure features but does so as a message rather than as a session-oriented protocol.

IPSec—IPSec is used for communication among two or more hosts, two or more subnets, or hosts and subnets. This IP network layer packet security protocol establishes VPNs via transport and tunnel mode encryption methods. For the transport method, the data portion of each packet—referred to as the encapsulation security payload (ESP)—is encrypted to achieve confidentiality. In the tunnel mode, the ESP payload and its header are encrypted. To achieve nonrepudiation, an additional authentication header (AH) is applied.

In establishing IPSec sessions in either mode, security associations (SAs) are established. SAs define which security parameters should be applied between the communicating parties as encryption algorithms, keys, initialization vectors, life span of keys, etc.

To increase the security of IPSec, use asymmetric encryption via Internet Security Association and Key Management Protocol/Oakley (ISAKMP/Oakley), which allows the key management, use of public keys, negotiation, establishment, modification and deletion of SAs and attributes. For authentication, the sender uses digital certificates. The connection is made secure by supporting the generation, authentication and distribution of the SAs and cryptographic keys.

Secure Shell (SSH)—SSH is a client-server program that opens a secure, encrypted command-line shell session from the Internet for remote login. Similar to a VPN, SSH uses strong cryptography to protect data, including passwords, binary files and administrative commands, transmitted between systems on a network. SSH is typically implemented by validating both parties' credentials via digital certificates. SSH is useful in securing Telnet and FTP services. It is implemented at the application layer, as opposed to operating at the network layer (IPSec implementation).

Secure Multipurpose Internet Mail Extensions (S/MIME)—S/MIME is a standard secure email protocol that authenticates the identity of the sender and receiver, verifies message integrity, and ensures the privacy of a message's contents, including attachments.

Secure Electronic Transactions (SET)—SET is a protocol developed jointly by VISA and MasterCard to secure payment transactions among all parties involved in credit card transactions. As an open system specification, SET is an application-oriented protocol that uses trusted third parties' encryption and digital signature processes, via a PKI of trusted third-party institutions, to address confidentiality of information, integrity of data, cardholder authentication, merchant authentication and interoperability.

ENCRYPTION RISK AND KEY PROTECTION

The security of encryption methods relies mainly on the secrecy of keys. In general, the more a key is used, the more vulnerable it will be to compromise. For example, password cracking tools for today's microcomputers can brute force every possible key combination for a cryptographic hashing algorithm with a 40-bit key in a matter of a few hours.

The randomness of key generation is also a significant factor in the ability to compromise a key. When passwords are tied into key generation, the strength of the encryption algorithm is diminished, particularly when common words are used. This significantly reduces the key space combinations to search for the key. For example, an eight-character password is comparable to a 32-bit key. When encrypting keys based on passwords, a password that lacks randomness will diminish a 128-bit encryption algorithm's capabilities. Therefore, it is essential that effective password syntax rules are applied and easily guessed passwords are prohibited.

SECTION 3—KNOWLEDGE CHECK

1. Select all that apply. The Internet perimeter should:
 - a. Detect and block traffic from infected internal end points.
 - b. Eliminate threats such as email spam, viruses and worms.
 - c. Format, encrypt and compress data.
 - d. Control user traffic bound toward the Internet.
 - e. Monitor and detect network ports for rogue activity.
2. The _____ layer of the OSI model ensures that data are transferred reliably in the correct sequence, and the _____ layer coordinates and manages user connections.
 - a. Presentation, data link
 - b. Transport, session
 - c. Physical, application
 - d. Data link, network
3. Choose three. The key benefits of the DMZ system are:
 - a. DMZs are based on logical rather than physical connections.
 - b. An intruder must penetrate three separate devices.
 - c. Private network addresses are not disclosed to the Internet.
 - d. Excellent performance and scalability as Internet usage grows.
 - e. Internal systems do not have direct access to the Internet.
4. Which of the following best states the role of encryption within an overall cybersecurity program?
 - a. Encryption is the primary means of securing digital assets.
 - b. Encryption depends upon shared secrets and is therefore an unreliable means of control.
 - c. A program's encryption elements should be handled by a third-party cryptologist.
 - d. Encryption is an essential but incomplete form of access control.
5. The number and types of layers needed for defense in depth are a function of:
 - a. Asset value, criticality, reliability of each control and degree of exposure.
 - b. Threat agents, governance, compliance and mobile device policy.
 - c. Network configuration, navigation controls, user interface and VPN traffic.
 - d. Isolation, segmentation, internal controls and external controls.

Page intentionally left blank



Section 4:

Security of Networks, Systems, Applications and Data

Topics covered in this section include:

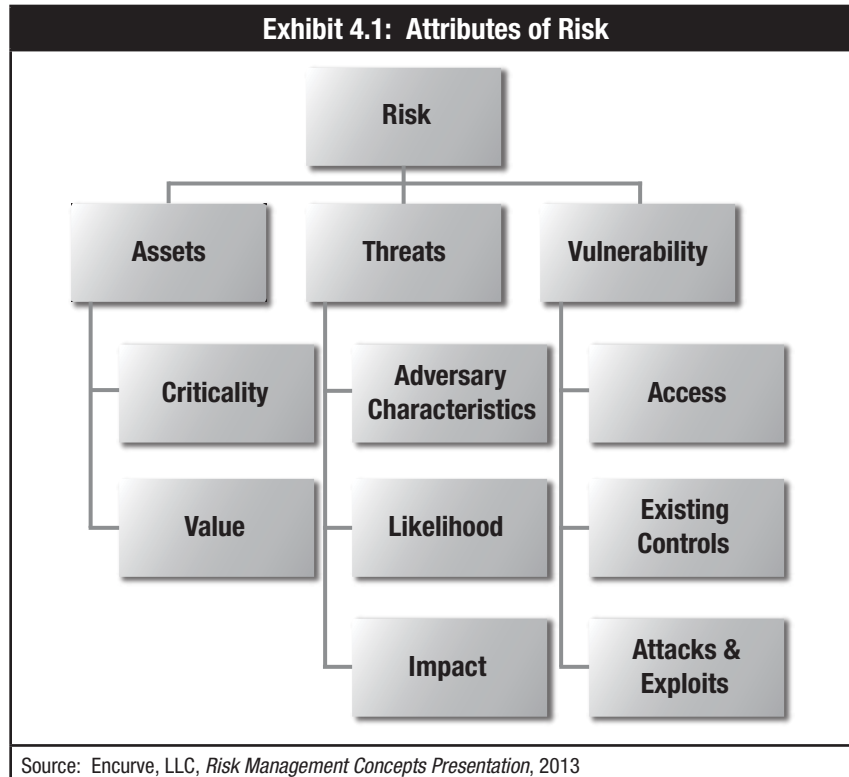
1. Risk analysis, risk assessments and risk mitigation strategies
2. Vulnerability scans, assessment and management
3. Penetration testing
4. Network management and configuration
5. Port numbers and protocols
6. Risk and controls for remote and wireless access
7. System hardening and virtualization
8. Specialized systems
9. Command line knowledge and tools
10. System development life cycle (SDLC)
11. Open Web Application Security Project (OWASP) top ten application security risk
12. Data classification process and requirements

Page intentionally left blank

TOPIC 1—PROCESS CONTROLS—RISK ASSESSMENTS

As previously mentioned, **risk** is defined as the possibility of loss of a digital **asset** resulting from a **threat** exploiting a **vulnerability**. Each of these attributes of risk must be analyzed to determine an organization's particular risk. The process of doing this analysis is called a **cyber risk assessment**.

While every risk assessment methodology has different nuances and approaches, most have three common inputs: **asset identification, threat assessment and vulnerability assessment**, as shown in **exhibit 4.1**.



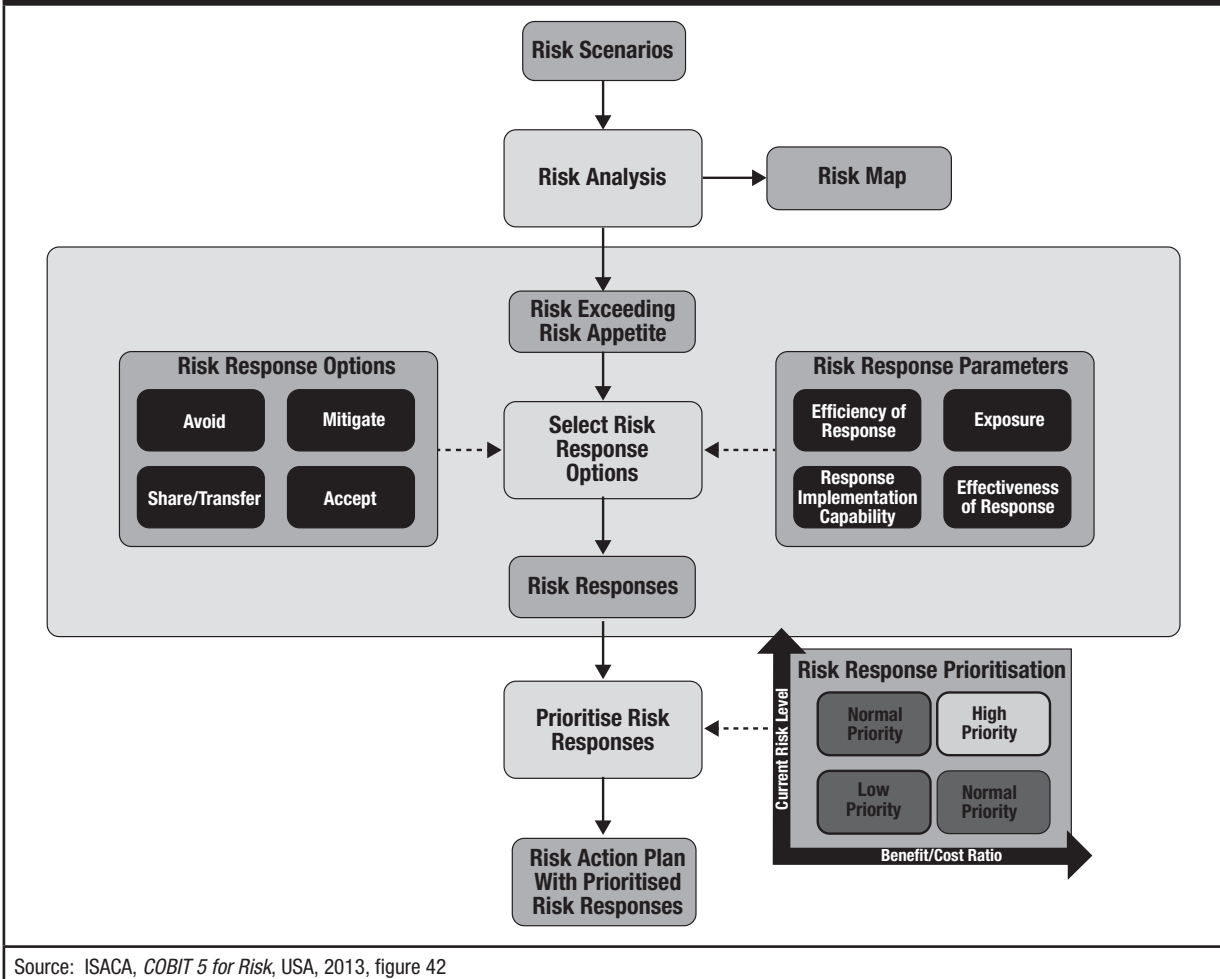
This process begins with an examination of the risk sources (threats and vulnerabilities) for their positive and negative consequences.

After evaluating each of these attributes, risk can be ranked according to likelihood and impact. Information used to estimate impact and likelihood usually comes from:

- Past experience or data and records (e.g., incident reporting)
- Reliable practices, international standards or guidelines
- Market research and analysis
- Experiments and prototypes
- Economic, engineering or other models
- Specialist and expert advice

Finally, existing controls and other mitigation strategies are evaluated to determine the level and effectiveness of risk mitigation currently in place and identify deficiencies and gaps that require attention. A risk response workflow is shown in **exhibit 4.2**.

Exhibit 4.2: Risk Response Workflow



Source: ISACA, COBIT 5 for Risk, USA, 2013, figure 42

It is critical for every cybersecurity practitioner to understand the basic concepts and nomenclature of the risk assessment process. If risk is not properly analyzed, the implementation of security is left to guesswork. In the following sections, common risk assessment processes will be covered in more detail.

RISK ANALYSIS

As stated previously, there are many methods used to bring the data collected on assets, threats and vulnerabilities together and analyze them to determine risk. Most rely on some process to pair and prioritize likelihoods and impacts. Additionally, risk analyses can be oriented toward one of the inputs, making the risk assessment asset-oriented, threat-oriented or vulnerability-oriented, as shown in **exhibit 4.3**.²²

Exhibit 4.3: Risk Assessment Orientations

Orientation	Description
Asset	Important assets are defined first, and then potential threats to those assets are analyzed. Vulnerabilities are identified that may be exploited to access the asset.
Threat	Potential threats are determined first, and then threat scenarios are developed. Based on the scenarios, vulnerabilities and assets of interest to the adversary are determined in relation to the threat.
Vulnerability	Vulnerabilities and deficiencies are identified first, then the exposed assets, and then the threat events that could be taken advantage of are determined.

²² National Institute of Standards and Technology (NIST), *Special Publication 800-30, Guide for Conducting Risk Assessments*, USA, September 2012

No one analysis orientation is better than the other; however, each has a bias that, if not considered, could weaken the analysis process resulting in some risk not being identified or properly prioritized. Some organizations will perform risk assessments from more than one orientation to compensate for the potential bias and generate a more thorough analysis.

EVALUATING SECURITY CONTROLS

Once risk is identified and prioritized, existing controls should be analyzed to determine their effectiveness in mitigating the risk. This analysis will result in a final risk ranking based on risk that has adequate controls, inadequate controls and no controls.

A very important criterion in control selection and evaluation is that the cost of the control (including its operation) should not exceed value of the asset it is protecting.

RISK ASSESSMENT SUCCESS CRITERIA

Choosing the exact method of analysis, including qualitative or quantitative approaches and determining the analysis orientation, takes considerable planning and knowledge of specific risk assessment methodologies. To be successful, the risk assessment process should fit the goals of the organization, adequately address the environment being assessed and use assessment methodologies that fit the data that can be collected.

The scope of the assessment must be clearly defined and understood by everyone involved in the risk assessment process. The process should be simple enough to be completed within the scope and time frame of the project yet rigorous enough to produce meaningful results.

It is important to understand the organization's unique risk appetite and cultural considerations when performing a risk assessment. Cultural aspects can have a significant impact on risk management. For example, financial institutions have more formal, regulated cultures where selection and implementation of stringent controls is acceptable, whereas a small entrepreneurial start-up may see some types of security controls as a hindrance to business.

Finally, risk assessment is not a one-off process. No organization is static; technology, business, regulatory and statutory requirements, people, vulnerabilities and threats are continuously evolving and changing. Therefore, successful risk assessment is an ongoing process to identify new risk and changes to the characteristics of existing and known risk.

MANAGING RISK

For risk that has inadequate or no controls, there are many options to address each risk, as shown in **exhibit 4.4**.

Exhibit 4.4: Risk Response Strategy	
Risk Mitigation	Description
Risk Reduction	The implementation of controls or countermeasures to reduce the likelihood or impact of a risk to a level within the organization's risk tolerance.
Risk Avoidance	Risk can be avoided by not participating in an activity or business.
Risk Transfer or Sharing	Risk can be transferred to a third party (e.g., insurance) or shared with a third party via contractual agreement.
Risk Acceptance	If the risk is within the organization's risk tolerance or if the cost of otherwise mitigating the risk is higher than the potential loss, then an organization can assume the risk and absorb any losses.

What strategy an organization chooses depends on many different things such as regulatory requirements, culture, mission, ability to mitigate risk and risk tolerance.

USING THE RESULTS OF THE RISK ASSESSMENT

The results of risk assessments are used for a variety of security management functions. These results need to be evaluated in terms of the organization's mission, risk tolerance, budgets and other resources, and cost of mitigation. Based on this evaluation, a mitigation strategy can be chosen for each risk and appropriate controls and countermeasures can be designed and implemented.

Risk assessment results can also be used to communicate the risk decisions and expectations of management throughout the organization through policies and procedures.

Finally, risk assessments can be used to identify areas where incident response capabilities need to be developed to quickly detect and respond to inherent or residual risk or where security controls cannot adequately address the threat.

TOPIC 2—PROCESS CONTROLS—VULNERABILITY MANAGEMENT

Vulnerabilities are continuously being discovered and organizations must be constantly vigilant in identifying them and quickly remediating.

Organizations need to identify and assess vulnerabilities to determine the threat and potential impact and to determine the best course of action in addressing each vulnerability. Vulnerabilities can be identified by information provided by software vendors (e.g., through the release of patches and updates) and by utilizing processes and tools that identify known vulnerabilities in the organization’s specific environment. The two most common techniques are vulnerability scanning and penetration testing.

VULNERABILITY MANAGEMENT

Vulnerability management starts by understanding the cybersecurity assets and where they reside—both physically and logically. This can be done by maintaining an asset inventory that details important information about each cyberasset such as location (physical or logical), criticality of the asset, the organizational owner of the asset and the type of information the asset stores or processes.

VULNERABILITY SCANS

Vulnerability scanning is the process of using proprietary or open source tools to search for known vulnerabilities. Often the same tools used by adversaries to identify vulnerabilities are used by organizations to locate vulnerabilities proactively.

Vulnerability assessment tools fall into two categories: host-based and network-based. Naming every tool is impractical because individual needs and budgets vary. Likewise, higher cost does not always equate to greater functionality, and tools can be found that are either free or free to try. Tools should be researched and selected based on corporate needs and return on investment, keeping in mind that combinations of tools often provide greater insight to your networks security posture.

Vulnerability scans should be conducted regularly to identify new vulnerabilities and ensure previously identified vulnerabilities have been properly corrected.

VULNERABILITY ASSESSMENT

The simplest definition of a **vulnerability** is “an exploitable weakness that results in a loss.” The method used to take advantage of a vulnerability is called an **exploit**. Vulnerabilities can occur in many different forms and at different architectural levels (for example, physical, operating system, application). **Exhibit 4.5** provides a list of common types of vulnerabilities.

Exhibit 4.5: Common Types of Vulnerabilities		
Type of Vulnerability	Cause	Cybersecurity Examples
Technical	Errors in design, implementation, placement or configuration	Coding errors Inadequate passwords Open network ports Lack of monitoring
Process	Errors in operation	Failure to monitor logs Failure to patch software
Organizational	Errors in management, decision, planning or from ignorance	Lack of policies Lack of awareness Failure to implement controls
Emergent	Interactions between, or changes in, environments	Cross-organizational failures Interoperability errors Implementing new technology

It is important to analyze vulnerabilities in the context of how they are exploited, and both vulnerabilities and exploits need to be considered in vulnerability assessments. Vulnerabilities and exploits can be identified in many ways. At a technical level, automated tools (both proprietary and open source) can be used to identify common vulnerabilities in computer and network implementations and configurations. Other vulnerability analysis tools include open source and proprietary sources such as SANS, MITRE and OWASP, software vendors, historical incidents, etc.

REMEDIATION

Once vulnerabilities are identified and assessed, appropriate remediation can take place to mitigate or eliminate the vulnerability. Most often, remediation will be through a patch management process but may also require reconfiguration of existing controls or addition of new controls.

REPORTING AND METRICS

Vulnerability management includes tracking vulnerabilities and the remediation efforts to mitigate them. This provides a clear opportunity to provide good qualitative metrics to the organization's management on the numbers and types of vulnerabilities, the potential impacts and the effort needed to mitigate them.

TOPIC 3—PROCESS CONTROLS—PENETRATION TESTING

Penetration testing includes identifying existing vulnerabilities and then using common exploit methods to:

- Confirm exposures
- Assess the level of effectiveness and quality of existing security controls
- Identify how specific vulnerabilities expose IT resources and assets
- Ensure compliance

Since penetration testing simulates actual attacks, it is important to plan these tests carefully. Failure to do so may result in ineffective results, negative impact on or damage to the organization's IT infrastructure or potential liability or criminal prosecution. Several considerations are important prior to any penetration testing:

- Clearly define the scope of the test including what systems or networks are within and out of scope, the type of exploits that may be used and the level of access allowed. These exploits can include network, social engineering, web, mobile application and other kinds of testing.
- Gather explicit, written permission from the organization authorizing the testing. This is the only accepted industry standard that distinguishes the service as authorized and legal.
- Ensure testers implement "Do no harm" procedures to ensure no assets are harmed, such as deletions, denial-of-service (DoS) or other negative impacts.
- Put in place communication and escalation plans for the organization and testers to communicate quickly during the tests.

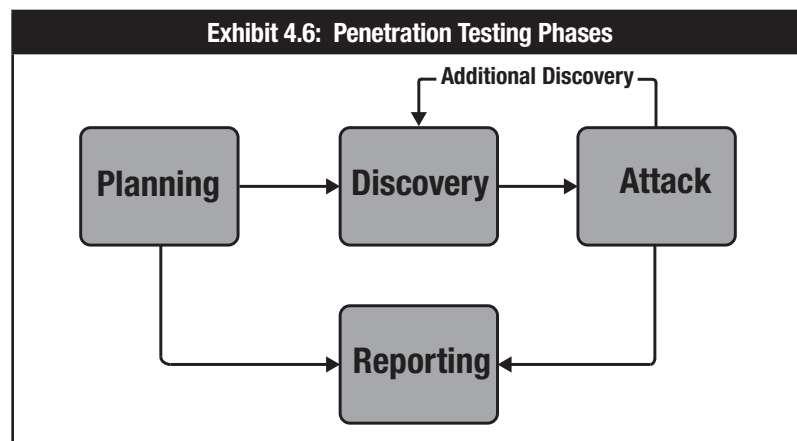
PENETRATION TESTERS

Penetration testing requires specialized knowledge of vulnerabilities, exploits, IT technology and the use of testing tools. It should not be performed by untrained or unqualified practitioners. Any penetration tests should be carefully planned to mitigate the risk of causing a service outage, and the results require careful interpretation and elimination of false positives.

Penetration testing can be covert (the general IT staff do not know the testing is going to take place) so that the reactions of the organization to detect and respond are also tested. Also, penetration testing can be external, from outside the organization, or internal, starting from a system behind the organization's firewall.²³

PENETRATION TESTING PHASES

Penetration testing can be divided into four main phases, as shown in **exhibit 4.6**.



²³ Encurve, LLC, *Attack and Penetration Delivery Guide*, 2014

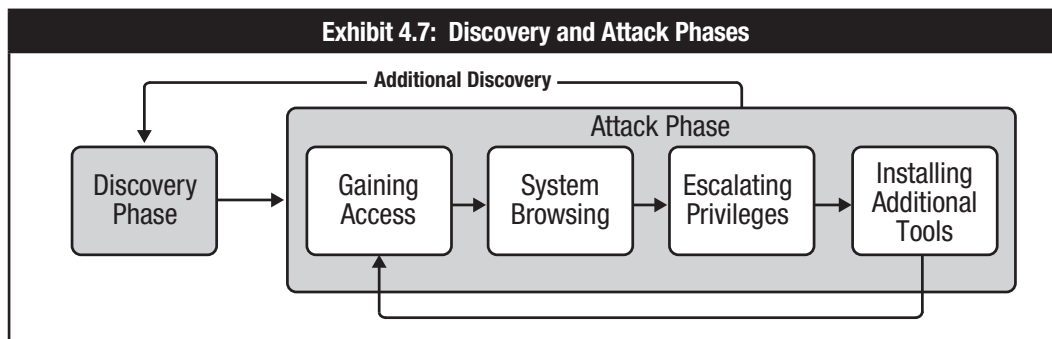
- 1. Planning:** In the planning phase, the goals are set, the scope is defined and the test is approved and documented by management. The scope determines if the penetration test is internal or external, limited to certain types of attacks or limited to certain networks or assets.
- 2. Discovery:** In the discovery phase, the penetration tester gathers information by conducting research on the organization and scans the networks for port and service identification. Techniques used to gather information include:
 - a. DNS interrogation, WHOIS queries and network sniffing to discover host name and IP address information
 - b. Search web servers and directory servers for employee names and contact information
 - c. Banner grabbing for application and service information
 - d. NetBIOS enumeration for system information
 - e. Dumpster diving and physical walk-throughs of the facilities to gather additional information
 - f. Social engineering, such as posing as a help desk agent and asking for passwords, posing as a user and calling the help desk to reset passwords or sending phishing emails

A vulnerability assessment is also conducted during the discovery phase. This involves comparing the services, applications and operating systems of the scanned host against vulnerability databases.

- 3. Attack:** The attack phase is the process of verifying previously identified vulnerabilities by attempting to exploit them. Metasploit® hosts a public database of quality-assured exploits. They rank exploits for safe testing.

Sometimes exploit attempts do not provide the tester with access, but they do give the tester additional information about the target and its potential vulnerabilities. If a tester is able to exploit a vulnerability, they can install more tools on the system or network to gain access to additional systems or resources.

A payload is the piece of software that lets a user control a computer system after it has been exploited. The payload is typically attached to and delivered by the exploit. Metasploit's most popular payload is called Meterpreter, which enables a user to upload and download files from the system, take screenshots and collect password hashes. The discovery and attack phases are illustrated in **exhibit 4.7**.



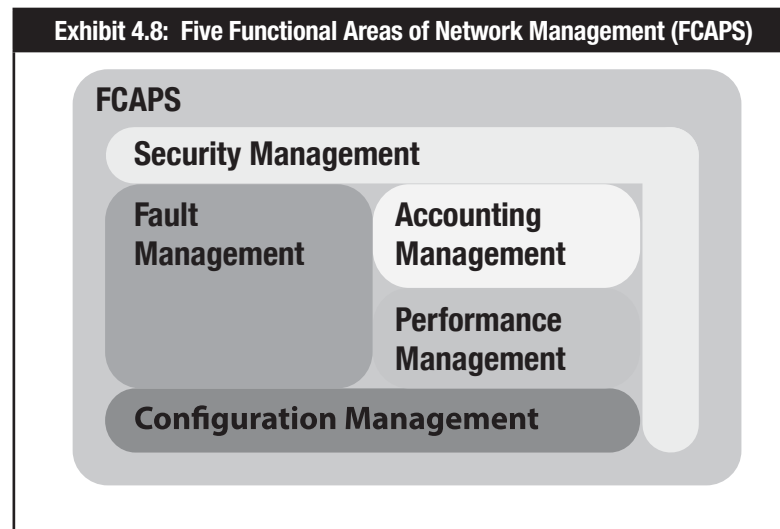
- 4. Reporting:** The reporting phase occurs simultaneously with the other phases. An assessment plan is developed during the planning phase. Logs are kept during the discovery and attack phases. And, at the conclusion of the penetration test, a report is developed to describe the vulnerabilities identified, assign risk ratings and provide mitigation plans.

TOPIC 4—NETWORK SECURITY

NETWORK MANAGEMENT

Network management is the process of assessing, monitoring, and maintaining network devices and connections. The International Organization for Standardization (ISO) network management model defines five functional areas of network management (FCAPS), listed below and shown in **exhibit 4.8**:

- **Fault Management**—Detect, isolate, notify and correct faults encountered in the network. This category analyzes traffic, trends, SMMP polls and alarms for automatic fault detection.
- **Configuration Management**—Configuration aspects of network devices include configuration file management, inventory management and software management.
- **Accounting Management**—Usage information of network resources.
- **Performance Management**—Monitor and measure various aspects of performance metrics so that acceptable performance can be maintained. This includes response time, link utilization and error rates. Administrators can monitor trends and set threshold alarms.
- **Security Management**—Provide access to network devices and corporate resources to authorized individuals. This category focuses on authentication, authorization, firewalls, network segmentation, IDS and notifications of attempted breaches.



LOCAL AREA NETWORK (LAN)²⁴

A LAN is a computer network covering a small local area. A few workstations and printers in a single room could comprise a LAN, as could three or four buildings in close proximity with thousands of devices connected together. The great increase in reasonably priced bandwidth has reduced the design effort required to provide cost-effective LAN solutions for organizations of any size.

New LANs are almost always implemented using switched Ethernet (802.3). Twisted-pair cabling (100-Base-T or better and, increasingly, wireless LANs) connects floor switches to the workstations and printers in the immediate area. Floor switches can be connected to each other with 1000-Base-T or fiber-optic cabling. In larger organizations, the floor switches may all be connected to larger, faster switches whose only purpose is to properly route the switch-to-switch data.

²⁴ ISACA, *CISA Review Manual 2015*, USA

LAN COMPONENTS²⁵

Components commonly associated with LANs are repeaters, hubs, bridges, switches and routers:

- **Repeaters**—Physical layer devices that extend the range of a network or connect two separate network segments together. Repeaters receive signals from one network segment and amplify (regenerate) the signal to compensate for signals (analog or digital) that are distorted due to a reduction of signal strength during transmission (i.e., attenuation).
- **Hubs**—Physical layer devices that serve as the center of a star-topology network or a network concentrator. Hubs can be active (if they repeat signals sent through them) or passive (if they merely split signals).
- **Bridges**—Data link layer devices developed in the early 1980s to connect LANs or create two separate LAN or WAN network segments from a single segment to reduce collision domains. The two segments work as different LANs below the data link level of the OSI reference model, but from that level and above, they behave as a single logical network. Bridges act as store-and-forward devices in moving frames toward their destination. This is achieved by analyzing the MAC header of a data packet, which represents the hardware address of an NIC. Bridges can also filter frames based on Layer 2 information. For example, they can prevent frames sent from predefined MAC addresses from entering a particular network. Bridges are software-based, and they are less efficient than other similar hardware-based devices such as switches. Therefore, bridges are not major components in today's enterprise network designs.
- **Layer 2 switches**—Layer 2 switches are data link level devices that can divide and interconnect network segments and help to reduce collision domains in Ethernet-based networks. Furthermore, switches store and forward frames, filtering and forwarding packets among network segments, based on Layer 2 MAC source and destination addresses, as bridges and hubs do at the data link layer. Switches, however, provide more robust functionality than bridges, through use of more sophisticated data link layer protocols which are implemented via specialized hardware called application-specific integrated circuits (ASICs). The benefits of this technology are performance efficiencies gained through reduced costs, low latency or idle time, and a greater number of ports on a switch with dedicated high-speed bandwidth capabilities. Switches are also applicable in WAN technology specifications.
- **Routers**—Similar to bridges and switches in that they link two or more physically separate network segments. The network segments linked by a router, however, remain logically separate and can function as independent networks. Routers operate at the OSI network layer by examining network addresses (i.e., routing information encoded in an IP packet). By examining the IP address, the router can make intelligent decisions to direct the packet to its destination. Routers differ from switches operating at the data link layer in that they use logically based network addresses, use different network addresses/segments off all ports, block broadcast information, block traffic to unknown addresses, and filter traffic based on network or host information. Routers are often not as efficient as switches since they are generally software-based devices and they examine every packet coming through, which can create significant bottlenecks within a network. Therefore, careful consideration should be taken as to where routers are placed within a network. This should include leveraging switches in network design as well as applying load balancing principles with other routers for performance efficiency considerations.
- **Layer 3 and 4 switches**—Advances in switch technology have also provided switches with operating capabilities at Layer 3 and Layer 4 of the OSI reference model.
 - A Layer 3 switch goes beyond Layer 2, acting at the network layer of the OSI model like a router. The Layer 3 switch looks at the incoming packet's networking protocol, e.g., IP. The switch compares the destination IP address to the list of addresses in its tables, to actively calculate the best way to send a packet to its destination. This creates a "virtual circuit"; i.e., the switch has the ability to segment the LAN within itself and will create a pathway between the receiving and the transmitting device to send the data. It then forwards the packet to the recipient's address. This provides the added benefit of reducing the size of network broadcast domains. Broadcast domains should be limited or aligned with business functional areas/workgroups within an organization, to reduce the risk of information leakage to those without a need to know, where systems can be targeted and their vulnerabilities exploited. The major difference between a router and a Layer 3 switch is that a router performs packet switching using a microprocessor, whereas a Layer 3 switch performs the switching using application ASIC hardware.
 - A Layer 4 switch allows for policy-based switching. With this functionality, Layer 4 switches can off-load a server by balancing traffic across a cluster of servers, based on individual session information and status.

²⁵ *Ibid.*

- **Layer 4-7 switches**—Also known as content-switches, content services switches, web-switches or application-switches. They are typically used for load balancing among groups of servers. Load balancing can be based on HTTP, HTTPS and/or VPN, or for any application TCP/IP traffic using a specific port. Content switches can also be used to perform standard operations such as SSL encryption/decryption to reduce the load on the servers receiving the traffic, and to centralize the management of digital certificates.
- **Gateways**—Devices that are protocol converters. Typically, they connect and convert between LANs and the mainframe, or between LANs and the Internet, at the application layer of the OSI reference model. Depending on the type of gateway, the operation occurs at various OSI layers. The most common form of gateway is a systems network architecture (SNA) gateway, converting between a TCP/IP, NetBios or Inter-network Packet Exchange (IPX) session (terminal emulator) and the mainframe.

WIDE AREA NETWORK (WAN)²⁶

A WAN is a data communications network that transmits information across geographically dispersed LANs such as among plant sites, cities and nations. WAN characteristics include:

- They are applicable to the physical and data link layers of the OSI reference model.
- Data flow can be simplex (one-way flow), half duplex (one way at a time) or full duplex (both ways at one time without turnaround delay).
- Communication lines can be either switched or dedicated

LAN/WAN SECURITY

LANs and WANs are particularly susceptible to people and virus-related threats because of the large number of people who have access rights.

The administrative and control functions available with network software might be limited. Software vendors and network users have recognized the need to provide diagnostic capabilities to identify the cause of problems when the network goes down or functions in an unusual manner. The use of logon IDs and passwords with associated administration facilities is only becoming standard now. Read, write and execute permission capabilities for files and programs are options available with some network operating system versions, but detailed automated logs of activity (audit trails) are seldom found on LANs. Fortunately, newer versions of network software have significantly more control and administration capabilities.

LANs can represent a form of decentralized computing. Decentralized local processing provides the potential for a more responsive computing environment; however, organizations do not always give the opportunity to efficiently develop staff to address the technical, operational and control issues that the complex LAN technology represents. As a result, local LAN administrators frequently lack the experience, expertise and time to effectively manage the computing environment.

LAN RISK AND ISSUES

LANs facilitate the storage and retrieval of programs and data used by a group of people. LAN software and practices also need to provide for the security of these programs and data. Unfortunately, most LAN software provides a low level of security. The emphasis has been on providing capability and functionality rather than security. As a result, risk associated with use of LANs includes:

- Loss of data and program integrity through unauthorized changes
- Lack of current data protection through inability to maintain version control
- Exposure to external activity through limited user verification and potential public network access from dial-in connections
- Virus and worm infection
- Improper disclosure of data because of general access rather than need-to-know access provisions
- Violation of software licenses by using unlicensed or excessive numbers of software copies
- Illegal access by impersonating or masquerading as a legitimate LAN user

²⁶ *Ibid.*

- Internal user's sniffing (obtaining seemingly unimportant information from the network that can be used to launch an attack such as network address information)
- Internal user's spoofing (reconfiguring a network address to pretend to be a different address)
- Destruction of the logging and auditing data

The LAN security provisions available depend on the software product, product version and implementation.

Commonly available network security administrative capabilities include:

- Declaring ownership of programs, files and storage.
- Limiting access to a read-only basis.
- Implementing record and file locking to prevent simultaneous update.
- Enforcing user ID/password sign-on procedures, including the rules relating to password length, format and change frequency.
- Using switches to implement port security policies rather than hubs or nonmanageable routers. This will prevent unauthorized hosts, with unknown MAC addresses, from connecting to the LAN.
- Encrypting local traffic using IPsec (IP security) protocol.

The use of these security procedures requires administrative time to implement and maintain. Network administration is often inadequate, providing global access because of the limited administrative support available when limited access is appropriate.

WIRELESS²⁷

Wireless technologies, in the simplest sense, enable one or more devices to communicate without physical connections, i.e., without requiring network or peripheral cabling. Wireless is a technology that enables organizations to adopt e-business solutions with tremendous growth potential. Wireless technologies use radio frequency transmissions/electromagnetic signals through free space as the means for transmitting data, whereas wired technologies use electrical signals through cables.

Wireless technologies range from complex systems (such as wireless wide area networks [WWANs], WLANs and cell phones) to simple devices (such as wireless headphones, microphones and other devices that do not process or store information). They also include Bluetooth® devices with a mini-radio frequency transceiver and infrared devices, such as remote controls, some cordless computer keyboards and mice, and wireless Hi-Fi stereo headsets, all of which require a direct line of sight between the transmitter and the receiver to close the link.

However, going wireless introduces new elements that must be addressed. For example, existing applications may need to be retrofitted to make use of wireless interfaces. Also, decisions need to be made regarding general connectivity—to facilitate the development of completely wireless mobile applications or other applications that rely on synchronization of data transfer between mobile computing systems and corporate infrastructure. Other issues include narrow bandwidth, the lack of a mature standard, and unresolved security and privacy issues.

Wireless networks serve as the transport mechanism between devices, and among devices and the traditional wired networks. Wireless networks are many and diverse, but are frequently categorized into four groups based on their coverage range:

- WANs
- LANs
- Wireless personal area networks (WPANs)
- Wireless ad hoc networks

²⁷ *Ibid.*

WIRELESS LOCAL AREA NETWORKS (WLAN)²⁸

WLANs allow greater flexibility and portability than traditional wired LANs. Unlike a traditional LAN, which requires a physical connection, a WLAN connects computers and other components to the network using an access point device. An access point, or wireless networking hub, communicates with devices equipped with wireless network adaptors within a specific range of the access point; it connects to a wired Ethernet LAN via an RJ-45 port. Access point devices typically have coverage areas (also referred to as cell or range) of up to 300 feet (approximately 100 meters). Users move freely within the cell with their laptop or other network devices. Cells can be linked together to allow users to “roam” within a building or between buildings. WLAN includes 802.11, HyperLAN, HomeRF and several others.

WLAN technologies conform to a variety of standards and offer varying levels of security features. The principal advantages of standards are to encourage mass production and to allow products from multiple vendors to interoperate. The most useful standard used currently is the IEEE 802.11 standard. 802.11 refers to a family of specifications for wireless LAN technology. 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients.

WIRED EQUIVALENT PRIVACY AND WI-FI PROTECTED ACCESS (WPA/WPA2)

IEEE 802.11’s Wired Equivalent Privacy (WEP) encryption uses symmetric, private keys, which means the end user’s radio-based NIC and access point must have the same key. This leads to periodic difficulties distributing new keys to each NIC. As a result, keys remain unchanged on networks for extended times. With static keys, several hacking tools easily break through the relatively weak WEP encryption mechanisms.

Because of the key reuse problem and other flaws, the current standardized version of WEP does not offer strong enough security for most corporate applications. Newer security protocols, such as 802.11i (WPA2) and Wi-Fi Protected Access (WPA), however, utilize public key cryptography techniques to provide effective authentication and encryption between users and access points.

PORTS AND PROTOCOLS²⁹

A port is a logical connection. When using the Internet communications protocol, Transmission Control Protocol/Internet Protocol (TCP/IP), designating a port is the way a client program specifies a particular server program on a computer in a network. Basically, a port number is a way to identify the specific process to which an Internet or other network message is to be forwarded when it arrives at a server. For TCP, User Datagram Protocol (UDP) and Internet Control Message Protocol (ICMP), a port number is a 16-bit integer that is put in the header attached to a unit of information (a message unit). This port number is passed logically between client and server transport layers and physically between the transport layer and the Internet protocol layer and then forwarded.

Higher-level applications that use TCP/IP such as the web protocol and hypertext transfer protocol (HTTP) use ports with preassigned numbers. These are well-known ports, to which numbers have been assigned by the Internet Assigned Numbers Authority (IANA). Some application processes are given port numbers dynamically when each connection is made.

PORT NUMBERS

Allowable port numbers range from 0 to 65535. Ports 0 to 1023 are reserved for certain privileged services—the well-known ports. For example, for the HTTP service, port 80 is defined as the default. Because it is preassigned, port 80 and some other ports do not have to be specified in the uniform resource locator (URL). That lets the user simply type in an Internet address or URL, such as www.isaca.org, without specifying the port number at the end of the URL; www.isaca.org:80, in this case. Either format will work in the browser.

²⁸ *Ibid.*

²⁹ Moody, R. “Ports and Port Scanning: An Introduction,” *ISACA Journal*, Volume 4, 2001, <http://isaca.org/Journal/Past-Issues/2001/Volume-5/Pages/Ports-and-Port-Scanning-An-Introduction.aspx>

PROTOCOL NUMBERS AND ASSIGNMENT SERVICES

Port numbers are divided into three ranges: the well-known ports, the registered ports and the dynamic and/or private ports. IANA records list all well-known and registered port numbers:

- **The well-known ports**—0 through 1023: Controlled and assigned by the IANA and, on most systems, can be used only by system (or root) processes or by programs executed by privileged users. The assigned ports use the first portion of the possible port numbers. Initially, these assigned ports were in the range 0-255. Currently, the range for assigned ports managed by the IANA has been expanded to the range 0-1023.
- **The registered ports**—1024 through 49151: Listed by the IANA and, on most systems, can be used by ordinary user processes or programs executed by ordinary users.
- **The dynamic and/or private ports**—49152 through 65535: Not listed by IANA because of their dynamic nature.

When a server program is started via a port connection, it is said to bind to its designated port number. When another client program wants to use that server, it also must send a request to bind to the designated port number. Ports are used in TCP to name the ends of logical connections that carry long-term conversations. To the extent possible, these same port assignments are used with UDP.

For example, a request for a file is sent through the browser software to a server accessible from the Internet. The request might be served from that host's file transfer protocol (FTP) application residing on a particular internal server. To pass the request to the FTP process residing on that remote server, the TCP software layer in the computer (the browser) specifies port number 21, which is the IANA assigned port for an FTP request, in the 16-bit port number integer that is appended to the request as part of header information. At the remote server, the TCP layer will read the port number (21) and forward the request to the FTP program on the server. Common services are implemented on the same port across different platforms. For example, the service generally runs on port 80 whether using UNIX or Windows operating system. These transport layer mechanisms along with the IP addresses for a connection (sender and receiver) uniquely identify a connection.

In a basic Internet type of computer configuration using multiple computers, a site server is installed behind a firewall and its databases are installed on a second computer behind a second firewall. Other configurations are possible, of course. In some cases, there is a corporate intranet with internal users and a database server behind a firewall, a site server, another firewall and external users (it is also useful to have external site server tools access). Each firewall would allow access to ports set open by the site server software. With many server software applications, a number of ports are set by default, for example, HTTP-80, HTTPS-443 (the standard secure web server port number), SMTP-25 and others. Commonly exploited ports and services are listed in **exhibit 4.9**.

Exhibit 4.9: Commonly Exploited Ports and Services

Port #	Service	Protocol	Port #	Service	Protocol
7	Echo	TCP/UDP	110	POP3 (post office protocol)	TCP
19	chargen	TCP	111/2049	SunRPC (remote procedure calls)	TCP/UDP
20-21	FTP (file transfer protocol)	TCP	135-139	NBT (NetBIOS over TCP/ IP)	TCP/UDP
23	Telnet (remote login)	TCP	161, 162	SNMP (Simple Network Management Protocol)	UDP
25	SMTP (simple mail transfer)	TCP	512	Exec	UDP
43	Whois	TCP/UDP	513	Login	TCP
53	DNS (domain name system)	TCP	514	Shell	TCP/UDP
69	TFTP (trivial file transfer)	6000-xxxx		protocol)	UDP
xxxx	X-Windows	TCP			
79	Finger	TCP	8000	HTTP	TCP/UDP
80	HTTP-low	TCP	8080	HTTP	TCP/UDP
107	Rtelnnet	TCP/UDP	31337	Back Orifice	UDP

VIRTUAL PRIVATE NETWORKS

When designing a VPN, it is important to ensure that the VPN can carry all types of data in a secure and private manner over any type of connection. Tunneling is the process of encapsulating one type of protocol in another. It transports higher-layer data over a VPN by Layer 2 protocols. One end of the tunnel is the client, and the other end is a connectivity device or a remote access server. Two common types of tunneling include:

- Point-to-point tunneling protocol (PPTP)—A Layer 2 protocol developed by Microsoft that encapsulates point-to-point protocol data. It is simple, but less secure than other tunneling protocols.
- Layer 2 tunneling protocol (L2TP)—A protocol that encapsulates point-to-point protocol data and is compatible among different manufacturers' equipment. The end points do not have to reside on the same packet-switched network and can remain isolated from other traffic.

VOICE-OVER INTERNET PROTOCOL (VOIP)³⁰

Users often expect that all voice communications are confidential. Any VoIP device is an IP device; therefore, it is vulnerable to the same types of attacks as any other IP device. A hacker or virus could potentially bring down the data and voice networks simultaneously in a single attack. Also, VoIP networks are still vulnerable to sniffing, DoS, traffic-flow disruption and toll fraud. Sniffing would allow the disclosure of sensitive information, such as user information, resulting in identity theft, which may be used to attack other data subsystems. Port scanning is often a precursor to a potential sniffing of the VoIP network. The ability to network sniff is becoming easier as many tools are readily available from open source web sites as opposed to highly expensive specialty diagnostic equipment used for time division multiplexing (TDM).

DoS, or the flooding of the data network with data, is a common issue in the protection of data networks but needs to be revisited as quality of service (QoS) becomes implemented for VoIP networks. The IP end point is often overlooked, but it can be singled out as a point of attack and flooded with data, causing the device to reboot and eventually become unusable.

Traffic flow disruption allows further exploitation of the previous two vulnerabilities, whereas the redirecting of packets facilitates the determination of packet routes, increasing the likelihood of sniffing.

Voice packets travel “in the clear” over IP networks, so they may be vulnerable to unauthorized sniffing. Unless network-based encryption is used, all voice RTP packets travel in the clear over the network and could be captured or copied by any network-monitoring device.

VoIP networks have a number of characteristics that make for special security requirements. There is no such thing as scheduled downtime in telephony. Outages may result in massive, widespread customer panic or outrage. There could also be disclosure of confidential information, which, like the loss of other kinds of data, could adversely affect the organization. Many security teams spend most of their time preventing outside attackers from penetrating a corporate firewall or Internet-accessible bastion servers. However, many companies spend little or no effort protecting the internal network infrastructure or servers from inside attacks. In the context of voice communications, a prime example is an employee listening to another employee's personal or company-confidential phone calls.

REMOTE ACCESS³¹

Today's organizations require remote access connectivity to their information resources for different types of users, such as employees, vendors, consultants, business partners and customer representatives. Remote access users can connect to their organization's networks with the same level of functionality that exists within their office. In doing so, the remote access design uses the same network standards and protocols applicable to the systems that they are accessing.

³⁰ Khan, K., “Introduction to Voice-over IP Technology”, *ISACA Journal*, Volume 2, 2005, www.isaca.org/Journal/Past-Issues/2005/Volume-2/Pages/Introduction-to-Voice-over-IP-Technology1.aspx

³¹ ISACA, *CISA Review Manual 2014*, USA

A viable option gaining increased use is TCP/IP Internet-based remote access. This access method is a cost-effective approach that enables organizations to take advantage of the public network infrastructures and connectivity options available, under which ISPs manage modems and dial-in servers, and DSL and cable modems reduce costs further to an organization. To effectively use this option, organizations establish a virtual private network over the Internet to securely communicate data packets over this public infrastructure.

Available VPN technologies apply the Internet Engineering Task Force (IETF) IPSec security standard. Advantages are their ubiquity, ease of use, inexpensive connectivity, and read, inquiry or copy only access. Disadvantages include that they are significantly less reliable than dedicated circuits, lack a central authority, and can be difficult to troubleshoot.

Organizations should be aware that using VPNs to allow remote access to their systems can create holes in their security infrastructure. The encrypted traffic can hide unauthorized actions or malicious software that can be transmitted through such channels. Intrusion detection systems (IDSs) and virus scanners able to decrypt the traffic for analysis and then encrypt and forward it to the VPN end point should be considered as preventive controls. A good practice will terminate all VPNs to the same end point in a so called VPN concentrator, and will not accept VPNs directed at other parts of the network.

Remote access risk includes:

- DoS, where remote users may not be able to gain access to data or applications that are vital for them to carry out their day-to-day business
- Malicious third parties, who may gain access to critical applications or sensitive data by exploiting weaknesses in communications software and network protocols
- Misconfigured communications software, which may result in unauthorized access or modification of an organization's information resources
- Misconfigured devices on the corporate computing infrastructure
- Host systems not secured appropriately, which could be exploited by an intruder gaining access remotely
- Physical security issues over remote users' computers

Remote access controls include:

- Policies and standards
- Proper authorizations
- Identification and authentication mechanisms
- Encryption tools and techniques such as use of a VPN
- System and network management

TOPIC 5—OPERATING SYSTEM SECURITY

SYSTEM/PLATFORM HARDENING

System hardening is the process of implementing security controls on a computer system. It is common for most computer vendors to set the default controls to be open, allowing ease of use over security. This creates significant vulnerabilities unless the system is hardened.

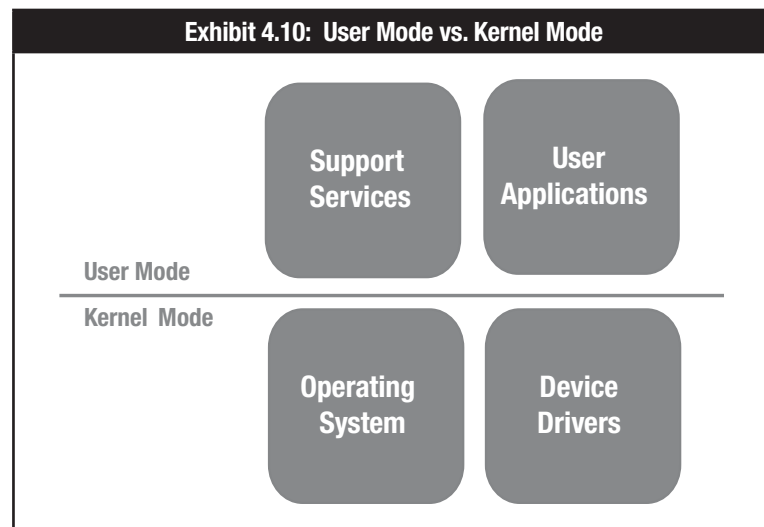
The actual process of determining what is hardened and to what level varies based on the risk and exposure of the system. Also, the exact controls available for hardening vary from operating system to operating system; however, some common controls include:

- Authentication and authorization
- File system permissions
- Access privileges
- Logging and system monitoring
- System services

Regardless of the specific operating system, system hardening should implement the principle of least privilege or access control.

MODES OF OPERATIONS

Most operating systems have two modes of operations—**kernel mode** for execution of privileged instructions for the internal operation of the system and **user mode** for normal activities. In kernel mode, there are no protections from errors or malicious activity and all parts of the system and memory are accessible. See **exhibit 4.10**.



Operating systems allow controlled access to kernel mode operations through system calls that usually require privileges. These privileges are defined on a user or program basis and should be limited under the principle of least privilege.

Most attacks seek to gain privileged or kernel mode access to the system in order to circumvent other security controls.

FILE SYSTEM PERMISSIONS

Operating systems have file systems that manage data files stored within the system and provide access controls to determine which users (or programs) have what type of access to a file. Common file accesses include creation, modification, read, write and deletion controls.

CREDENTIALS AND PRIVILEGES

The access any particular user has to a system is controlled through a series of mechanisms. A user's credentials define who they are and what permissions they have to access resources within the system.

Passwords are the standard mechanism to authenticate a user to the system and must be managed correctly to ensure they are not easily guessed or compromised. Most operating systems provide controls around passwords such as minimum length, lifetime for any particular password and how many attempts to use a password are allowed before denying access.

Another key user control is the privileges assigned to a particular user. These privileges must be carefully chosen and controlled to prevent misuse or compromise. Assignment of privileges should follow the principle of least privilege required for a user to do their job.

Administrators can also limit the ways in which users can access systems. For example, administrators can set logon constraints based on the time of day, the total time logged on, the source address and unsuccessful logon attempts.

PLATFORM HARDENING

Security practitioners must understand the types and roles of accounts on each platform they are protecting. For example, Windows differentiates between files and devices such as printers, whereas everything in UNIX is considered to be a file to include physical devices.

For the cybersecurity practitioner, identifying the location of critical information is imperative not only to security, but also incident response.

In UNIX, the following directories require additional consideration:

- /etc/passwd—Maintains user account and password information
- /etc/shadow—Retains the encrypted password of the corresponding account
- /etc/group—Contains group information for each account
- /etc/gshadow—Contains secure group account information
- /bin—Location of executable files
- /boot—Contains files for booting system
- /kernel—Kernel files
- /sbin—Contains executables, often for administration
- /usr—Include administrative commands

For Windows, you need not look any further than the Registry—a central hierarchical database that stores configuration settings and options.³² A hive is a logical group of keys, subkeys and values in the registry that has a set of supporting files and backups of its data.³³

- HKEY_CURRENT_CONFIG—Contains volatile information generated at boot
- HKEY_CURRENT_USER—Settings specific to current user
- HKEY_LOCAL_MACHINE\SAM—Holds local and domain account information
- HKEY_LOCAL_MACHINE\Security—Contains security policy referenced and enforced by kernel
- HKEY_LOCAL_MACHINE\Software—Contains software and Windows settings
- HKEY_LOCAL_MACHINE\System—Contains information about Windows system setup
- HKEY_USERS\DEFAULT—Profile for Local System account

Most of the supporting files for the hives are in the %SystemRoot%\System32\Config directory. These files are updated each time a user logs on.³⁴

³² Microsoft Press; *Microsoft Computer Dictionary*, 5th edition, USA, 2002

³³ Microsoft; Registry Hives, <http://msdn.microsoft.com/en-us/library/windows/desktop/ms724877%28v=vs.85%29.aspx>

³⁴ *Ibid.*

COMMAND LINE KNOWLEDGE

Cybersecurity professionals often use command line tools as part of their security routine. The following list provides ten popular command line tools for cybersecurity:

- Nmap—Network port scanner and service detector
- Metasploit—Penetration testing software
- Aircrack-ng—802.11 WEP and WPA-PSK keys cracking program
- Snort®—Open source IDS/IPS
- Netstat—Displays detailed network status information
- Netcat—Networking utility that reads and writes data across network connections, using the TCP/IP protocol
- Tcpdump—Command line packet analyzer
- John the Ripper—password cracker
- Kismet—02.11 layer 2 wireless network detector, sniffer and IDS
- OpenSSH/PuTTY/SSH—program for logging into or executing commands on a remote machine.

Useful UNIX commands for the cybersecurity practitioner are listed in **exhibit 4.11**.

Exhibit 4.11: UNIX Commands	
Command	Description
finger {userid}	Display information about a user
cat	Display or concatenate file
cd	Change directory
chmod	Change file permissions Note: UNIX permissions are managed using octal notation by user, group, and others. Manipulating permissions is above the purpose of this material but are critical as you further your cybersecurity career.
cp	Copy
date	Display current date and time
diff	Display differences between text files
grep	Find string in file
ls	Directory list. Useful switches: -a Display all files * -d Display only directories -l Display long listing -u Display files by access (newest first) -U Display results by creation (newest first) Note: Unlike Windows, UNIX does not afford the opportunity to “turn on” hidden files. Referred to as dot files, these file names begin with a “.”, hence the name. To view these protected system files you must use the -a switch. [ls -a or ls -al]
man	Displays help
mkdir	Make directory
mv	Move/rename file
ps	Display active processes
pwd	Displays the current directory
rm	Delete file
rmdir	Delete directory
sort	Sort data
whoami	Tells you who you are logged in as

LOGGING AND SYSTEM MONITORING

Logging provides the basic data required to monitor and detect unauthorized activity and to analyze potential security breaches. A variety of tools can be used with IPS and security incident and event management (SIEM) to enable the monitoring of anomalies and potential threats. Most operating systems have a wide range of events and transactions that can be recorded and stored for troubleshooting, performance and security monitoring. Examples of common security events include authentication failures (incorrect passwords) and logging of accesses to critical system files.

Determining exactly what and how much to log takes careful consideration. Logging too much activity can make analysis difficult, as well as waste resources such as the disk space to store the activity. Logging too little will not provide adequate information to detect attacks.

VIRTUALIZATION

Virtualization provides an enterprise with a significant opportunity to increase efficiency and decrease costs in its IT operations.

At a high level, virtualization allows multiple OSs (guests), to coexist on the same physical server (host), in isolation of one another. Virtualization creates a layer between the hardware and the guest OSs to manage shared processing and memory resources on the host. Often, a management console provides administrative access to manage the virtualized system. There are advantages and disadvantages, as shown in **exhibit 4.12**.

Exhibit 4.12: Advantages and Disadvantages of Virtualization ³⁵	
Advantages	Disadvantages
<ul style="list-style-type: none"> • Server hardware costs may decrease for both server builds and server maintenance. • Multiple OSs can share processing capacity and storage space that often goes to waste in traditional servers, thereby reducing operating costs. • The physical footprint of servers may decrease within the data center. • A single host can have multiple versions of the same OS, or even different OSs, to facilitate testing of applications for performance differences. • Creation of duplicate copies of guests in alternate locations can support business continuity efforts. • Application support personnel can have multiple versions of the same OS, or even different OSs, on a single host to more easily support users operating in different environments. • A single machine can house a multitier network in an educational lab environment without costly reconfigurations of physical equipment. • Smaller organizations that had performed tests in the production environment may be better able to set up logically separate, cost-effective development and test environments. • If set up correctly, a well-built, single access control on the host can provide tighter control for the host's multiple guests. 	<ul style="list-style-type: none"> • Inadequate configuration of the host could create vulnerabilities that affect not only the host, but also the guests. • Exploits of vulnerabilities within the host's configuration, or a DoS attack against the host, could affect all of the host's guests. • A compromise of the management console could grant unapproved administrative access to the host's guests. • Performance issues of the host's own OS could impact each of the host's guests. • Data could leak between guests if memory is not released and allocated by the host in a controlled manner. • Insecure protocols for remote access to the management console and guests could result in exposure of administrative credentials.
Source: ISACA, <i>CISA Review Manual 2015</i> , USA, exhibit 5.10	

Although virtualization offers significant advantages, they come with risk that an enterprise must manage effectively. Because the host in a virtualized environment represents a potential single point of failure within the system, a successful attack on the host could result in a compromise that is larger in both scope and impact.

³⁵ ISACA, *CISA Review Manual 2014*, USA

To address this risk, an enterprise can often implement and adapt the same principles and best practices for a virtualized server environment that it would use for a server farm. These include the following:

- Strong physical and logical access controls, especially over the host and its management console
- Sound configuration management practices and system hardening for the host, including patching, antivirus, limited services, logging, appropriate permissions and other configuration settings
- Appropriate network segregation, including the avoidance of virtual machines in the demilitarized zone (DMZ) and the placement of management tools on a separate network segment
- Strong change management practices

SPECIALIZED SYSTEMS

Some computer systems and applications are very specialized and may have unique threats and risk and require different types of controls.

Examples of specialized systems include **supervisory control and data acquisition (SCADA)** systems or other real-time monitoring or control systems that operate in specialized environments.

SCADA systems control industrial and manufacturing processes, power generation, air traffic control systems, and emergency communications and defense systems.

Historically, these systems were designed as stand-alone systems and because of the real-time nature of their applications often did not have any “overhead” software that would slow down operations. However, these systems are not commonly networked and often have few of the common controls found in more commercial systems.

Because of the importance of these systems on critical operations, they can be targeted by many different adversaries, and the impact of a successful attack can be catastrophic or even life threatening.

Many existing SCADA systems did not consider security in their design or deployment, and while vendors are improving security, these systems require careful assessment of risk and threats and often require special controls to compensate for inherent weaknesses.

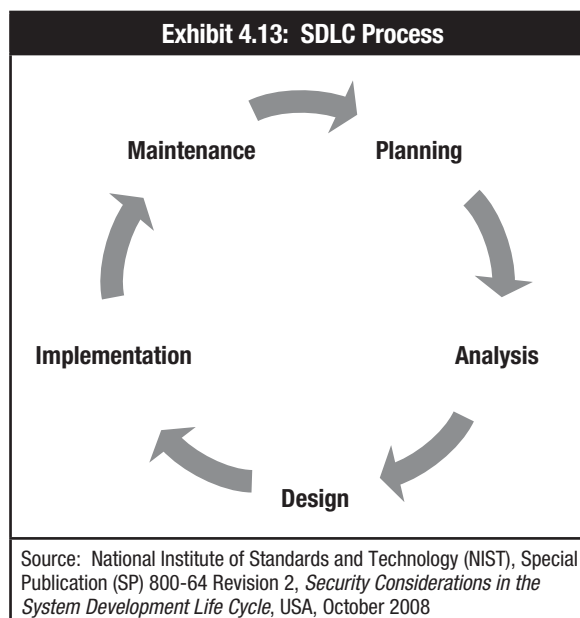
Page intentionally left blank

TOPIC 6—APPLICATION SECURITY

Insecure applications open your organization up to external attackers who may try to use unauthorized code to manipulate the application to access, steal, modify or delete sensitive data. Application security measures should be applied during the design and development phase of the application, followed by routine security countermeasures used throughout the life cycle.

SYSTEM DEVELOPMENT LIFE CYCLE (SDLC)³⁶

Organizations often commit significant resources (e.g., people, applications, facilities and technology) to develop, acquire, integrate and maintain application systems that are critical to the effective functioning of key business processes. The SDLC process, shown in **exhibit 4.13**, guides the phases deployed in the development or acquisition of a software system and, depending on the methodology, may even include the controlled retirement of the system.



The SDLC includes:

- IT processes for managing and controlling project activity
- An objective for each phase of the life cycle that is typically described with key deliverables, a description of recommended tasks and a summary of related control objectives for effective management
- Incremental steps or deliverables that lay the foundation for the next phase

Specifically, the SDLC is a formal process to characterize design requirements and should include:

- Business requirements containing descriptions of what a system should do
- Functional requirements and the use of case models describing how users will interact with a system
- Technical requirements, design specifications and coding specifications describing how the system will interact, conditions under which the system will operate and the information criteria that the system should meet
- Risk mitigation and control requirements to protect the integrity of the system, confidentiality of information stored, processed or communicated as well as adequate authentication and authorization mechanisms

³⁶ ISACA, *CISA Review Manual 2014*, USA

SECURITY WITHIN SDLC

The design and deployment of controls will often be undertaken as a systems development project. While there are several project management techniques that can be used to manage system development projects, they should be an integral and equal part of any SDLC process.

DESIGN REQUIREMENTS

Not considering the security in the design of a system or application is one of the major contributing factors to today's cybersecurity vulnerabilities, making it easier for systems to be compromised. Too often, security is an afterthought, and controls are retrofitted in an ad hoc way only after security weaknesses are identified.

Security and risk mitigation should be formal design criteria in any SDLC process and start with threat and risk assessment of the proposed system, identification of controls, implementation of those controls, and testing and review.

TESTING

The testing phase of SDLC includes:

- Verification and validation that a program, subsystem or application, and the designed security controls perform the functions for which they have been designed
- Determination of whether the units being tested operate without any malfunction or adverse effect on other components of the system
- A variety of development methodologies and organizational requirements to provide for a large range of testing schemes or levels

From a security perspective, this should include vulnerability and control testing.

REVIEW PROCESS

Code review processes vary from informal processes to very formal walk-throughs, team review or code inspections. Security should be an integrated part of any review process.

SEPARATION OF DEVELOPMENT, TESTING AND PRODUCTION ENVIRONMENTS

Development and testing environments are relatively open and often have fewer access controls due to the collaborative nature of the development process. It is important to separate the development, testing and production environments to minimize a compromise or misconfiguration being introduced or cascading through the process. Different access controls (credentials) should be used between the different environments.

Also, if production data are used in the test environment, private or personally identifiable information should be scrambled so that confidential information is not inadvertently disclosed.

OWASP TOP TEN

The Open Web Application Security Project (OWASP) is an open community dedicated to application security. Each year, OWASP publishes a list of the top 10 application security risks. **Exhibit 4.14** provides the top 10 application security risks for 2013.

Exhibit 4.14: Top 10 Application Security Risks in 2013

Attack Vector	Description of Security Risk
Injection	Injection flaws occur when untrusted data is sent to an interpreter. The attacker can trick the interpreter into executing unintended commands or accessing unauthorized data. Injection flaws are prevalent and are often found in SQL and LDAP queries and OS commands.
Broken Authentication and Session Management	If an application function related to authentication or session management is not implemented correctly, it can allow an attacker to compromise passwords, keys or session tokens and impersonate users.
Cross-Site Scripting (XSS)	XSS flaws occur when an application takes untrusted data and sends it to a web browser without proper validation. This is the most prevalent web application security flaw. Attackers can use XSS to hijack user sessions, insert hostile content, deface web sites and redirect users.
Insecure Direct Object References	A direct object reference occurs when a developer exposes a reference to an internal implementation object. Attackers can manipulate these references to access unauthorized data.
Security Misconfiguration	Security settings must be defined, implemented and maintained for applications, frameworks, application servers, web servers, database servers and platforms. Security misconfiguration can give attackers unauthorized access to system data or functionality.
Sensitive Data Exposure	If web applications do not properly secure sensitive data through the use of encryption, attackers may steal or modify sensitive data such as health records, credit cards, tax IDs and authentication credentials.
Missing Function Level Access Control	When function level access rights are not verified, attackers can forge requests to access functionality without authorization.
Cross-Site Request Forgery (CSRF)	A CSRF attack occurs when an attacker forces a user's browser to send forged HTTP requests, including session cookies. This allows an attacker to trick victims into performing operations on the illegitimate web site.
Using Components with Known Vulnerabilities	Certain components such as libraries, frameworks and other software modules usually run with full privileges. Attackers can exploit a vulnerable component to access data or take over a server.
Unvalidated Redirects and Forwards	Web applications frequently redirect or forward users to other pages. When untrusted data are used to determine the destination, an attacker can redirect victims to phishing or malware sites.

Application controls are controls over input, processing and output functions. They include methods to help ensure data accuracy, completeness, validity, verifiability and consistency, thus achieving data integrity and data reliability.

Application controls may consist of edit tests, totals, reconciliations and identification, and reporting of incorrect, missing or exception data. Automated controls should be coupled with manual procedures to ensure proper investigation of exceptions. Implementation of these controls helps ensure system integrity, that applicable system functions operate as intended, and that information contained by the system is relevant, reliable, secure and available when needed. Application controls include:

- Firewalls
- Encryption programs
- Anti-malware programs
- Spyware detection/removal programs
- Biometric authentication

In order to reduce application security risk, OWASP recommends the following:

- Define application security requirements
- Utilize good application security architecture practices from the start of the application design
- Build strong and usable security controls
- Integrate security into the development lifecycle
- Stay current on application vulnerabilities

ADDITIONAL THREATS

It is important for the aspiring security practitioner to recognize that there are many sources of security-related advice, best practices and recommendations. Just because a threat does not make it into a “top” list for a year does not mean that you can forget it.

Other security threats to be aware of include:

- **Covert Channel**—Means of illicitly transferring information between systems using existing infrastructure. Covert channels are simple, stealthy attacks that often go undetected.
- **Race condition**—According to Rouse, “an undesirable situation that occurs when a device or system attempts to perform two or more operations at the same time, but because of the nature of the device or system, the operations must be done in the proper sequence in order to be done correctly.”³⁷ Race conditions vary; however, these vulnerabilities all afford opportunities for unauthorized network access.³⁸
- **Return-oriented attack**—Frequently used technique to exploit memory corruption vulnerabilities. Simply stated, it allows an attacker to execute code despite the technological advances such as nonexecutable stacks and nonexecutable heaps. Memory corruption vulnerabilities occur “when a privileged program is coerced into corrupting its own memory space, such that the memory areas corrupted have an impact on the secure functioning of the program.”
- **Steganography**—The art or practice of concealing a message, image or file within another message, image or file. Media files are ideal because of their large size.

WIRELESS APPLICATION PROTOCOL

Wireless Application Protocol (WAP) is a general term used to describe the multilayered protocol and related technologies that bring Internet content to wireless mobile devices such as smartphones. WAP protocols are largely based on Internet technologies. The motivation for developing WAP was to extend Internet technologies to wireless networks and devices.

WAP supports most wireless networks and is supported by all operating systems specifically engineered for handheld devices and some mobile phones. These kinds of devices that use displays and access the Internet run what are called micro-browsers, which have small file sizes that can accommodate the low-memory constraints of hand held devices and the low-bandwidth constraints of a wireless hand held network. Although WAP supports Hypertext Markup Language (HTML) and extensible markup language (XML), the Wireless Markup Language (WML) language (an XML application) is designed specifically for small screens and one- hand navigation without a keyboard.

The following are general issues and exposures related to wireless access:

- **The interception of sensitive information**—Information is transmitted through the air, which increases the potential for unprotected information to be intercepted by unauthorized individuals.
- **The loss or theft of devices**—Wireless devices tend to be relatively small, making them much easier to steal or lose. If encryption is not strong, a hacker can easily get at the information that is password- or PIN-protected. Theft or loss can result in the loss of data that have been stored on these devices.
- **The misuse of devices**—Devices can be used to gather information or intercept information that is being passed over wireless networks for financial or personal benefit.
- **Distractions caused by the devices**—The use of wireless devices distract the user. If these devices are being used in situations where an individual’s full attention is required (e.g., driving a car), they could result in an increase in the number of accidents.
- **Possible health effects of device usage**—The safety or health hazards have not yet been identified. However, there are currently a number of concerns with respect to electromagnetic radiation, especially for those devices that must be held beside the head.
- **Wireless user authentication**—There is a need for stronger wireless user authentication and authorization tools at the device level. The current technology is just emerging.
- **File security**—Wireless phones and PDAs do not use the type of file access security that other computer platforms can provide.

³⁷ Rouse, Margaret; *Race Condition*, September 2005, <http://searchstorage.techtarget.com/definition/race-condition>

³⁸ Herath, Nishad; “The State of Return Oriented Programming in Contemporary Exploits,” Security Intelligence, 3 March 2014, <http://securityintelligence.com/return-oriented-programming-rop-contemporary-exploits/#.VFkNEBa9bD0>

- **WEP security encryption**—WEP security depends particularly on the length of the encryption key and on the usage of static WEP (many users on a WLAN share the same key) or dynamic WEP (per-user, per-session, dynamic WEP key tied to the network logon). The 64-bit encryption keys that are in use in the WEP standard encryption can be easily broken by the currently available computing power. Static WEP, used in many WLANs for flexibility purposes, is a serious security risk, as a static key can easily be lost or broken, and, once this has occurred, all of the information is available for viewing and use. An attacker possessing the WEP key could also sniff packets being transmitted and decrypt them.
- **Interoperability**—Most vendors offer 128-bit encryption modes. However, they are not standardized, so there is no guarantee that they will interoperate. The use of the 128-bit encryption key has a major impact on performance with 15-20 percent degradation being experienced. Some vendors offer proprietary solutions; however, this only works if all access points and wireless cards are from the same vendor.
- **Translation point**—The location where information being transmitted via the wireless network is converted to the wired network. At this point, the information, which has been communicated via the WAP security model using Wireless Transport Layer Security, is converted to the secure socket layer, where the information is decrypted and then encrypted again for communication via TCP/IP.

Page intentionally left blank

TOPIC 7—DATA SECURITY

Databases can be individually protected with control that is similar to protections applied at the system level. Specific controls that can be placed at the database level include:

- Authentication and authorization of access
- Access controls limiting or controlling the type of data that can be accessed and what types of accesses are allowed (such as read-only, read and write, or delete).
- Logging and other transactional monitoring
- Encryption and integrity controls
- Backups

The controls used to protect databases should be designed in conjunction with system and application controls and form another layer of protection in a defense in depth scheme.

DATA CLASSIFICATION

The information an organization uses can be of varying value and importance. For example, some information may be public and require minimal protection while other information such as national security information, health or other personal information or trade secrets could result in significant harm to the organization if inadvertently released, deleted or modified.

It is important for an organization to understand the sensitivity of information and classify data based on its sensitivity and the impact of release or loss of the information.

Data classification works by tagging data with metadata based on a classification taxonomy. This enables data to be found quickly and efficiently, cuts back on storage and backup costs and helps to allocate and maximize resources. Classification levels should be kept to a minimum. They should be simple designations that assign different degrees of sensitivity and criticality.

Data classification should be defined in a data classification policy that provides definition of different classes of information and how each class of information should be handled and protected. In addition, the classification scheme should convey the association of the data and their supporting business processes.

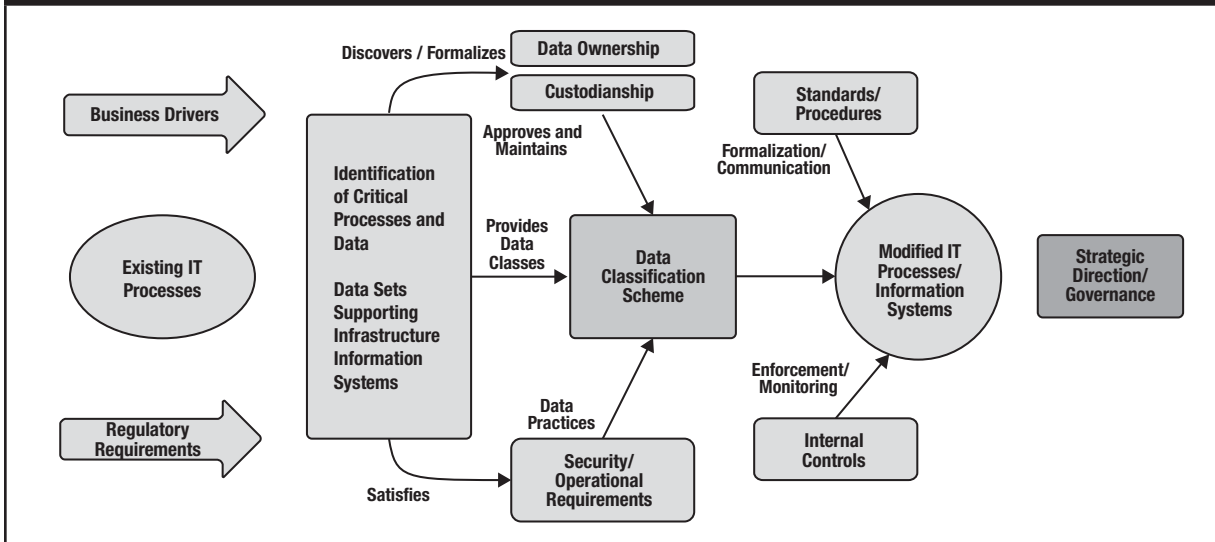
In some cases, local regulations may impact data classification and handling such as those controlled by data protection acts. For example, the US Sarbanes-Oxley Act defines which data records must be stored and for how long.

Information may also need to be reclassified based on changes to its importance. For example, prior to a product release, details of the design, pricing and other information may be confidential and need significant protection; however, after the product is announced, this information may become public and not require the same levels of protection.

DATA OWNERS

Another important consideration for data security is defining the data owner. Although IT applies the security controls and monitoring of business data, the data do not belong to IT. Business information belongs to whoever is ultimately responsible for the business process. The owner is usually responsible for determining the data classification and, therefore, the level of protection required. The data owner may be an individual who creates the data or an organizational element that acts as a custodian of the information. The data classification process is shown in **exhibit 4.15**.

Exhibit 4.15: Data Classification Process

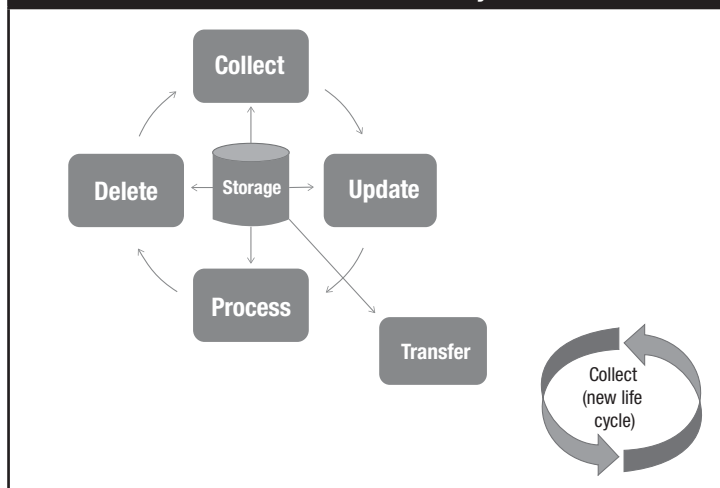


When classifying data, the following requirements should be considered:

- **Access and authentication**—Determine access requirements including defining users profiles, access approval criteria and validation procedures.
- **Confidentiality**—Determine where sensitive data are stored and how they are transmitted.
- **Privacy**—Utilize controls to warn an affected user that his or her information is about to be used.
- **Availability**—Determine the uptime and downtime tolerances for different data types.
- **Ownership and distribution**—Establish procedures to protect data from unauthorized copy and distribution.
- **Integrity**—Protect data from unauthorized changes using change control procedures and automated monitoring and detection for unauthorized changes and manipulation.
- **Data retention**—Determine retention periods and preserve specific versions of software, hardware, authentication credentials and encryption keys to ensure availability.
- **Auditability**—Keep track of access, authorizations, changes and transactions.

After data classification has been assigned, security controls can be established such as encryption, authentication and logging. Security measures should increase as the level of data sensitivity or criticality increases. The full data life cycle is shown in **exhibit 4.16**.

Exhibit 4.16: Data Life Cycle



DATABASE SECURITY

Database security protects stored files and information in an organization's network database. One of the best ways to secure this information is with the digital rights management (DRM), which refers to access control technologies that can be used by hardware manufacturers, publishers, copyright holders and individuals to impose limitations on the usage of digital content and devices. Organizations can also restrict access to specific instances of digital works or devices. Users are only given access to the files they need to prevent internal attacks and attacks that dupe employees into providing secure data.

Another database security element is controlling access to hard copy backups such as tape drives and hard disks. Tape management systems (TMS) and disk management systems (DMS) often include physical security procedures that guard access to backup machines as well as inventory control systems to account for database backups.

Page intentionally left blank

SECTION 4—KNOWLEDGE CHECK

1. Put the steps of the penetration testing phase into the correct order.
 - a. Attack
 - b. Discovery
 - c. Reporting
 - d. Planning
2. System hardening should implement the principle of _____ or _____.
 - a. Governance, compliance
 - b. Least privilege, access control
 - c. Stateful inspection, remote access
 - d. Vulnerability assessment, risk mitigation
3. Select all that apply. Which of the following are considered functional areas of network management as defined by ISO?
 - a. Accounting management
 - b. Fault management
 - c. Firewall management
 - d. Performance management
 - e. Security management
4. Virtualization involves:
 - a. The creation of a layer between physical and logical access controls.
 - b. Multiple guests coexisting on the same server in isolation of one another.
 - c. Simultaneous use of kernel mode and user mode.
 - d. DNS interrogation, WHOIS queries and network sniffing.
5. Vulnerability management begins with an understanding of cybersecurity assets and their locations, which can be accomplished by:
 - a. Vulnerability scanning.
 - b. Penetration testing.
 - c. Maintaining an asset inventory.
 - d. Using command line tools.

Page intentionally left blank



CYBERSECURITY NEXUS

Section 5:

Incident Response

Topics covered in this section include:

1. Distinctions between events and incidents
2. Incident categories and types
3. Security event management
4. Key elements of incident response plans
5. Legal requirements of investigation and evidence preservation
6. Requirements for forensic investigations
7. Business continuity planning and disaster recovery

Page intentionally left blank

TOPIC 1—EVENT VS. INCIDENT

All organizations need to put significant effort into protecting and preventing cyberattacks from causing harm or disruption. However, security controls are not perfect and cannot completely eliminate all risk; therefore, it is important that organizations prepare for, and are capable of detecting and managing, potential cybersecurity problems.

EVENT VS. INCIDENT

It is important to distinguish between an event and an incident because the two terms are often used synonymously, even though they have different meanings. An event is any change, error or interruption within an IT infrastructure such as a system crash, a disk error or a user forgetting their password. The National Institute of Standards and Technology (NIST) defines an event as “any observable occurrence in a system or network.”³⁹

While there is general agreement on what an event is, there is a greater degree of variety in defining an incident. NIST defines an incident as “a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.” Another commonly used definition is: “The attempted or successful unauthorized access, use, disclosure, modification or loss of information or interference with system or network operations.” Many organizations define an incident as the activity of a human threat agent. Others would include anything disruptive, including a court order for discovery of electronic information or disruption from a natural disaster.

Regardless of the exact definition used by a particular organization, it is important to distinguish between events that are handled in the normal course of business and incidents that require security and investigative expertise to manage.

TYPES OF INCIDENTS

A cybersecurity incident is an adverse event that negatively impacts the confidentiality, integrity and availability of data. Cybersecurity incidents may be unintentional, such as someone forgetting to activate an access list in a router, or intentional, such as a targeted attack by a hacker. These events may also be classified as technical or physical. Technical incidents include viruses, malware, denial-of-service (DoS) and system failure. Physical incidents may include social engineering and lost or stolen laptops or mobile devices.

There are many types of cybersecurity-related incidents, and new types of incidents emerge frequently. US-CERT provides categories of security incidents and reporting time frames used by federal agencies, shown in **exhibit 5.1**.

Exhibit 5.1: Security Incidents and Reporting Time Frames			
Category	Name	Description	Reporting Time Frame
CAT 1	Unauthorized Access	An individual gains logical or physical access without permission to a network, system, application, data or other resource	Within 1 hour of discovery/ detection
CAT 2	Denial-of-service (DoS)	An attack that successfully prevents or impairs normal authorized functionality of networks, systems or applications by exhausting resources	Within 2 hours of discovery/ detection if the successful attack is still ongoing
CAT 3	Malicious Code	Successful installation of malicious software (e.g., virus, worm, Trojan horse or other code-based malicious entity) that infects an operating system or application	Daily; within 1 hour of discovery/detection if widespread
CAT 4	Improper Usage	A person violates acceptable computing use policies	Weekly
CAT 5	Scans/Probes/ Attempted Access	Any activity that seeks to access or identify a computer, open ports, protocols, service or any combination	Monthly
CAT 6	Investigation	Unconfirmed incidents that are potentially malicious or anomalous activity	N/A

³⁹ National Institute of Standards and Technology (NIST), *Special Publication 800-61 Revision 2, Computer Security Incident Handling Guide*, USA, August 2012

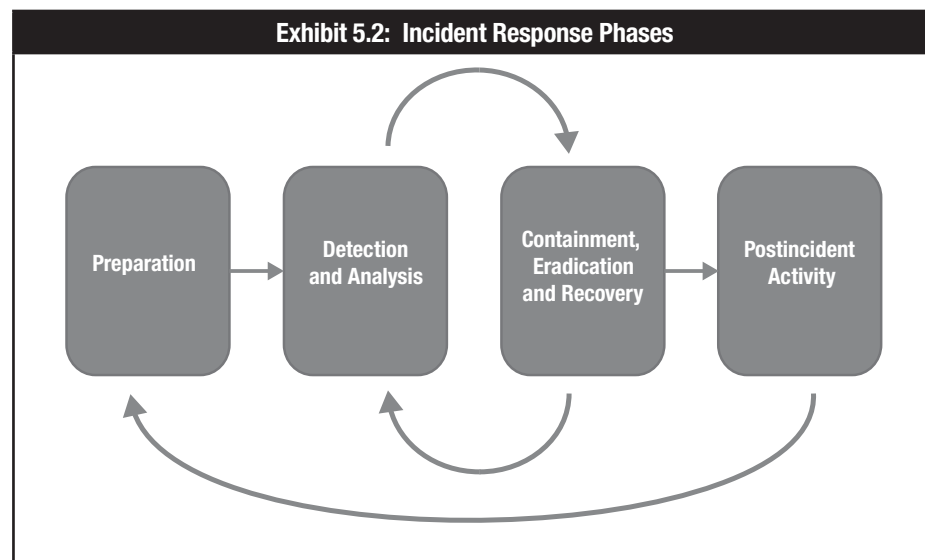
Page intentionally left blank

TOPIC 2—SECURITY INCIDENT RESPONSE

WHAT IS INCIDENT RESPONSE?⁴⁰

Incident response is a formal program that prepares an entity for an incident. Incident response phases are shown in **exhibit 5.2**. Incident response generally includes:

1. **Preparation** to establish roles, responsibilities and plans for how an incident will be handled
2. **Detection and Analysis** capabilities to identify incidents as early as possible and effectively assess the nature of the incident
3. **Investigation** capability if identifying an adversary is required
4. **Mitigation and Recovery** procedures to contain the incident, reduce losses and return operations to normal
5. **Postincident Analysis** to determine corrective actions to prevent similar incidents in the future



WHY DO WE NEED INCIDENT RESPONSE?

Waiting until an incident occurs to figure out what to do is a recipe for disaster. Adequate incident response planning and implementation allows an organization to respond to an incident in a systematic manner that is more effective and timely. Organizations that do not plan for a cybersecurity incident will suffer greater losses for a more extended period of time. The current trend shows an increase in incident occurrences. These attacks are becoming more sophisticated and are resulting in escalating losses.

In addition, many national regulations and international standards require the development of incident response capabilities. Compliance regulations such as Payment Card Industry (PCI) and Federal Deposit Insurance Corporation (FDIC) provide strict requirements for security policies and incident response planning.

ELEMENTS OF AN INCIDENT RESPONSE PLAN

The following model proposed by Schultz, Brown and Longstaff presents the six-phase model of incident response including preparation, identification, containment, eradication, restoration and follow-up:²⁵

- **Preparation**—This phase prepares an organization to develop an incident response plan prior to an incident. Sufficient preparation facilitates smooth execution. Activities in this phase include:
 - Establishing an approach to handle incidents
 - Establishing policy and warning banners in information systems to deter intruders and allow information collection
 - Establishing a communication plan to stakeholders

⁴⁰ ISACA, *CISM Review Manual 2014*, USA

- Developing criteria on when to report an incident to authorities
- Developing a process to activate the incident management team
- Establishing a secure location to execute the incident response plan
- Ensuring equipment needed is available
- **Identification**—This phase aims to verify if an incident has happened and find out more details about the incident. Reports on possible incidents may come from information systems, end users or other organizations. Not all reports are valid incidents, as they may be false alarms or may not qualify as an incident. Activities in this phase include:
 - Assigning ownership of an incident or potential incident to an incident handler
 - Verifying that reports or events qualify as an incident
 - Establishing chain of custody during identification when handling potential evidence
 - Determining the severity of an incident and escalating it as necessary
- **Containment**—After an incident has been identified and confirmed, the IMT is activated and information from the incident handler is shared. The team will conduct a detailed assessment and contact the system owner or business manager of the affected information systems/assets to coordinate further action. The action taken in this phase is to limit the exposure. Activities in this phase include:
 - Activating the incident management/response team to contain the incident
 - Notifying appropriate stakeholders affected by the incident
 - Obtaining agreement on actions taken that may affect availability of a service or risk of the containment process
 - Getting the IT representative and relevant virtual team members involved to implement containment procedures
 - Obtaining and preserving evidence
 - Documenting and taking backups of actions from this phase onward
 - Controlling and managing communication to the public by the public relations team
- **Eradication**—When containment measures have been deployed, it is time to determine the root cause of the incident and eradicate it. Eradication can be done in a number of ways: restoring backups to achieve a clean state of the system, removing the root cause, improving defenses and performing vulnerability analysis to find further potential damage from the same root cause. Activities in this phase include:
 - Determining the signs and cause of incidents
 - Locating the most recent version of backups or alternative solutions
 - Removing the root cause. In the event of worm or virus infection, it can be removed by deploying appropriate patches and updated antivirus software.
 - Improving defenses by implementing protection techniques
 - Performing vulnerability analysis to find new vulnerabilities introduced by the root cause
- **Recovery**—This phase ensures that affected systems or services are restored to a condition specified in the service delivery objectives (SDO) or business continuity plan (BCP). The time constraint up to this phase is documented in the RTO. Activities in this phase include:
 - Restoring operations to normal
 - Validating that actions taken on restored systems were successful
 - Getting involvement of system owners to test the system
 - Facilitating system owners to declare normal operation
- **Lessons learned**—At the end of the incident response process, a report should always be developed to share what occurred, what measures were taken and the results after the plan was executed. Part of the report should contain lessons learned that provide the IMT and other stakeholders valuable learning points of what could have been done better. These lessons should be developed into a plan to enhance the incident management capability and the documentation of the incident response plan. Activities in this phase include:
 - Writing the incident report
 - Analyzing issues encountered during incident response efforts
 - Proposing improvement based on issues encountered
 - Presenting the report to relevant stakeholders

SECURITY EVENT MANAGEMENT

In order to prepare for and identify an incident, organizations use a myriad of security tools, such as vulnerability assessments, firewalls and intrusion detection systems (IDSs), that collect a high volume of data. However, security teams have to analyze and interpret this overwhelming amount of data, referred to as log data overload. An emerging solution to this problem is security event management (SEM). SEM systems automatically aggregate and correlate security event log data across multiple security devices. This allows security analysts to focus on a manageable list of critical events.

Security incidents are often made up of a series of events that occur throughout a network. By correlating data, the SEM can take many isolated events and combine them to create one single relevant security incident. These systems use either rule-based or statistical correlation. Rule-based correlations create situation-specific rules that establish a pattern of events. Statistical correlation uses algorithms to calculate threat levels incurred by relevant events on various IT assets.

There are a variety of SEM solutions available that provide real-time monitoring, correlation of events, notifications and console views. In addition, security incident and event management (SIEM) systems take the SEM capabilities and combine them with the historical analysis and reporting features of security information management (SIM) systems.

Information security teams should periodically analyze the trends found from SEM or SIEM systems, such as attempted attack types or most frequently targeted resources. This allows the organization to investigate incidents as well as allocate appropriate resources to prevent future incidents.

Page intentionally left blank

TOPIC 3—INVESTIGATIONS, LEGAL HOLDS AND PRESERVATION

INVESTIGATIONS

Cybersecurity incident investigations include the collection and analysis of evidence with the goal of identifying the perpetrator of an attack or unauthorized use or access. This may overlap with, but is distinctly separate from, the technical analysis used in incident response where the objective is to understand the nature of the attack, what happened and how it occurred.

The goals of an investigation can conflict with the goals of incident response. Investigations may require the attack or unauthorized access to continue while it is analyzed and evidence is collected, whereas remediation may destroy evidence or preclude further investigation. The organization's management must be an integral part of making decisions between investigating and remediation.

Investigations may be conducted for criminal activity (as defined by governmental statutes and legislation), violations of contracts or violations of an organization's policies. Cybersecurity investigators may also assist in other types of investigations where computers or networks were used in the commission of other crimes, such as harassment where email was used.

An investigation may take place entirely in-house, or may be conducted by a combination of in-house personnel, service providers and law enforcement or regulators.

EVIDENCE PRESERVATION

It is very important to preserve evidence in any situation. Most organizations are not well equipped to deal with intrusions and electronic crimes from an operational and procedural perspective, and they respond to it only when the intrusion has occurred and the risk is realized. The evidence loses its integrity and value in legal proceedings if it has not been preserved and subject to a documented chain of custody. This happens when the incident is inappropriately managed and responded to in an *ad hoc* manner.

For evidence to be admissible in a court of law, the chain of custody needs to be maintained accurately and chronologically. The chain of evidence essentially contains information regarding:

- Who had access to the evidence (chronological manner)
- The procedures followed in working with the evidence (such as disk duplication, virtual memory dump)
- Proof that the analysis is based on copies that are identical to the original evidence (could be documentation, checksums, time stamps)

The evidence of a computer crime exists in the form of log files, file time stamps, contents of memory, etc. Other sources include browser history, contact lists, cookies, documents, hidden files, images, metadata, temporary files and videos. While not comprehensive, it helps provide context for the cybersecurity novice as to how much information is available to responders. The ability to locate and capture evidence is dependent on data type, investigators' skills and experience, and tools.

Rebooting the system or accessing files could result in such evidence being lost, corrupted or overwritten. Therefore, one of the first steps taken should be copying one or more images of the attacked system. Memory content should also be dumped to a file before rebooting the system. Any further analysis must be performed on an image of the system and on copies of the memory dumped—not on the original system in question.

In addition to protecting the evidence, it is also important to preserve the chain of custody. **Chain of custody** is a term that refers to documenting, in detail, how evidence is handled and maintained, including its ownership, transfer and modification. This is necessary to satisfy legal requirements that mandate a high level of confidence regarding the integrity of evidence.

LEGAL REQUIREMENTS

Investigations have clearly defined legal requirements and these vary from country to country. Only trained investigators working with legal counsel should undertake investigations. Some of the legal issues that may be applicable include:

- Evidence collection and storage
- Chain of custody of evidence
- Searching or monitoring communications
- Interviews or interrogations
- Licensing requirements
- Law enforcement involvement
- Labor, union and privacy regulation

These and other legal considerations are evolving when applied to cyberspace and vary, sometimes significantly, from jurisdiction to jurisdiction. Failure to perform an investigation in compliance with the appropriate legal requirements may create criminal or civil liabilities for the investigator and organization or may result in an inability to pursue legal remedies.

Many attacks are international in scope, and navigating the different (and sometimes conflicting) legal issues can be challenging, adding complexity to cybersecurity investigations. In some countries, private individuals and organizations are not permitted to carry out investigations and require law enforcement.

TOPIC 4—FORENSICS

By definition, **digital forensics** is the “process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable in any legal proceedings (i.e., a court of law),” according to D. Rodney McKemmish in his book *Computer and Intrusion Forensics*.⁴¹ Computer forensics includes activities that involve the exploration and application of methods to gather, process, interpret and use digital evidence that help to substantiate whether an incident happened such as:

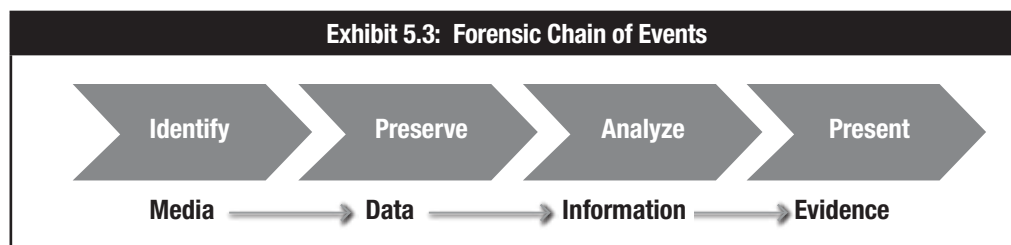
- Providing validation that an attack actually occurred
- Gathering digital evidence that can later be used in judicial proceedings

Any electronic document or data can be used as digital evidence, provided there is sufficient manual or electronic proof that the contents of digital evidence are in their original state and have not been tampered with or modified during the process of collection and analysis.

It is important to use industry-specified best practices, proven tools and due diligence to provide reasonable assurance of the quality of evidence. It is also important to demonstrate integrity and reliability of evidence for it to be acceptable to law enforcement authorities. For example, if the IS auditor “boots” a computer suspected of containing stored information that might represent evidence in a court case, the auditor cannot later deny that they wrote data to the hard drive because the boot sequence writes a record to the drive. This is the reason specialist tools are used to take a true copy of the drive, which is then used in the investigation.

There are four major considerations in the chain of events in regards to evidence in digital forensics. They are shown in **exhibit 5.3** and listed as follows:

- **Identify**—Refers to the identification of information that is available and might form the evidence of an incident.
- **Preserve**—Refers to the practice of retrieving identified information and preserving it as evidence. The practice generally includes the imaging of original media in presence of an independent third party. The process also requires being able to document chain-of-custody so that it can be established in a court of law.
- **Analyze**—Involves extracting, processing and interpreting the evidence. Extracted data could be unintelligible binary data after it has been processed and converted into human readable format. Interpreting the data requires an in-depth knowledge of how different pieces of evidence may fit together. The analysis should be performed using an image of media and not the original.
- **Present**—Involves a presentation to the various audiences such as management, attorneys, court, etc



Acceptance of the evidence depends upon the manner of presentation (as it should be convincing), qualifications of the presenter, and credibility of the process used to preserve and analyze the evidence. The assurance professional should give consideration to key elements of computer forensics during audit planning. These key elements are described in the following subsections.

⁴¹ McKemmish, D. Rodney. *Computer and Intrusion Forensics*, Artech House, USA, 2003

DATA PROTECTION

To prevent sought-after information from being altered, all measures must be in place. It is important to establish specific protocols to inform appropriate parties that electronic evidence will be sought and to not destroy it by any means. Infrastructure and processes for incident response and handling should be in place to permit an effective response and forensic investigation if an event or incident occurs.

DATA ACQUISITION

All information and data required should be transferred into a controlled location; this includes all types of electronic media such as fixed disk drives and removable media. Each device must be checked to ensure that it is write-protected. This may be achieved by using a device known as a write-blocker. It is also possible to get data and information from witnesses or related parties by recorded statements. By volatile data, investigators can determine what is currently happening on a system. This kind of data includes open ports, open files, active processes, user logons and other data present in RAM. This information is lost when the computer is shut down.

IMAGING

Imaging is a process that allows one to obtain a bit-for-bit copy of data to avoid damage of original data or information when multiple analyses may be performed. The imaging process is made to obtain residual data, such as deleted files, fragments of deleted files and other information present, from the disk for analysis. This is possible because imaging duplicates the disk surface, sector by sector. With appropriate tools, it is sometimes possible to recover destroyed information (erased even by reformatting) from the disk's surface.

EXTRACTION

This process consists of identification and selection of data from the imaged data set. This process should include standards of quality, integrity and reliability. The extraction process includes software used and media where an image was made. The extraction process could include different sources such as system logs, firewall logs, IDS logs, audit trails and network management information.

INTERROGATION

Interrogation is used to obtain prior indicators or relationships, including telephone numbers, IP addresses and names of individuals, from extracted data.

INGESTION/NORMALIZATION

This process converts the information extracted to a format that can be understood by investigators. It includes conversion of hexadecimal or binary data into readable characters or a format suitable for data analysis tools. It is possible to create relationships from data by extrapolation, using techniques such as fusion, correlation, graphing, mapping or time lining, which could be used in the construction of the investigation's hypothesis.

REPORTING

The information obtained from digital forensics has limited value when it is not collected and reported in the proper way. A report must state why the system was reviewed, how the computer data were reviewed and what conclusions were made from this analysis. The report should achieve the following goals:⁴²

- Accurately describe the details of an incident
- Be understandable to decision makers
- Be able to withstand a barrage of legal scrutiny
- Be unambiguous and not open to misinterpretation
- Be easily referenced
- Contain all information required to explain conclusions reached
- Offer valid conclusions, opinions or recommendations when needed
- Be created in a timely manner

⁴² Mandia, Kevin, Matt Pepe, Chris Prosis, *Incident Response & Computer Forensics, 2nd Edition*, McGraw Hill/Osborne, USA, 2003

The report should also identify the organization, sample reports and restrictions on circulation (if any) and include any reservations or qualifications that the assurance professional has with respect to the assignment.

NETWORK TRAFFIC ANALYSIS

Network traffic analysis identifies patterns in network communications. Traffic analysis does not need to have the actual content of the communication but analyzes where traffic is taking place, when and for how long communications occur, and the size of information transferred.

Traffic analysis can be used proactively to identify potential anomalies in communications or during incident response to develop footprints that identify different attacks or the activities of different individuals.

LOG FILE ANALYSIS

Many types of tools have been developed to help reduce the amount of information contained in audit records and to delineate useful information from the raw data. On most systems, audit trail software can create large files, which can be extremely difficult to analyze manually. The use of automated tools is likely to be the difference between unused audit trail data and an effective review. Some of the types of tools include:

- **Audit reduction tools**—These are preprocessors designed to reduce the volume of audit records to facilitate manual review. Before a security review, these tools can remove many audit records known to have little security significance. (This alone may cut in half the number of records in the audit trail.) These tools generally remove records generated by specified classes of events; for example, records generated by nightly backups might be removed.
- **Trend/variance-detection tools**—These look for anomalies in user or system behavior. It is possible to construct more sophisticated processors that monitor usage trends and detect major variations. For example, if a user typically logs in at 09.00, but appears at 04.30 one morning, this may indicate a security problem that may need to be investigated.
- **Attack-signature-detection tools**—These look for an attack signature, which is a specific sequence of events indicative of an unauthorized access attempt. A simple example would be repeated failed logon attempts.

DIGITAL FORENSIC TOOLS

Forensics tools can be sorted into four categories: computer, memory, mobile devices and network.

- **Computer**—Examine non-volatile digital media. Due to the number of tools on the market, we will not discuss specific tools. Vendors base their tools on different platforms (i.e., Windows, Linux, etc.). Most are propriety; however, open source options do exist. Similarly, some are restricted to law enforcement and/or government agencies. Ultimately, business requirements will determine selection.
- **Memory**—Used to acquire and analyze volatile memory
- **Mobile device**—Consists of both software and hardware components. Due to the wide number of devices, manufacturers and intended scope, we will not discuss specific tools. Here cables perform similar to write blockers for computer forensics.
- **Network**—Monitoring and analysis of network traffic. Options range from command-line tools previously mentioned to high-end deep packet inspection appliances. Wireshark® is a free, open-source packet analyzer.

Additionally, you may encounter and be expected to use various support applications. One example is VMware®—virtualization software that allows users to run multiple instances of operating systems on a physical PC.

TIME LINES

Time lines are chronological graphs where events related to an incident can be mapped to look for relationships in complex cases. Time lines can provide simplified visualization for presentation to management and other nontechnical audiences.

ANTI-FORENSICS

Programmers develop anti-forensics tools to make it difficult or impossible for investigators to retrieve information during an investigation. There are numerous ways people can hide information.

Anti-forensics tactics, techniques and procedures (TTPs) include, but are not limited to:

- Securely deleting data
- Overwriting metadata
- Preventing data creation
- Encrypting data
- Encrypting network protocols
- Hiding data in slack space or other unallocated locations
- Hiding data or a file within another file (steganography)

TOPIC 5—DISASTER RECOVERY AND BUSINESS CONTINUITY PLANS

When incident response plans fail to control an incident, the incident could escalate into a disaster.

WHAT IS A DISASTER?

Disasters are disruptions that cause critical information resources to be inoperative for a period of time, adversely impacting organizational operations. The disruption could be a few minutes to several months, depending on the extent of damage to the information resource. Most important, disasters require recovery efforts to restore operational status.

A disaster may be caused by natural calamities, such as earthquakes, floods, tornadoes and fire, or a disaster may be caused by events precipitated by humans such as terrorist attacks, hacker attacks, viruses or human error. Many disruptions start as mere incidents. Normally, if the organization has a help desk or service desk, it would act as the early warning system to recognize the first signs of an upcoming disruption. Often, such disruptions (e.g., gradually deteriorating database performance) go undetected. Until these “creeping disasters” strike (the database halts), they cause only infrequent user complaints.

A cybersecurity-related disaster may occur when a disruption in service is caused by system malfunctions, accidental file deletions, untested application releases, loss of backup, network DoS attacks, intrusions or viruses. These events may require action to recover operational status in order to resume service. Such actions may necessitate restoration of hardware, software or data files.

BUSINESS CONTINUITY AND DISASTER RECOVERY

The purpose of business continuity planning (BCP)/disaster recovery planning (DRP) is to enable a business to continue offering critical services in the event of a disruption and to survive a disastrous interruption to activities. Rigorous planning and commitment of resources are necessary to adequately plan for such an event.

BCP takes into consideration:

- Those critical operations that are necessary to the survival of the organization.
- The human/material resources supporting them
- Predisaster readiness covering incident response management to address all relevant incidents affecting business processes
- Evacuation procedures
- Procedures for declaring a disaster (escalation procedures)
- Circumstances under which a disaster should be declared. All interruptions are not disasters, but a small incident not addressed in a timely or proper manner may lead to a disaster. For example, a virus attack not recognized and contained in time may bring down the entire IT facility.
- The clear identification of the responsibilities in the plan
- The clear identification of the persons responsible for each function in the plan
- The clear identification of contract information
- The step-by-step explanation of the recovery process
- The clear identification of the various resources required for recovery and continued operation of the organization

BCP is primarily the responsibility of senior management, because they are entrusted with safeguarding the assets and the viability of the organization, as defined in the BCP/DRP policy. The BCP is generally followed by the business and supporting units, to provide a reduced but sufficient level of functionality in the business operations immediately after encountering an interruption, while recovery is taking place.

Depending on the complexity of the organization, there could be one or more plans to address the various aspects of BCP and DRP. These plans do not necessarily have to be integrated into one single plan. However, each has to be consistent with other plans to have a viable BCP strategy.

Even if similar processes of the same organization are handled at a different geographic location, the BCP and DRP solutions may be different for different scenarios. Solutions may be different due to contractual requirements (e.g., the same organization is processing an online transaction for one client and the back office is processing for another client). A BCP solution for the online service will be significantly different than one for the back office processing.

BUSINESS IMPACT ANALYSIS

The first step in preparing a new BCP is to identify the business processes of strategic importance—those key processes that are responsible for both the permanent growth of the business and for the fulfillment of the business goals. Ideally, the BCP/DRP should be supported by a formal executive policy that states the organization's overall target for recovery and empowers those people involved in developing, testing and maintaining the plans.

Based on the key processes, a business impact analysis (BIA) process should begin to determine time frames, priorities, resources and interdependencies that support the key processes. Business risk is directly proportional to the impact on the organization and the probability of occurrence of the perceived threat. Thus, the result of the BIA should be the identification of the following:

- The human resources, data, infrastructure elements and other resources (including those provided by third parties) that support the key processes
- A list of potential vulnerabilities—the dangers or threats to the organization
- The estimated probability of the occurrence of these threats
- The efficiency and effectiveness of existing risk mitigation controls (risk countermeasures)

Information is collected for the BIA from different parts of the organization which own key processes/ applications. To evaluate the impact of downtime for a particular process/application, the impact bands are developed (i.e., high, medium, low) and, for each process, the impact is estimated in time (hours, days, weeks). The same approach is used when estimating the impact of data loss. If necessary, the financial impact may be estimated using the same techniques, assigning the financial value to the particular impact band. In addition, data for the BIA may be collected on the time frames needed to supply vital resources—how long the organization may run if a supply is broken or when the replacement has arrived.

The BIA should answer three important questions:

1. What are the different business processes?
2. What are the critical information resources related to an organization's critical business processes?
3. What is the critical recovery time period for information resources in which business processing must be resumed before significant or unacceptable losses are suffered?

SUPPLY CHAIN CONSIDERATION

NIST defines the information and communications technology (ICT) supply chain as “a complex, globally distributed, and interconnected ecosystem that is long, has geographically diverse routes, and consists of multiple tiers of outsourcing.” This environment is interdependent on public and private entities for development, integration and delivery of ICT products and services.⁴³

The complexity of supply chains and impact requires persistent awareness of risk and consideration. The most significant factors contributing to the fragility of supply chains are economic, environmental, geopolitical and technological.⁴⁴

Whether it is the rapid adoption of open source software, tampering of physical hardware or natural disasters taking down data centers, supply chains require risk management. An example of this was described in an article in Forbes: Flooding in Thailand created significant shortages in the hard disk drive market, which cost well-known electronics manufacturers millions of dollars in losses.⁴⁵

⁴³ Boyens, Jon; Celia Paulsen; Rama Moorthy; Nadya Bartol; *NIST SP 800-161, 2nd draft: Supply Chain Risk Management Practices for Federal Information Systems and Organization*, NIST, USA, 2014

⁴⁴ Rodrigue, Jean-Paul; *Risk in Global Supply Chains*, https://people.hofstra.edu/geotrans/eng/ch9en/conc9en/supply_chain_risks.html

⁴⁵ Culp, Steve, “Supply Chain Risk a Hidden Liability for Many Companies,” *Forbes*, 8 October 2012, www.forbes.com/sites/steveculp/2012/10/08/supply-chain-risk-a-hidden-liability-for-many-companies

Products or services manufactured anywhere may contain vulnerabilities that can present opportunities for ICT supply chain-related compromises. It is especially important to consider supply chain risk from system development, to include research and development (R&D) through useful life and ultimately retirement/disposal of products.

RECOVERY TIME OBJECTIVES (RTO)

RTO is defined as the amount of time allowed for the recovery of a business function or resource after a disaster occurs. The RTO is usually determined based on the point where the ongoing cost of the loss is equal to the cost of recovery.

RECOVERY POINT OBJECTIVE (RPO)

RPO is defined as the acceptable data loss in case of a disruption of operations. It indicates the earliest point in time to which it is acceptable to recover data. In other words, it is the last known point of good data.

To ensure an effective incident management plan or disaster recovery plan, the RTO and RPO must be closely linked. A short RTO may be difficult to achieve if there is a large amount of data to be restored (RPO).

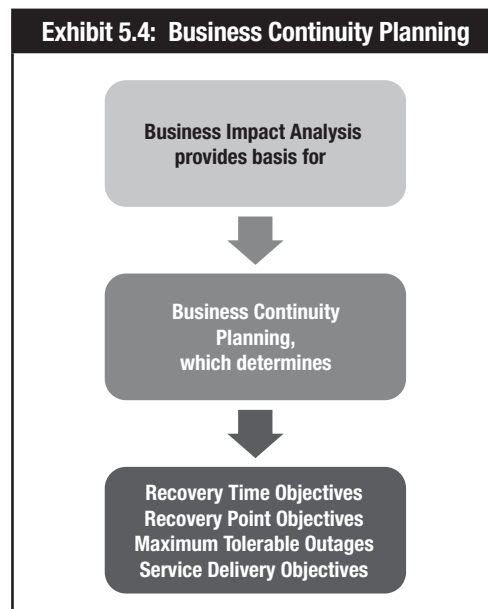
IS BUSINESS CONTINUITY PLANNING

In the case of IS BCP, the approach is the same as in BCP with the exception being that the continuity of IS processing is threatened. IS processing is of strategic importance—it is a critical component since most key business processes depend on the availability of key systems, infrastructure components and data.

The IS BCP should be aligned with the strategy of the organization. The criticality of the various application systems deployed in the organization depends on the nature of the business as well as the value of each application to the business.

The value of each application to the business is directly proportional to the role of the information system in supporting the strategy of the organization. The components of the information system (including the technology infrastructure components) are then matched to the applications (e.g., the value of a computer or a network is determined by the importance of the application system that uses it).

Therefore, the information system BCP/DRP is a major component of an organization's overall business continuity and disaster recovery strategy. If the IS plan is a separate plan, it must be consistent with and support the corporate BCP. See **exhibit 5.4**.



RECOVERY CONCEPTS

Data recovery is the process of restoring data that has been lost, accidentally deleted, corrupted or made inaccessible for any reason. Recovery processes vary depending on the type and amount of data lost, the backup method employed and the backup media. An organization's DRP must provide the strategy for how data will be recovered and assign recovery responsibilities.

BACKUP PROCEDURES

Backup procedures are used to copy files to a second medium such as a disk, tape or the cloud. Backup files should be kept at an offsite location. Backups are usually automated using operating system commands or backup utility programs. Most backup programs compress the data so that the backups require fewer media.

There are three types of data backups: full, incremental and differential. Full backups provide a complete copy of every selected file on the system, regardless of whether it was backed up recently. This is the slowest backup method but the fastest method for restoring data. Incremental backups copy all files that have changed since the last backup was made, regardless of whether the last backup was a full or incremental backup. This is the fastest backup method but the slowest method for restoring data. Differential backups copy only the files that have changed since the last full backup. The file grows until the next full backup is performed.

SECTION 5—KNOWLEDGE CHECK

1. Arrange the steps of the incident response process into the correct order.
 - a. Mitigation and recovery
 - b. Investigation
 - c. Postincident analysis
 - d. Preparation
 - e. Detection and analysis
2. Which element of an incident response plan involves obtaining and preserving evidence?
 - a. Preparation
 - b. Identification
 - c. Containment
 - d. Eradication
3. Select three. The chain of custody contains information regarding:
 - a. Disaster recovery objectives, resources and personnel.
 - b. Who had access to the evidence, in chronological order.
 - c. Labor, union and privacy regulations.
 - d. Proof that the analysis is based on copies identical to the original evidence.
 - e. The procedures followed in working with the evidence.
4. NIST defines a(n) as a “violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.”
 - a. Disaster
 - b. Event
 - c. Threat
 - d. Incident
5. Select all that apply. A business impact analysis (BIA) should identify:
 - a. The circumstances under which a disaster should be declared.
 - b. The estimated probability of the identified threats actually occurring.
 - c. The efficiency and effectiveness of existing risk mitigation controls.
 - d. A list of potential vulnerabilities, dangers and/or threats.
 - e. Which types of data backups (full, incremental and differential) will be used.

Page intentionally left blank

Security Implications and Adoption of Evolving Technology

Topics covered in this section include:

1. Trends in the current threat landscape
2. Characteristics and targets of advanced persistent threats (APTs)
3. Mobile device vulnerabilities, threats and risk
4. BYOD and consumerization of IT and mobile devices
5. Risk and benefits of cloud and digital collaboration

Page intentionally left blank

TOPIC 1—CURRENT THREAT LANDSCAPE

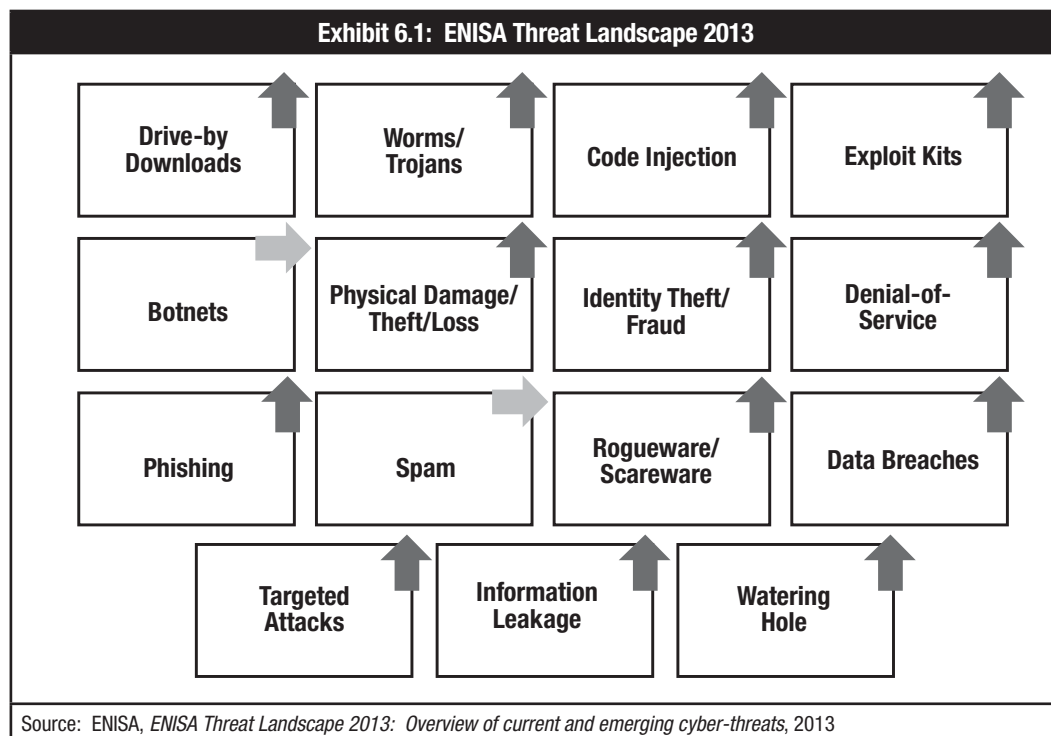
A **threat landscape**, also referred to as a threat environment, is a collection of threats. The cybersecurity threat landscape is constantly changing and evolving as new technologies are developed and cyberattacks and tools become more sophisticated. A threat landscape developed by ENISA is shown in **exhibit 6.1**. Corporations are becoming increasingly dependent on digital technologies that can be susceptible to cyber security risk. Cloud computing, social media, and mobile computing are changing how organizations use and share information. They provide increased levels of access and connectivity, which create larger openings for cybercrime.

Cybercriminals are usually motivated by one or more of the following:

- Financial gains
- Intellectual property (espionage)
- Politics (hacktivism)

Recent trends in the cyberthreat landscape include:

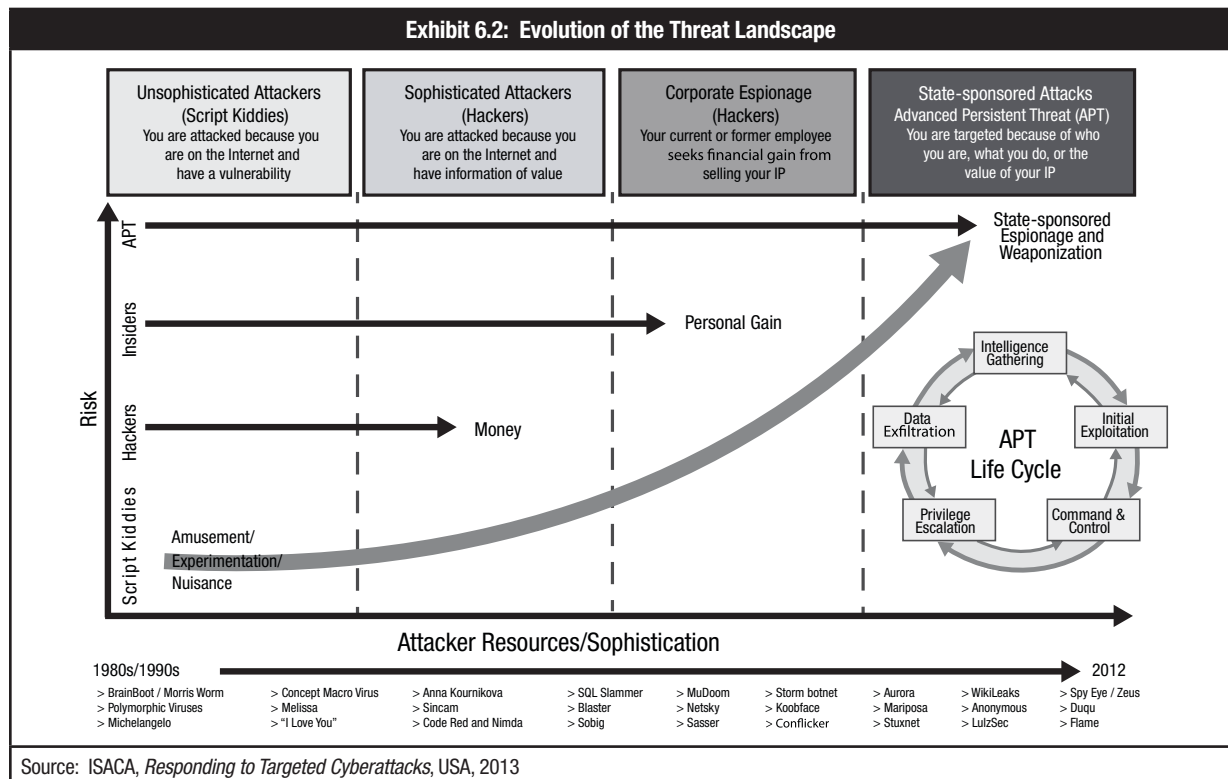
- Threat agents are more sophisticated in their attacks and use of tools.
- Attack patterns are now being applied to mobile devices. This is of particular concern for mobile and other small digital devices that are interconnected and often have poor security controls.
- Multiple nation states have the capabilities to infiltrate government and private targets (cyberwarfare).
- Cloud computing results in large concentrations of data within a small number of facilities, which are likely targets for attackers.
- Social networks have become a primary channel for communication, knowledge collection, marketing and dissemination of information. Attackers can misuse social networks to gain personal data and promulgate misinformation.
- Big data refers to large collections of structured and unstructured data and the usage of large infrastructure, applications, web services and devices. The popularity of big data as an asset allows for the potential for big data breaches.



Page intentionally left blank

TOPIC 2—ADVANCED PERSISTENT THREATS

Advanced persistent threats (APTs) are relatively new phenomena for many organizations. Although the motives behind them are not entirely new, the degree of planning, resources employed and techniques used in APT attacks are unprecedented. These threats demand a degree of vigilance and a set of countermeasures that are above and beyond those routinely used to counter everyday security threats from computer hackers, viruses or spammers.⁴⁶ Exhibit 6.2 shows the evolution of the threat landscape.



DEFINING APTS

It should be noted that not everyone agrees on precisely what constitutes an APT. Many experts regard it as nothing new. Some see it as simply the latest evolution in attack techniques that have been developing over many years. Others claim the term is misleading, pointing out that many attacks classed as APTs are not especially clever or novel. A few define it in their own terms, for example, as an attack that is professionally managed, or one that follows a particular modus operandi, or one launched by a foreign intelligence service, or perhaps one that targets and relentlessly pursues a specific enterprise.

In fact, all of these descriptions are true. The defining characteristics of an APT are very simple: An **APT** is a targeted threat that is composed of various complex attack vectors and can remain undetected for an extended period of time. It is a specifically targeted and sophisticated attack that keeps coming after the victim. Unlike many other types of criminal acts, it is not easily deflected by a determined, defensive response. An example of an APT is spear phishing, where social engineering techniques are used to masquerade as a trusted party to obtain important information such as passwords from the victim.

⁴⁶ ISACA, *Advanced Persistent Threats: How to Manage the Risk to Your Business*, USA, 2013

APT CHARACTERISTICS

Attacks of this kind are quite different from the ones that enterprises might have experienced in the past. Most organizations have at some point encountered one or more opportunistic attacks from small-time criminals, hackers or other mischief makers. But most APT attacks originate from more sinister sources. They are often the work of professional teams employed by organized crime groups, determined activists or governments. This means they are likely to be well-planned, sophisticated, well-resourced and potentially more damaging.

APT attacks vary significantly in their approach; however, they share the following characteristics:

- **Well-researched**—APT agents thoroughly research their targets, plan their use of resources and anticipate countermeasures.
- **Sophisticated**—APT attacks are often designed to exploit multiple vulnerabilities in a single attack. They employ an extensive framework of attack modules designed for executing automated tasks and targeting multiple platforms.
- **Stealthy**—APT attacks often go undetected for months and sometimes years. They are unannounced and disguise themselves using obfuscation techniques or hide in out-of-reach places.
- **Persistent**—APT attacks are long-term projects with a focus on reconnaissance. If one attack is successfully blocked, the perpetrators respond with new attacks. And, they are always looking for methods or information to launch future attacks.

APT TARGETS

APTs target companies of all sizes across all sectors of industry and all geographic regions that contain high-value assets. Staff of all levels of seniority, ranging from administrative assistants to chief executives, can be selected as a target for a spear-phishing attack. Small companies and contractors might be penetrated because they are a supplier of services to a targeted victim. Individuals might be selected if they are perceived to be a potential stepping stone to help gain access to the ultimate target.

No industry with valuable secrets or other sources of commercial advantage that can be copied or undermined through espionage is safe from an APT attack. No enterprise that controls money transfers, processes credit card data or stores personally identifiable data on individuals can be sheltered from criminal attacks. Likewise, no industry that supplies or supports critical national infrastructure is immune from an intrusion by cyberwarriors.

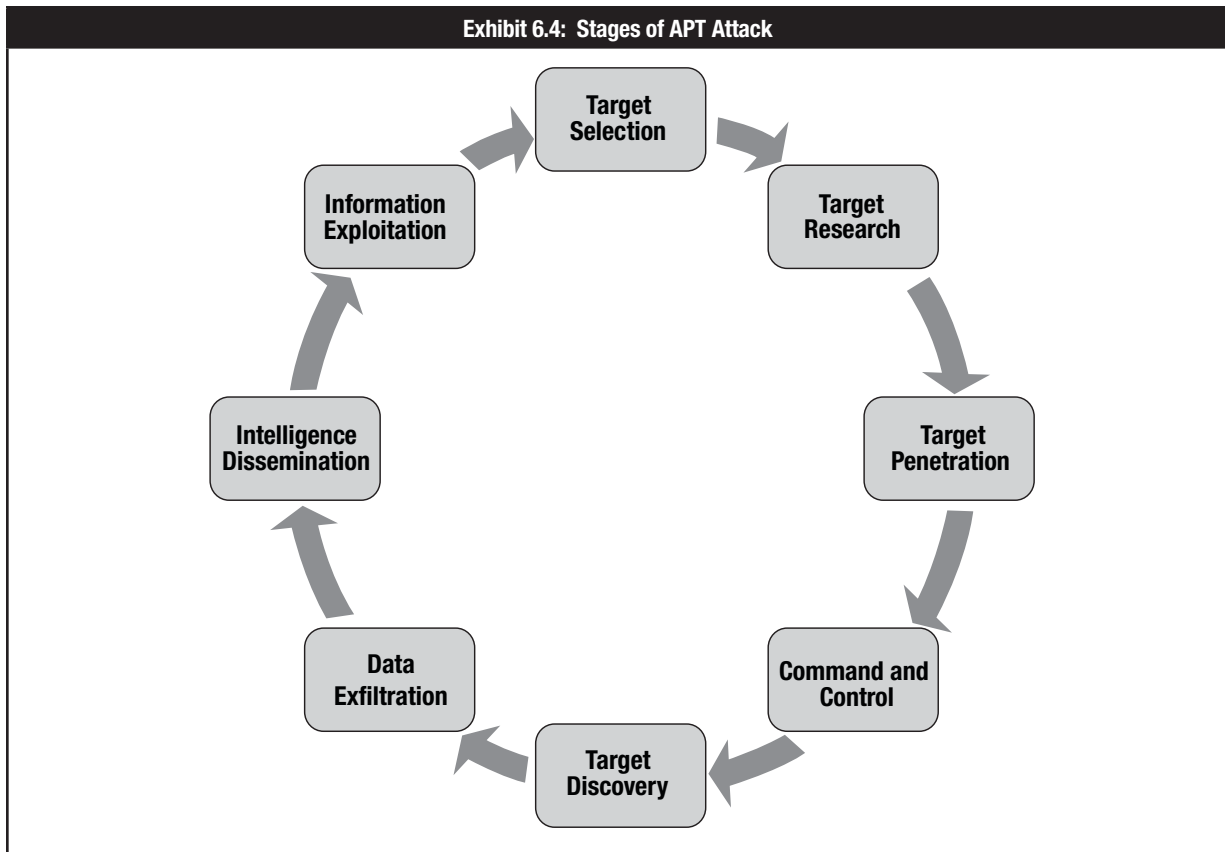
APT attacks often encompass third-party organizations delivering services to targeted enterprises. Third-party suppliers can be perceived by an attacker as the weakest link of large companies and government departments because they are generally less well protected. No matter how effective a company's external perimeter security might be, it can be of limited value unless extended across its supply chain.

Exhibit 6.3 lists the primary actors behind APT threats. It sets out their overall goals as well as the potential business impact of their attacks.

Exhibit 6.3: APT Types and Impacts		
Threat	What They Seek	Business Impact
Intelligence agencies	Political, defense or commercial trade secrets	Loss of trade secrets or commercial, competitive advantage
Criminal groups	Money transfers, extortion opportunities, personal identity information or any secrets for potential onward sale	Financial loss, large-scale customer data breach or loss of trade secrets
Terrorist groups	Production of widespread terror through death, destruction and disruption	Loss of production and services, stock market irregularities, and potential risk to human life
Activist groups	Confidential information or disruption of services	Major data breach or loss of service
Armed forces	Intelligence or positioning to support future attacks on critical national infrastructure	Serious damage to facilities in the event of a military conflict

STAGES OF AN APT ATTACK

Even though no two APT attacks are exactly alike, they often follow a similar life cycle, shown in **exhibit 6.4**. They start with intelligence gathering, which includes selecting and researching their target, planning the attack and collecting and analyzing data from an initial penetration. The attacker then establishes command and control, collecting targeted information. That information is then exfiltrated to the attacker's location to be disseminated or exploited.



Page intentionally left blank

TOPIC 3—MOBILE TECHNOLOGY—VULNERABILITIES, THREATS AND RISK

Security for mobile technology is a function of the risk associated with its use. Despite positive and negative impacts, security teams must deal with the risk common to all mobile devices and applications. **Exhibit 6.5** provides a number of illustrative examples.

Exhibit 6.5: Mobile Technology Vulnerabilities, Threats and Risk ⁴⁷		
Vulnerability	Threat	Risk
Information travels across wireless networks that are often less secure than wired networks.	Malicious outsiders can do harm to the enterprise.	Information interception resulting in a breach of sensitive data, damage to enterprise reputation, compromised adherence to regulation or legal action
Mobility provides the users with the opportunity to leave enterprise boundaries, thereby eliminating many security controls.	Mobile devices cross boundaries and network perimeters, carrying malware, and can bring this malware into the enterprise network.	Malware propagation, which can result in data leakage, data corruption and unavailability of necessary data; physical theft
Bluetooth (BT) technology makes it very convenient for many users to have hands-free conversations; however, it is often left on and is then discoverable.	Hackers can discover the device and then launch an attack.	Device corruption, lost data, call interception, possible exposure of sensitive information
Unencrypted information is stored on the device.	In the event that a malicious outsider intercepts data in transit or steals a device, or if the employee loses the device, the data are readable and usable.	Exposure of sensitive data, resulting in damage to the enterprise, customers or employees
Lost data may affect employee productivity.	Mobile devices may be lost or stolen due to their portability. Data on these devices are not always backed up.	Workers dependent on mobile devices unable to work in the event of broken, lost or stolen devices, and data that are not backed up
The device has no authentication requirements applied.	If the device is lost or stolen, outsiders can access the device and all its data.	Data exposure, resulting in damage to the enterprise and liability and regulation issues
The enterprise is not managing the device.	If no mobile device strategy exists, employees may choose to bring in their own, unsecured devices. While these devices may not connect to the virtual private network (VPN), they may interact with emails or store sensitive documents.	Data leakage, malware propagation, unknown data loss in the event of device loss or theft
The device allows installation of unverified/unsigned third-party applications.	Applications may carry malware that propagates Trojan horses or viruses. The applications may also transform the device into a gateway for malicious outsiders to enter the enterprise network.	Malware propagation, data leakage, intrusion to the enterprise network

This illustrative list, while not exhaustive, nevertheless shows that mobile technology presents risk that needs to be managed through technical and organizational steps. The following sections examine risk categories in more detail.

PHYSICAL RISK

Mobile devices tend to be small, by definition. They are easily lost (or stolen), particularly in public areas. This increases the general physical risk, given that advanced smartphones are often seen as interesting targets for pickpockets. As users increasingly rely on their mobile devices, loss or theft is more likely to create disruptive conditions and may leave employees unable to work for prolonged periods of time.

⁴⁷ ISACA, *Securing Mobile Devices Using COBIT 5 for Information Security*, USA, 2012

The security consequences of device loss are more serious. For example, unprotected and transient data, such as lists of calls, texts or calendar items, may be compromised, allowing attackers to harvest large amounts of data. With criminal intent, perpetrators may be able to recover deleted data and a history of the use of the mobile device.

An additional significant risk is identity theft, which may occur as a result of obtaining and analyzing a stolen or lost mobile device. Many mainstream OSs for smart devices mandate the link to a user account with the provider, thus greatly increasing the risk of losing one's digital identity with the actual device.

The link between device and account is sometimes subject to even greater risk when value-added services are offered as an add-on to the existing user account. Some OSs offer a "secure" repository for enriched user data ranging from personal information to automated credit card storage and payment functionality. The risk of entrusting such sensitive data to a mobile device ("all in one place") should not be neglected.

From a security management perspective, several attempts have been undertaken to prevent, or at least mitigate, the threat of device loss or theft:

- Cell-based tracking and locating the device
- Remote shutdown/wipe capabilities
- Remote SIM card lock capabilities

While these facilities do provide a degree of security, they still leave a window of exposure to attackers exploring the device, possibly using analytical tools that will circumvent the standard OS features. This threat is particularly significant because enforcing strong passwords and encryption on mobile devices may be restricted due to OS limitations.

ORGANIZATIONAL RISK

As with many other technologies, mobile devices have rapidly pervaded enterprises at all levels. They are now available to most users, either through corporate provisioning or bring your own device (BYOD) schemes. In terms of data, information and knowledge that exist across the enterprise, many users have privileged access that is often replicated on their mobile devices.

Whereas corporate PC environments have been the target of hardening and protective measures for many years, mobile devices and their comparatively weak security mechanisms are more difficult to manage and control. As an example, C-suite and senior managers will often be heavy mobile users, and any successful compromise of their devices could certainly cause major damage.

Another important organizational risk arises from the growing complexity and diversity of common mobile devices. Whereas early cell phones required no more than the most basic knowledge about how to use a keyboard, smartphones offer anything from simple telephony to highly complex applications. Even for experienced users, this level of complexity may be challenging, and many smartphones are thought to be conducive to human error and user-based security issues. Examples such as inadvertent data roaming or involuntary GPS tagging show how many users simply do not understand the extended features of their devices.

At the same time, the rapid succession of new generations of hardware requires constant adaptation on the part of users and enterprises. The comparatively long systems management cycles found in larger enterprises may cause difficulties when facing the usual turnaround time of approximately two years for new mobile devices. Likewise, the life span of mobile OSs and applications is becoming much shorter.

The resulting risk to users is aggravated by the fact that few enterprises offer formal or informal training for mobile device use. Users are literally left on their own when it comes to adopting and using new technology and new services.

TECHNICAL RISK

Activity Monitoring and Data Retrieval

In general, mobile devices use service-based OSs with the ability to run multiple services in the background. While early variants of these OSs were fairly transparent and controllable in terms of activity, more recent versions show a tendency to “simplify” the user interface by restricting the user’s ability to change low-level settings. However, monitoring and influencing activity is a core functionality of spyware and malware, as is covert data retrieval. Data can be intercepted in real time as they are being generated on the device. Examples include sending each email sent on the device to a hidden third-party address, letting an attacker listen in on phone calls or simply opening microphone recording. Stored data such as a contact list or saved email messages can also be retrieved. **Exhibit 6.6** shows an overview of targets and the corresponding risk.

Exhibit 6.6: Activity Monitoring and Data Retrieval Risk ⁴⁸	
Target	Risk
Messaging	Generic attacks on SMS text, MMS-enriched transmission of text and contents
	Retrieval of online and offline email contents
	Insertion of service commands by SMS cell broadcast texts
	Arbitrary code execution via SMS/MMS
	ML-enabled SMS text or email
	Redirect or phishing attacks by HTML-enabled SMS text or email
Audio	Covert call initiation, call recording
	Open microphone recording
Pictures/Video	Retrieval of still pictures and videos, for instance, by piggybacking the usual “share” functionality in most mobile apps
	Covert picture or video taking and sharing, including traceless wiping of such material
Geolocation	Monitoring and retrieval of GPS positioning data, including date and time stamps
Static data	Contact list, calendar, tasks, notes retrieval
History	Monitoring and retrieval of all history files in the device or on SIM card (calls, SMS, browsing, input, stored passwords, etc.)
Storage	Generic attacks on device storage (hard disk or solid state disk [SSD]) and data replicated there

In practice, the risk has already materialized for most common device platforms and OSs.

In combination with attacks on connectivity, the risk of activity monitoring/influencing and covert data retrieval is significant.

UNAUTHORIZED NETWORK CONNECTIVITY

Most spyware or malware—once placed on a mobile device—will require one or more channels for communicating with the attacker. While “sleepy” malware may have a period of latency and remain dormant for weeks or months, data and information harvested will eventually need to be transmitted from the mobile device to another destination.

Similarly, the command and control functionality often found in malware requires a direct link between the mobile device and the attacker, particularly when commands and actions are to be executed and monitored in real time (e.g., eavesdropping or covert picture taking). **Exhibit 6.7** shows the most common vectors for unauthorized network connectivity and the typical risk that comes with them.

⁴⁸ ISACA, *Securing Mobile Devices Using COBIT 5 for Information Security*, USA, 2012

Exhibit 6.7: Unauthorized Connectivity Risk⁴⁹

Vector	Risk
Email	Simple to complex data transmission (including large files)
SMS	Simple data transmission, limited command and control (service command) facility
H P get/post	Generic attack vector for browser-based connectivity, command and control
CP/UDP socket	Lower-level attack vector for simple to complex data transmission
DNS exfiltration	Lower-level attack vector for simple to complex data transmission, slow but difficult to detect
Bluetooth	Simple to complex data transmission, profile-based command and control facility, generic attack vector for close proximity
WLAN/WiMAX	Generic attack vector for full command and control of target, equivalent to wired network

These vectors of connectivity may be used in combination, for example, when browser-based command and control functionality is used via Bluetooth in a close-proximity scenario. An important point to note is the relative anonymity of wireless connectivity vectors, particularly Bluetooth and WLAN/WiMAX. The risk of ad hoc attacks on mobile devices is significantly higher when anonymous connectivity is provided by third parties, for example, in airport lounges or coffee shops.

WEB VIEW/USER INTERFACE (UI) IMPERSONATION

While most mobile devices support all relevant browser protocols, the presentation to the user is modified by the mobile service provider. This is mainly done to optimize viewing on small screens. However, web pages viewed on a typical (smaller) device often show “translated” content, including modifications to the underlying code.

In UI impersonation, malicious apps present a UI that impersonates the native device or that of a legitimate app. When the victim supplies authentication credentials, these are transmitted to the attacker. This is conducive to impersonation attacks that are similar to generic phishing.

Typical web view applications allow attacks on the proxy level (phishing credentials while proxying to a legitimate web site) and on the presentation level (fake web site presented through mobile web view). This type of risk is prevalent in banking applications where several cases of malware have been documented. Given the attractiveness of payment data and user credentials, web view and impersonation risk is likely to increase in the future.

SENSITIVE DATA LEAKAGE

With the emergence of new work patterns and the need for decentralized data availability, mobile devices often store large amounts of sensitive data and information. As an example, confidential presentations and spreadsheets are often displayed directly from a smart mobile device rather than using a laptop computer.

The amount of storage space found on many devices is growing and, on average, almost any device will soon be capable of storing several gigabytes of data. This greatly increases the risk of data leakage, particularly when mobile devices store replicated information from organizational networks. This is often the case when standard email and calendar applications automatically replicate emails with attachments, or mobile OSs offer the convenience of replicating selected folders between mobile device and desktop device. **Exhibit 6.8** shows the information targeted and possible risk.

⁴⁹ *Ibid.*

Exhibit 6.8: Sensitive Data Leakage Risk ⁵⁰	
Type of Information	Risk
Identity	International Mobile Equipment Identity (IMEI), manufacturer device ID, customized user information
	Hardware/firmware and software release stats, also disclosing known
	weaknesses or potential zero-day exploits
Credentials	User names and passwords, keystrokes
	Authorization tokens, certificates (S/MIME, PGP, etc.)
Location Files	GPS coordinates, movement tracking, location/behavioral inference
	All files stored at operating system/file system level

Sensitive data leakage can be inadvertent or can occur through side channel attacks. Even a legitimate application may have flaws in the usage of the device. As a result, information and authentication credentials may be exposed to third parties. Depending on the nature of the information leaked, additional risk may arise.

Mobile devices provide a fairly detailed picture of what their users do, where they are and their preferences. Side channel attacks over prolonged periods of time allow the building of a detailed user profile in terms of movements, behavior and private/business habits. Users who may be considered at risk may require additional physical protection.

Sensitive data leakage allowing the prediction of users' behavior patterns and activities is becoming more significant as many users prefer to set their devices to "always on" mode to benefit from legitimate services such as navigation or local points of interest.

UNSAFE SENSITIVE DATA STORAGE

While most mobile OSs offer protective facilities such as storage encryption, many applications store sensitive data such as credentials or tokens as plaintext. Furthermore, data stored by the user is often replicated without encryption, and many standardized files such as Microsoft Office® presentations and spreadsheets are stored unencrypted for quick access and convenience.

Another risk associated with unsafe storage of sensitive data is the use of public cloud services for storage purposes. Many mobile device providers have introduced cloud services that offer a convenient way of storing, sharing and managing data in a public cloud. However, these services target the private consumer, and the security functionality would not normally stand up to organizational (corporate) requirements.

This risk has another dimension: when data and information are stored or replicated in public clouds, terms and conditions generally rule out any form of responsibility or liability, requiring the user to make individual security arrangements. In an organizational context, these limitations may increase the risk of sensitive data storage, particularly in a BYOD scenario.

UNSAFE SENSITIVE DATA TRANSMISSION

Mobile devices predominantly rely on wireless data transmission, except for the few cases when they are physically connected to a laptop or desktop computer. As outlined previously, these transmissions create a risk of unauthorized network connectivity, particularly when using WLAN/WiMAX or Bluetooth at close proximity. As a new transmission protocol, NFC increases the risk at very short range, for example, when transmitting payment data over a distance of several inches.

Even if data at rest is protected by encryption and other means, transmission is not always encrypted. Mobile users are likely to use unsecured public networks frequently, and the large number of known attacks on WLAN and Bluetooth are a significant risk.

⁵⁰ *Ibid.*

Automatic network recognition, a common feature in mobile OSs, may link to WLANs available in the vicinity, memorizing Service Set Identifiers (SSIDs) and channels. For many major providers of public WLANs, these SSIDs are identical across the world. This is intentional and convenient; however, the risk of an evil twin attack increases with the use of generic names that the mobile device will normally accept without verification.

While many enterprises have implemented VPN solutions for their users, these may not be workable on mobile devices that are used both for business and personal transactions. Given the relative complexity of configuring and activating VPN on mobile devices, users may deactivate protected data transmission to access another service that does not support VPN. Even for split-tunnel VPN installations—offering a VPN to the enterprise while keeping the open link to the public network—the risk of an at-source attack is still high.

DRIVE-BY VULNERABILITIES

In contrast to desktop or laptop computers, mobile devices offer only rudimentary applications for office-based work. In many cases, device size restricts the display and edit capabilities. As a consequence, typical word processing, spreadsheet and presentation software on mobile devices tends to be optimized for opening and reading rather than editing information. Similarly, popular document formats such as Adobe® portable document format (PDF) are implemented, more or less, as a read-only solution designed for a cursory read rather than full-scale processing.

At the same time, it has become common practice to insert active content into documents and PDF files. These may be full hyperlinks or shortened links, or embedded documents and macros. This is known as an attack vector for malware and other exploits.

The restricted nature of mobile device applications leads to an increased risk of drive-by attacks because these apps may not recognize malformed links and omit the usual warnings that users could expect from the desktop versions of Microsoft Office or PDF applications.

In practice, these vulnerabilities create risk and a number of threats for end users, for example, the insertion of illegal material, inadvertent use of “premium” services via SMS/MMS or bypassing two-factor authentication mechanisms.

TOPIC 4—CONSUMERIZATION OF IT AND MOBILE DEVICES

CONSUMERIZATION OF IT

Mobile devices have had a profound impact on the way business is conducted and on behavior patterns in society. They have greatly increased productivity and flexibility in the workplace, to the extent that individuals are now in a position to work from anywhere at any given time. Likewise, the computing power of smart devices has enabled them to replace desktop PCs and laptops for many business applications.

Manufacturers and service providers alike have created both new devices and new business models such as mobile payments or subscription downloads using a pay-as-you-go model. Simultaneously, consumerization of devices has relegated enterprises, at least in some cases, to followers rather than opinion leaders in terms of which devices are used and how they are used.

The impact of using mobile devices falls into two broad categories:

- The hardware itself has been developed to a level at which computing power and storage are almost equivalent to PC hardware. In accordance with Moore's Law, a typical smartphone represents the equivalent of what used to be a midrange machine a decade ago.
- New mobile services have created new business models that are changing organizational structures and society as a whole.

Consumerization is not limited to devices. New, freely available applications and services provide better user experiences for things like note-taking, video conferencing, email and cloud storage than their respective corporate-approved counterparts. Instead of being provided with company-issued devices and software, employees are using their own solutions that better fit with their lifestyle, user needs and preferences.

BYOD

General mobility and location-independent accessibility have enhanced business practices and have allowed enterprises to focus on core activities while reducing the amount of office space used. For employees, mobile devices have brought greater flexibility, for example, in bring your own device (BYOD) scenarios.

The idea of using privately owned mobile devices has quickly taken hold as a concept, and many enterprises are now facing a new obstacle: when centralized procurement and provisioning of mobile devices are slow or cumbersome, many users have developed the expectation of simply "plugging in" their own units to achieve productivity in a quick and pragmatic manner.

The obvious downside is the proliferation of devices with known (or unknown) security risk, and the formidable challenge of managing device security against several unknowns. However, as the workforce changes, there are clear signs that BYOD is becoming an important job motivation factor, because employees are no longer willing to accept technology restrictions.

While BYOD may be seen as an enabler, it has also brought a number of new risk areas and associated threats. These need to be balanced with the advantages of mobile device use, taking into account the security needs of the individual as well as the enterprise. Therefore, security management should address both the innovative potential and the risk and threats of flexible device use because it is unlikely that restrictions or bans on certain types of devices will be effective even in the medium term. Indeed, the fact that some enterprises have attempted a ban on certain devices has allowed the prohibited technology to gain a foothold within the corporate landscape—particularly if that technology is already widely accepted among private users. As a result, enterprises with a restrictive perspective on innovative devices will always be behind the threat curve and thus exposed to unnecessary risk. The pros and cons of BYOD are listed in **exhibit 6.9**.

Exhibit 6.9: Pros and Cons of BYOD

Pros	Cons
<ul style="list-style-type: none">• Shifts costs to user• Worker satisfaction• More frequent hardware upgrades• Cutting-edge technology with the latest features and capabilities	<ul style="list-style-type: none">• IT loss of control• Known or unknown security risk• Acceptable Use Policy is more difficult to implement• Unclear compliance and ownership of data

TOPIC 5—CLOUD AND DIGITAL COLLABORATION

According to NIST and the Cloud Security Alliance (CSA), **cloud computing** is defined as a “model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”

Cloud computing offers enterprises a way to save on the capital expenditure associated with traditional methods of managing IT. Common platforms offered in the cloud include Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Virtualization and service-oriented architectures (SOAs) act as key enablers behind the scenes. Though attractive, cloud computing is not without its own set of risk, first and foremost of which is the safety and security of the data that are entrusted in the care of cloud providers.⁵¹

Similar to the use of any third-party contract, it is important for organizations to ensure that their cloud provider has a security system in place equivalent to or better than the organization’s own security practice. Many cloud providers are ISO27001 or FIPS 140-2 certified. In addition, organizations can request audits of the cloud provider. The security audits should cover the facilities, networks, hardware and operating systems within the cloud infrastructure.

RISK OF CLOUD COMPUTING

The challenge for cloud computing is to protect data within public and private clouds as well as ensure governance, risk management and compliance are addressed across the full, integrated environment. NIST outlines the following top security risk for cloud infrastructure:

- **Loss of governance**—The client usually relinquishes some level of control to the cloud provider, which may affect security, especially if the SLAs leave a gap in security defenses.
- **Lock-in**—It can be difficult for a client to migrate from one provider to another, which creates a dependency on a particular cloud provider for service provision.
- **Isolation failure**—One characteristic of cloud computing is shared resources. Although not commonplace, the failure of mechanisms that separate storage, memory, routing and reputation between different tenants can create risk.
- **Compliance**—Migrating to the cloud may create a risk in the organization achieving certification if the cloud provider cannot provide compliance evidence.
- **Management interface compromise**—The customer management interface can pose an increased risk because it is accessed through the Internet and mediates access to larger sets of resources.
- **Data protection**—It may be difficult for clients to check the data handling procedures of the cloud provider.
- **Insecure or incomplete data deletion**—Because of the multiple tenancies and the reuse of hardware resources, there is a greater risk that data are not deleted completely, adequately, or in a timely manner.
- **Malicious insider**—Cloud architects have extremely high-risk roles. A malicious insider could cause a great degree of damage.

These risk can lead to a number of different threat events. The CSA lists the following as the top cloud computing threats:⁵²

1. Data breaches
2. Data loss
3. Account hijacking
4. Insecure application programming interfaces (APIs)
5. Denial-of-service (DoS)
6. Malicious insiders
7. Abuse of cloud services
8. Insufficient due diligence
9. Shared technology issues

⁵¹ ISACA, *Top Business/Technology Issues Survey Results*, USA, 2011

⁵² Cloud Security Alliance (CSA), *The Notorious Nine: Cloud Computing Top Threats in 2013*, 2013

WEB APPLICATION RISK

In implementing and adapting their cloud-based strategies, enterprises tend to include SaaS offerings, sometimes extending this to critical business processes and related applications. Despite the fact that these service offerings may bring business advantages, they nevertheless generate data-in-flow vulnerabilities that may be exploited by cybercrime and cyberwarfare. The resulting risk is exacerbated by the fact that many vendors and hardware providers (e.g., for mobile devices), supply cloud-based freeware designed to enforce user loyalty. This is often the case for data synchronization, handling of popular file types such as music or pictures, and personal information such as email and calendar entries.

The application layer within the overall IT environment is particularly susceptible to zero-day exploits, as witnessed by many practical examples. Even major software vendors frequently update and patch their applications, but new attack vectors using such applications emerge almost on a daily basis. In terms of cybercrime and cyberwarfare, the market for zero-day exploits is a lively one, and the time span from discovery to recognition and remediation is increasing.

Likewise, the propagation of complex malware has been growing over the past several years. From a cybercrime and cyberwarfare perspective, recent specimens of malware show a higher level of sophistication and persistence than the basic varieties used by opportunistic attackers. While software vendors are quick to address malware in terms of recognition and removal, there is a significant residual risk of malware becoming persistent in target enterprises.

Secondary malware attacks—where APTs make use of already installed simple malware—are often successful where the environmental conditions are conducive to user error or lack of vigilance, namely in home user or traveling user scenarios. In practice, removal of the primary malware (a fairly simple process) often allays any further suspicion and causes users and security managers to be lulled into a false sense of security. The secondary and very complex malware may have infiltrated the system, presenting a known and simple piece of primary malware as bait.

BENEFITS OF CLOUD COMPUTING

Although cloud computing is attractive to attackers because of the massive concentrations of data, cloud defenses can be more robust, scalable and cost-effective. The European Union Agency for Network and Information Security (ENISA) provides the following top security benefits of cloud computing:

- **Market drive**—Because security is a top priority for most cloud customers, cloud providers have a strong driver for increasing and improving their security practices.
- **Scalability**—Cloud technology allows for the rapid reallocation of resources, such as those for filtering, traffic shaping, authentication and encryption, to defensive measures.
- **Cost-effective**—All types of security measures are cheaper when implemented on a large scale. The concentration of resources provides for cheaper physical perimeter and physical access control and easier and cheaper application of many security-related processes.
- **Timely and effective updates**—Updates can be rolled out rapidly across a homogeneous platform.
- **Audit and evidence**—Cloud computing can provide forensic images of virtual machines, which results in less downtime for forensic investigations.

Although there are many benefits of cloud computing, there is risk involved as well. **Exhibit 6.10** lists the benefits and risk of cloud computing.

Exhibit 6.10: Benefits and Risk of Cloud Computing

Benefits	Risk
<ul style="list-style-type: none"> • Market drive for the cloud • Scalability • Cost-effective implementation • Timely and effective updates • Audit and evidence capabilities 	<ul style="list-style-type: none"> • Loss of governance • Lock-in to one provider • Isolation failure • Compliance • Data protection • Customer management interface compromise • Insecure or incomplete data deletion • Malicious insider

Page intentionally left blank

SECTION 6—KNOWLEDGE CHECK

1. _____ is defined as “a model for enabling convenient, on-demand network access to a shared pool of configurable resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management or service provider interaction.”
 - a. Software as a Service (SaaS)
 - b. Cloud computing
 - c. Big data
 - d. Platform as a Service (PaaS)
2. Select all that apply. Which of the following statements about advanced persistent threats (APTs) are true?
 - a. APTs typically originate from sources such as organized crime groups, activists or governments.
 - b. APTs use obfuscation techniques that help them remain undiscovered for months or even years.
 - c. APTs are often long-term, multi-phase projects with a focus on reconnaissance.
 - d. The APT attack cycle begins with target penetration and collection of sensitive information.
 - e. Although they are often associated with APTs, intelligence agencies are rarely the perpetrators of APT attacks.
3. Smart devices, BYOD strategies and freely available applications and services are all examples of:
 - a. The reorientation of technologies and services designed around the individual end user.
 - b. The primacy of external threats to business enterprises in today’s threat landscape.
 - c. The stubborn persistence of traditional communication methods.
 - d. The application layer’s susceptibility to APTs and zero-day exploits.
4. Choose three. Which types of risk are typically associated with mobile devices?
 - a. Organizational risk
 - b. Compliance risk
 - c. Technical risk
 - d. Physical risk
 - e. Transactional risk
5. Which three elements of the current threat landscape have provided increased levels of access and connectivity, and therefore increased opportunities for cybercrime?
 - a. Text messaging, Bluetooth technology and SIM cards
 - b. Web applications, botnets and primary malware
 - c. Financial gains, intellectual property and politics
 - d. Cloud computing, social media and mobile computing

Page intentionally left blank



CYBERSECURITY NEXUS

Appendices

Appendix A—Knowledge Statements

Appendix B—Glossary

Appendix C—Knowledge Check Answers

Appendix D—Additional Resources

Page intentionally left blank

APPENDIX A—KNOWLEDGE STATEMENTS

DOMAIN 1: CYBERSECURITY CONCEPTS

- 1.1 Knowledge of cybersecurity principles used to manage risk related to the use, processing, storage and transmission of information or data
- 1.2 Knowledge of security management
- 1.3 Knowledge of risk management processes, including steps and methods for assessing risk
- 1.4 Knowledge of threat actors (e.g., script kiddies, non-nation state sponsored, and nation state sponsored)
- 1.5 Knowledge of cybersecurity roles
- 1.6 Knowledge of common adversary tactics, techniques, and procedures (TTPs)
- 1.7 Knowledge of relevant laws, policies, procedures and governance requirements
- 1.8 Knowledge of cybersecurity controls

DOMAIN 2: CYBERSECURITY ARCHITECTURE PRINCIPLES

- 2.1 Knowledge of network design processes, to include understanding of security objectives, operational objectives and trade-offs
- 2.2 Knowledge of security system design methods, tools and techniques
- 2.3 Knowledge of network access, identity and access management
- 2.4 Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption)
- 2.5 Knowledge of network security architecture concepts, including topology, protocols, components and principles (e.g., application of defense in depth)
- 2.6 Knowledge of malware analysis concepts and methodology
- 2.7 Knowledge of intrusion detection methodologies and techniques for detecting host- and network-based intrusions via intrusion detection technologies
- 2.8 Knowledge of defense in depth principles and network security architecture
- 2.9 Knowledge of encryption algorithms (e.g., Internet Protocol Security [IPSEC], Advanced Encryption Standard [AES], Generic Routing Encapsulation [GRE])
- 2.10 Knowledge of cryptography
- 2.11 Knowledge of encryption methodologies
- 2.12 Knowledge of how traffic flows across the network (i.e., transmission and encapsulation)
- 2.13 Knowledge of network protocols (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP], Dynamic Host Configuration Protocol [DHCP]), and directory services (e.g., domain name system [DNS])

DOMAIN 3: SECURITY OF NETWORK, SYSTEM, APPLICATION AND DATA

- 3.1 Knowledge of vulnerability assessment tools, including open source tools, and their capabilities
- 3.2 Knowledge of basic system administration, network and operating system hardening techniques.
- 3.3 Knowledge of risk associated with virtualizations
- 3.4 Knowledge of penetration testing
- 3.5 Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring) and tools
- 3.6 Knowledge of remote access technology
- 3.7 Knowledge of UNIX command line
- 3.8 Knowledge of system and application security threats and vulnerabilities
- 3.9 Knowledge of system life cycle management principles, including software security and usability
- 3.10 Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance and reliability
- 3.11 Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, cover channel, replay, return-oriented attacks, malicious code)
- 3.12 Knowledge of social dynamics of computer attackers in a global context
- 3.13 Knowledge of secure configuration management techniques

- 3.14 Knowledge of capabilities and applications of network equipment including hubs, routers, switches, bridges, servers, transmission media and related hardware
- 3.15 Knowledge of communication methods, principles and concepts that support the network infrastructure
- 3.16 Knowledge of the common networking protocols (e.g., Transmission Control Protocol and Internet Protocol [TCP/IP]) and services (e.g., web, email, domain name system [DNS]) and how they interact to provide network communications
- 3.17 Knowledge of different types of network communication (e.g., local area network [LAN], wide area network [WAN], metropolitan area network [MAN], wireless local area network [WLAN], wireless wide area network [WWAN])
- 3.18 Knowledge of virtualization technologies and virtual machine development and maintenance
- 3.19 Knowledge of application security (e.g., system development life cycle [SDLC], vulnerabilities, best practices)
- 3.20 Knowledge of risk threat assessment

DOMAIN 4: INCIDENT RESPONSE

- 4.1 Knowledge of incident categories for responses
- 4.2 Knowledge of business continuity/disaster recovery
- 4.3 Knowledge of incident response and handling methodologies
- 4.4 Knowledge of security event correlation tools
- 4.5 Knowledge of processes for seizing and preserving digital evidence (e.g., chain of custody)
- 4.6 Knowledge of types of digital forensics data
- 4.7 Knowledge of basic concepts and practices of processing digital forensic data
- 4.8 Knowledge of anti-forensics tactics, techniques and procedures (TTPS)
- 4.9 Knowledge of common forensic tool configuration and support applications (e.g., VMware®, Wireshark®)
- 4.10 Knowledge of network traffic analysis methods
- 4.11 Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files

DOMAIN 5: SECURITY OF EVOLVING TECHNOLOGY

- 5.1 Knowledge of emerging technology and associated security issues, risk and vulnerabilities
- 5.2 Knowledge of risk associated with mobile computing
- 5.3 Knowledge of cloud concepts around data and collaboration
- 5.4 Knowledge of risk of moving applications and infrastructure to the cloud
- 5.5 Knowledge of risk associated with outsourcing
- 5.6 Knowledge of supply chain risk management processes and practices

APPENDIX B—GLOSSARY

A

Acceptable interruption window—The maximum period of time that a system can be unavailable before compromising the achievement of the enterprise's business objectives.

Acceptable use policy—A policy that establishes an agreement between users and the enterprise and defines for all parties' the ranges of use that are approved before gaining access to a network or the Internet.

Access control list (ACL)—An internal computerized table of access rules regarding the levels of computer access permitted to logon IDs and computer terminals. Also referred to as access control tables.

Access path—The logical route that an end user takes to access computerized information. Typically includes a route through the operating system, telecommunications software, selected application software and the access control system.

Access rights—The permission or privileges granted to users, programs or workstations to create, change, delete or view data and files within a system, as defined by rules established by data owners and the information security policy.

Accountability—The ability to map a given activity or event back to the responsible party.

Advanced Encryption Standard (AES)—A public algorithm that supports keys from 128 bits to 256 bits in size.

Advanced persistent threat (APT)—An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives using multiple attack vectors (NIST SP800-61).

The APT:

1. Pursues its objectives repeatedly over an extended period of time
2. Adapts to defenders' efforts to resist it
3. Is determined to maintain the level of interaction needed to execute its objectives

Adversary—A threat agent.

Adware—A software package that automatically plays, displays or downloads advertising material to a computer after the software is installed on it or while the application is being used. In most cases, this is done without any notification to the user or without the user's consent. The term adware may also refer to software that displays advertisements, whether or not it does so with the user's consent; such programs display advertisements as an alternative to shareware registration fees. These are classified as adware in the sense of advertising supported software, but not as spyware. Adware in this form does not operate surreptitiously or mislead the user, and it provides the user with a specific service.

Alert situation—The point in an emergency procedure when the elapsed time passes a threshold and the interruption is not resolved. The enterprise entering into an alert situation initiates a series of escalation steps.

Alternate facilities—Locations and infrastructures from which emergency or backup processes are executed, when the main premises are unavailable or destroyed; includes other buildings, offices or data processing centers.

Alternate process—Automatic or manual process designed and established to continue critical business processes from point-of-failure to return-to-normal.

Analog—A transmission signal that varies continuously in amplitude and time and is generated in wave formation. Analog signals are used in telecommunications.

Anti-malware—A technology widely used to prevent, detect and remove many categories of malware, including computer viruses, worms, Trojans, keyloggers, malicious browser plug-ins, adware and spyware.

Antivirus software—An application software deployed at multiple points in an IT architecture. It is designed to detect and potentially eliminate virus code before damage is done and repair or quarantine files that have already been infected.

Application layer—In the Open Systems Interconnection (OSI) communications model, the application layer provides services for an application program to ensure that effective communication with another application program in a network is possible. The application layer is not the application that is doing the communication; a service layer that provides these services.

Architecture—Description of the fundamental underlying design of the components of the business system, or of one element of the business system (e.g., technology), the relationships among them, and the manner in which they support enterprise objectives.

Asset—Something of either tangible or intangible value that is worth protecting, including people, information, infrastructure, finances and reputation.

Asymmetric key (public key)—A cipher technique in which different cryptographic keys are used to encrypt and decrypt a message. See public key encryption.

Attack—An actual occurrence of an adverse event.

Attack mechanism—A method used to deliver the exploit. Unless the attacker is personally performing the attack, an attack mechanism may involve a payload, or container, that delivers the exploit to the target.

Attack vector—A path or route used by the adversary to gain access to the target (asset). There are two types of attack vectors: ingress and egress (also known as data exfiltration).

Attenuation—Reduction of signal strength during transmission.

Audit trail—A visible trail of evidence enabling one to trace information contained in statements or reports back to the original input source.

Authentication—The act of verifying the identity of a user and the user's eligibility to access computerized information. Authentication is designed to protect against fraudulent logon activity. It can also refer to the verification of the correctness of a piece of data.

Authenticity—Undisputed authorship.

Availability—Ensuring timely and reliable access to and use of information.

B

Back door—A means of regaining access to a compromised system by installing software or configuring existing software to enable remote access under attacker-defined conditions.

Bandwidth—The range between the highest and lowest transmittable frequencies. It equates to the transmission capacity of an electronic line and is expressed in bytes per second or Hertz (cycles per second).

Bastion—System heavily fortified against attacks.

Biometrics—A security technique that verifies an individual’s identity by analyzing a unique physical attribute, such as a handprint.

Block cipher—A public algorithm that operates on plaintext in blocks (strings or groups) of bits.

Botnet—A term derived from “robot network;” is a large automated and distributed network of previously compromised computers that can be simultaneously controlled to launch large-scale attacks such as a denial-of-service attack on selected victims.

Boundary—Logical and physical controls to define a perimeter between the organization and the outside world.

Bridges—Data link layer devices developed in the early 1980s to connect local area networks (LANs) or create two separate LAN or wide area network (WAN) network segments from a single segment to reduce collision domains. Bridges act as store- and-forward devices in moving frames toward their destination. This is achieved by analyzing the MAC header of a data packet, which represents the hardware address of an NIC.

Bring your own device (BYOD)—An enterprise policy used to permit partial or full integration of user-owned mobile devices for business purposes.

Broadcast—A method to distribute information to multiple recipients simultaneously.

Brute force—A class of algorithms that repeatedly try all possible combinations until a solution is found.

Brute force attack—Repeatedly trying all possible combinations of passwords or encryption keys until the correct one is found.

Buffer overflow—Occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information—which has to go somewhere—can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity. In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user’s files, change data, or disclose confidential information. Buffer overflow attacks are said to have arisen because the C programming language supplied the framework, and poor programming practices supplied the vulnerability.

Business continuity plan (BCP)—A plan used by an enterprise to respond to disruption of critical business processes. Depends on the contingency plan for restoration of critical systems.

Business impact analysis/assessment (BIA)—Evaluating the criticality and sensitivity of information assets. An exercise that determines the impact of losing the support of any resource to an enterprise, establishes the escalation of that loss over time, identifies the minimum resources needed to recover, and prioritizes the recovery of processes and the supporting system. This process also includes addressing income loss, unexpected expense, legal issues (regulatory compliance or contractual), interdependent processes, and loss of public reputation or public confidence.

C

Certificate (Certification) authority (CA)—A trusted third party that serves authentication infrastructures or enterprises and registers entities and issues them certificates.

Certificate revocation list (CRL)—An instrument for checking the continued validity of the certificates for which the certification authority (CA) has responsibility. The CRL details digital certificates that are no longer valid. The time gap between two updates is very critical and is also a risk in digital certificates verification.

Chain of custody—A legal principle regarding the validity and integrity of evidence. It requires accountability for anything that will be used as evidence in a legal proceeding to ensure that it can be accounted for from the time it was collected until the time it is presented in a court of law. Includes documentation as to who had access to the evidence and when, as well as the ability to identify evidence as being the exact item that was recovered or tested. Lack of control over evidence can lead to it being discredited. Chain of custody depends on the ability to verify that evidence could not have been tampered with. This is accomplished by sealing off the evidence, so it cannot be changed, and providing a documentary record of custody to prove that the evidence was at all times under strict control and not subject to tampering.

Checksum—A mathematical value that is assigned to a file and used to “test” the file at a later date to verify that the data contained in the file has not been maliciously changed. A cryptographic checksum is created by performing a complicated series of mathematical operations (known as a cryptographic algorithm) that translates the data in the file into a fixed string of digits called a hash value, which is then used as the checksum. Without knowing which cryptographic algorithm was used to create the hash value, it is highly unlikely that an unauthorized person would be able to change data without inadvertently changing the corresponding checksum. Cryptographic checksums are used in data transmission and data storage. Cryptographic checksums are also known as message authentication codes, integrity check-values, modification detection codes or message integrity codes.

Chief Information Security Officer (CISO)—The person in charge of information security within the enterprise.

Chief Security Officer (CSO)—The person usually responsible for all security matters both physical and digital in an enterprise.

Cipher—An algorithm to perform encryption.

Ciphertext—Information generated by an encryption algorithm to protect the plaintext and that is unintelligible to the unauthorized reader.

Cleartext—Data that is not encrypted. Also known as plaintext.

Cloud computing—Convenient, on-demand network access to a shared pool of resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Collision—The situation that occurs when two or more demands are made simultaneously on equipment that can handle only one at any given instant (Federal Standard 1037C).

Common Attack Pattern Enumeration and Classification (CAPEC)—A catalogue of attack patterns as “an abstraction mechanism for helping describe how an attack against vulnerable systems or networks is executed” published by the MITRE Corporation.

Compartmentalization—A process for protecting very high value assets or in environments where trust is an issue. Access to an asset requires two or more processes, controls or individuals.

Compliance—Adherence to, and the ability to demonstrate adherence to, mandated requirements defined by laws and regulations, as well as voluntary requirements resulting from contractual obligations and internal policies.

Compliance documents—Policies, standard and procedures that document the actions that are required or prohibited. Violations may be subject to disciplinary actions.

Computer emergency response team (CERT)—A group of people integrated at the enterprise with clear lines of reporting and responsibilities for standby support in case of an information systems emergency. This group will act as an efficient corrective control, and should also act as a single point of contact for all incidents and issues related to information systems.

Computer forensics—The application of the scientific method to digital media to establish factual information for judicial review. This process often involves investigating computer systems to determine whether they are or have been used for illegal or unauthorized activities. As a discipline, it combines elements of law and computer science to collect and analyze data from information systems (e.g., personal computers, networks, wireless communication and digital storage devices) in a way that is admissible as evidence in a court of law.

Confidentiality—Preserving authorized restrictions on access and disclosure, including means for protecting privacy and proprietary information.

Configuration management—The control of changes to a set of configuration items over a system life cycle.

Consumerization—A new model in which emerging technologies are first embraced by the consumer market and later spread to the business.

Containment—Actions taken to limit exposure after an incident has been identified and confirmed.

Content filtering—Controlling access to a network by analyzing the contents of the incoming and outgoing packets and either letting them pass or denying them based on a list of rules. Differs from packet filtering in that it is the data in the packet that are analyzed instead of the attributes of the packet itself (e.g., source/target IP address, transmission control protocol [TCP] flags).

Control—The means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of an administrative, technical, management, or legal nature. Also used as a synonym for safeguard or countermeasure.

Countermeasure—Any process that directly reduces a threat or vulnerability.

Critical infrastructure—Systems whose incapacity or destruction would have a debilitating effect on the economic security of an enterprise, community or nation.

Criticality—The importance of a particular asset or function to the enterprise, and the impact if that asset or function is not available.

Criticality analysis—An analysis to evaluate resources or business functions to identify their importance to the enterprise, and the impact if a function cannot be completed or a resource is not available.

Cross-site scripting (XSS)—A type of injection, in which malicious scripts are injected into otherwise benign and trusted web sites. Cross-site scripting (XSS) attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it. (OWASP)

Cryptography—The art of designing, analyzing and attacking cryptographic schemes.

Cryptosystem—A pair of algorithms that take a key and convert plaintext to ciphertext and back.

Cybercop—An investigator of activities related to computer crime.

Cyberespionage—Activities conducted in the name of security, business, politics or technology to find information that ought to remain secret. It is not inherently military.

Cybersecurity—The protection of information assets by addressing threats to information processed, stored, and transported by internetworked information systems.

Cybersecurity architecture—Describes the structure, components and topology (connections and layout) of security controls within an enterprise's IT infrastructure. The security architecture shows how defense in depth is implemented and how layers of control are linked and is essential to designing and implementing security controls in any complex environment.

Cyberwarfare—Activities supported by military organizations with the purpose to threaten the survival and well-being of society/foreign entity.

D

Data classification—The assignment of a level of sensitivity to data (or information) that results in the specification of controls for each level of classification. Levels of sensitivity of data are assigned according to predefined categories as data are created, amended, enhanced, stored or transmitted. The classification level is an indication of the value or importance of the data to the enterprise.

Data custodian—The individual(s) and department(s) responsible for the storage and safeguarding of computerized data.

Data Encryption Standard (DES)—An algorithm for encoding binary data. It is a secret key cryptosystem published by the National Bureau of Standards (NBS), the predecessor of the US National Institute of Standards and Technology (NIST). DES and its variants has been replaced by the Advanced Encryption Standard (AES).

Data leakage—Siphoning out or leaking information by dumping computer files or stealing computer reports and tapes.

Data owner—The individual(s), normally a manager or director, who has responsibility for the integrity, accurate reporting and use of computerized data.

Data retention—Refers to the policies that govern data and records management for meeting internal, legal and regulatory data archival requirements.

Database—A stored collection of related data needed by enterprises and individuals to meet their information processing and retrieval requirements.

Decentralization—The process of distributing computer processing to different locations within an enterprise.

Decryption—A technique used to recover the original plaintext from the ciphertext so that it is intelligible to the reader. The decryption is a reverse process of the encryption.

Decryption key—A digital piece of information used to recover plaintext from the corresponding ciphertext by decryption.

Defense in depth—The practice of layering defenses to provide added protection. Defense in depth increases security by raising the effort needed in an attack. This strategy places multiple barriers between an attacker and an enterprise's computing and information resources.

Demilitarized zone (DMZ)—A screened (firewalled) network segment that acts as a buffer zone between a trusted and untrusted network. A DMZ is typically used to house systems such as web servers that must be accessible from both internal networks and the Internet.

Denial-of-service (DoS) attack—An assault on a service from a single source that floods it with so many requests that it becomes overwhelmed and is either stopped completely or operates at a significantly reduced rate.

Digital certificate—A piece of information, a digitized form of signature, that provides sender authenticity, message integrity and nonrepudiation. A digital signature is generated using the sender's private key or applying a one-way hash function.

Digital forensics—The process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable in any legal proceedings.

Digital signature—A piece of information, a digitized form of signature, that provides sender authenticity, message integrity and nonrepudiation. A digital signature is generated using the sender's private key or applying a one-way hash function.

Disaster—A sudden, unplanned calamitous event causing great damage or loss. Any event that creates an inability on an organization's part to provide critical business functions for some predetermined period of time. Similar terms are business interruption, outage and catastrophe.

The period when enterprise management decides to divert from normal production responses and exercises its disaster recovery plan (DRP). It typically signifies the beginning of a move from a primary location to an alternate location.

Disaster recovery plan (DRP)—A set of human, physical, technical and procedural resources to recover, within a defined time and cost, an activity interrupted by an emergency or disaster.

Discretionary access control (DAC)—A means of restricting access to objects based on the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject.

Domain name system (DNS)—A hierarchical database that is distributed across the Internet that allows names to be resolved into IP addresses (and vice versa) to locate services such as web and email servers.

Domain name system (DNS) exfiltration—Tunneling over DNS to gain network access. Lower-level attack vector for simple to complex data transmission, slow but difficult to detect.

Due care—The level of care expected from a reasonable person of similar competency under similar conditions.

Due diligence—The performance of those actions that are generally regarded as prudent, responsible and necessary to conduct a thorough and objective investigation, review and/or analysis.

Dynamic ports—Dynamic and/or private ports--49152 through 65535: Not listed by IANA because of their dynamic nature.

E

Eavesdropping—Listening a private communication without permission.

E-commerce—The processes by which enterprises conduct business electronically with their customers, suppliers and other external business partners, using the Internet as an enabling technology. E-commerce encompasses both business-to-business (B2B) and business-to-consumer (B2C) e-commerce models, but does not include existing non-Internet e-commerce methods based on private networks such as electronic data interchange (EDI) and Society for Worldwide Interbank Financial Telecommunication (SWIFT).

Egress—Network communications going out.

Elliptical curve cryptography (ECC)—An algorithm that combines plane geometry with algebra to achieve stronger authentication with smaller keys compared to traditional methods, such as RSA, which primarily use algebraic factoring. Smaller keys are more suitable to mobile devices.

Encapsulation security payload (ESP)—Protocol, which is designed to provide a mix of security services in IPv4 and IPv6. ESP can be used to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service (a form of partial sequence integrity), and (limited) traffic flow confidentiality (RFC 4303). The ESP header is inserted after the IP header and before the next layer protocol header (transport mode) or before an encapsulated IP header (tunnel mode).

Encryption—The process of taking an unencrypted message (plaintext), applying a mathematical function to it (encryption algorithm with a key) and producing an encrypted message (ciphertext).

Encryption algorithm—A mathematically based function or calculation that encrypts/decrypts data.

Encryption key—A piece of information, in a digitized form, used by an encryption algorithm to convert the plaintext to the ciphertext.

Eradication—When containment measures have been deployed after an incident occurs, the root cause of the incident must be identified and removed from the network. Eradication methods include: restoring backups to achieve a clean state of the system, removing the root cause, improving defenses and performing vulnerability analysis to find further potential damage from the same root cause.

Ethernet—A popular network protocol and cabling scheme that uses a bus topology and carrier sense multiple access/collision detection (CSMA/CD) to prevent network failures or collisions when two devices try to access the network at the same time.

Event—Something that happens at a specific place and/or time.

Evidence—Information that proves or disproves a stated issue. Information that an auditor gathers in the course of performing an IS audit; relevant if it pertains to the audit objectives and has a logical relationship to the findings and conclusions it is used to support.

Exploit—Full use of a vulnerability for the benefit of an attacker.

F

File transfer protocol (FTP)—A protocol used to transfer files over a Transmission Control Protocol/ Internet Protocol (TCP/IP) network (Internet, UNIX, etc.).

Firewall—A system or combination of systems that enforces a boundary between two or more networks, typically forming a barrier between a secure and an open environment such as the Internet.

Forensic examination—The process of collecting, assessing, classifying and documenting digital evidence to assist in the identification of an offender and the method of compromise.

Freeware—Software available free of charge.

G

Gateway—A device (router, firewall) on a network that serves as an entrance to another network.

Governance—Ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making; and monitoring performance and compliance against agreed-on direction and objectives. Conditions can include the cost of capital, foreign exchange rates, etc. Options can include shifting manufacturing to other locations, subcontracting portions of the enterprise to third parties, selecting a product mix from many available choices, etc.

Governance, Risk Management and Compliance (GRC)—A business term used to group the three close-related disciplines responsible for the protection of assets and operations.

Guideline—A description of a particular way of accomplishing something that is less prescriptive than a procedure.

H

Hacker—An individual who attempts to gain unauthorized access to a computer system.

Hash function—An algorithm that maps or translates one set of bits into another (generally smaller) so that a message yields the same result every time the algorithm is executed using the same message as input. It is computationally infeasible for a message to be derived or reconstituted from the result produced by the algorithm or to find two different messages that produce the same hash result using the same algorithm.

Hash total—The total of any numeric data field in a document or computer file. This total is checked against a control total of the same field to facilitate accuracy of processing.

Hashing—Using a hash function (algorithm) to create hash valued or checksums that validate message integrity.

Hijacking—An exploitation of a valid network session for unauthorized purposes.

Honeypot—A specially configured server, also known as a decoy server, designed to attract and monitor intruders in a manner such that their actions do not affect production systems. Also known as “decoy server.”

Horizontal defense in depth—Controls are placed in various places in the path to access an asset.

Hubs—A common connection point for devices in a network, hubs are used to connect segments of a local area network (LAN). A hub contains multiple ports. When a packet arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets.

Human firewall—A person prepared to act as a network layer of defense through education and awareness.

Hypertext Transfer Protocol (HTTP)—A communication protocol used to connect to servers on the World Wide Web. Its primary function is to establish a connection with a web server and transmit hypertext markup language (HTML), extensible markup language (XML) or other pages to client browsers.

I

IEEE (Institute of Electrical and Electronics Engineers)—Pronounced I-triple-E; an organization composed of engineers, scientists and students. Best known for developing standards for the computer and electronics industry.

IEEE 802.11—A family of specifications developed by the Institute of Electrical and Electronics Engineers (IEEE) for wireless local area network (WLAN) technology. 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients.

Imaging—A process that allows one to obtain a bit-for-bit copy of data to avoid damage of original data or information when multiple analyses may be performed. The imaging process is made to obtain residual data, such as deleted files, fragments of deleted files and other information present, from the disk for analysis. This is possible because imaging duplicates the disk surface, sector by sector.

Impact—Magnitude of loss resulting from a threat exploiting a vulnerability.

Impact analysis—A study to prioritize the criticality of information resources for the enterprise based on costs (or consequences) of adverse events. In an impact analysis, threats to assets are identified and potential business losses determined for different time periods. This assessment is used to justify the extent of safeguards that are required and recovery time frames. This analysis is the basis for establishing the recovery strategy.

Incident—Any event that is not part of the standard operation of a service and that causes, or may cause, an interruption to, or a reduction in, the quality of that service.

Incident response—The response of an enterprise to a disaster or other significant event that may significantly affect the enterprise, its people, or its ability to function productively. An incident response may include evacuation of a facility, initiating a disaster recovery plan (DRP), performing damage assessment, and any other measures necessary to bring an enterprise to a more stable status.

Incident response plan—The operational component of incident management. The plan includes documented procedures and guidelines for defining the criticality of incidents, reporting and escalation process, and recovery procedures.

Information security—Ensures that within the enterprise, information is protected against disclosure to unauthorized users (confidentiality), improper modification (integrity), and nonaccess when required (availability).

Information security program—The overall combination of technical, operational and procedural measures and management structures implemented to provide for the confidentiality, integrity and availability of information based on business requirements and risk analysis.

Information systems (IS)—The combination of strategic, managerial and operational activities involved in gathering, processing, storing, distributing and using information and its related technologies.

Information systems are distinct from information technology (IT) in that an information system has an IT component that interacts with the process components.

Infrastructure as a Service (IaaS)—Offers the capability to provision processing, storage, networks and other fundamental computing resources, enabling the customer to deploy and run arbitrary software, which can include operating systems (OSs) and applications.

Ingestion—A process to convert information extracted to a format that can be understood by investigators. See also Normalization.

Ingress—Network communications coming in.

Inherent risk—The risk level or exposure without taking into account the actions that management has taken or might take (e.g., implementing controls).

Injection—A general term for attack types which consist of injecting code that is then interpreted/ executed by the application (OWASP).

Intangible asset—An asset that is not physical in nature. Examples include: intellectual property (patents, trademarks, copyrights, processes), goodwill and brand recognition.

Integrity—The guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity.

Intellectual property—Intangible assets that belong to an enterprise for its exclusive use. Examples include: patents, copyrights, trademarks, ideas, and trade secrets.

International Standards Organization (ISO)—The world’s largest developer of voluntary International Standards.

Internet Assigned Numbers Authority (IANA)— Responsible for the global coordination of the DNS root, IP addressing, and other Internet protocol resources.

Internet Control Message Protocol (ICMP)—A set of protocols that allow systems to communicate information about the state of services on other systems. For example, ICMP is used in determining whether systems are up, maximum packet sizes on links, whether a destination host/network/port is available. Hackers typically use (abuse) ICMP to determine information about the remote site.

Internet protocol (IP)—Specifies the format of packets and the addressing scheme.

Internet protocol (IP) packet spoofing—An attack using packets with the spoofed source Internet packet (IP) addresses. This technique exploits applications that use authentication based on IP addresses. This technique also may enable an unauthorized user to gain root access on the target system.

Internet service provider (ISP)—A third party that provides individuals and enterprises with access to the Internet and a variety of other Internet-related services.

Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX)—IPX is layer 3 of the open systems interconnect (OSI) model network protocol; SPX is layer 4 transport protocol. The SPX layer sits on top of the IPX layer and provides connection- oriented services between two nodes on the network.

Interrogation—Used to obtain prior indicators or relationships, including telephone numbers, IP addresses and names of individuals, from extracted data.

Intruder—Individual or group gaining access to the network and its resources without permission.

Intrusion detection—The process of monitoring the events occurring in a computer system or network to detect signs of unauthorized access or attack.

Intrusion detection system (IDS)—Inspects network and host security activity to identify suspicious patterns that may indicate a network or system attack.

Intrusion Prevention—A preemptive approach to network security used to identify potential threats and respond to them to stop, or at least limit, damage or disruption.

Intrusion prevention system (IPS)—A system designed to not only detect attacks, but also to prevent the intended victim hosts from being affected by the attacks.

Investigation—The collection and analysis of evidence with the goal to identifying the perpetrator of an attack or unauthorized use or access.

IP address—A unique binary number used to identify devices on a TCP/IP network.

IP Authentication Header (AH)—Protocol used to provide connectionless integrity and data origin authentication for IP datagrams (hereafter referred to as just “integrity”) and to provide protection against replays. (RFC 4302). AH ensures data integrity with a checksum that a message authentication code, such as MD5, generates. To ensure data origin authentication, AH includes a secret shared key in the algorithm that it uses for authentication. To ensure replay protection, AH uses a sequence number field within the IP authentication header.

IP Security (IPSec)—A set of protocols developed by the Internet Engineering Task Force (IETF) to support the secure exchange of packets.

IT governance—The responsibility of executives and the board of directors; consists of the leadership, organizational structures and processes that ensure that the enterprise's IT sustains and extends the enterprise's strategies and objectives.

K

Kernel mode—Used for execution of privileged instructions for the internal operation of the system. In kernel mode, there are no protections from errors or malicious activity and all parts of the system and memory are accessible.

Key length—The size of the encryption key measured in bits.

Key risk indicator (KRI)—A subset of risk indicators that are highly relevant and possess a high probability of predicting or indicating important risk. See also Risk Indicator.

Keylogger—Software used to record all keystrokes on a computer.

L

Latency—The time it takes a system and network delay to respond. More specifically, system latency is the time a system takes to retrieve data. Network latency is the time it takes for a packet to travel from source to the final destination.

Layer 2 switches—Data link level devices that can divide and interconnect network segments and help to reduce collision domains in Ethernet-based networks.

Layer 3 and 4 switches—Switches with operating capabilities at layer 3 and layer 4 of the open systems interconnect (OSI) model. These switches look at the incoming packet's networking protocol, e.g., IP, and then compare the destination IP address to the list of addresses in their tables, to actively calculate the best way to send a packet to its destination.

Layer 4-7 switches—Used for load balancing among groups of servers. Also known as content- switches, content services switches, web-switches or application-switches.

Legacy system—Outdated computer systems.

Likelihood—The probability of something happening.

Local area network (LAN)—Communication network that serves several users within a specified geographic area. A personal computer LAN functions as a distributed processing system in which each computer in the network does its own processing and manages some of its data. Shared data are stored in a file server that acts as a remote disk drive for all users in the network.

Log—To record details of information or events in an organized record-keeping system, usually sequenced in the order in which they occurred.

Logical access—Ability to interact with computer resources granted using identification, authentication and authorization.

Logical access controls—The policies, procedures, organizational structure and electronic access controls designed to restrict access to computer software and data files.

M

Media access control (MAC) address—A unique identifier assigned to network interfaces for communications on the physical network segment.

MAC header—Represents the hardware address of an network interface controller (NIC) inside a data packet.

Mail relay server—An electronic mail (email) server that relays messages so that neither the sender nor the recipient is a local user.

Mainframe—A large high-speed computer, especially one supporting numerous workstations or peripherals.

Malware—Short for malicious software. Designed to infiltrate, damage or obtain information from a computer system without the owner's consent. Malware is commonly taken to include computer viruses, worms, Trojan horses, spyware and adware. Spyware is generally used for marketing purposes and, as such, is not malicious, although it is generally unwanted. Spyware can, however, be used to gather information for identity theft or other clearly illicit purposes.

Mandatory access control (MAC)—A means of restricting access to data based on varying degrees of security requirements for information contained in the objects and the corresponding security clearance of users or programs acting on their behalf.

Man-in-the-middle attack—An attack strategy in which the attacker intercepts the communication stream between two parts of the victim system and then replaces the traffic between the two components with the intruder's own, eventually assuming control of the communication.

Masking—A computerized technique of blocking out the display of sensitive information, such as passwords, on a computer terminal or report.

Message authentication code—An American National Standards Institute (ANSI) standard checksum that is computed using Data Encryption Standard (DES).

Message digest—A smaller extrapolated version of the original message created using a message digest algorithm.

Message digest algorithm—Message digest algorithms are SHA1, MD2, MD4 and MD5. These algorithms are one-way functions unlike private and public key encryption algorithms. All digest algorithms take a message of arbitrary length and produce a 128-bit message digest.

Metropolitan area network (MAN)—A data network intended to serve an area the size of a large city.

Miniature fragment attack—Using this method, an attacker fragments the IP packet into smaller ones and pushes it through the firewall, in the hope that only the first of the sequence of fragmented packets would be examined and the others would pass without review.

Mirrored site—An alternate site that contains the same information as the original. Mirrored sites are set up for backup and disaster recovery and to balance the traffic load for numerous download requests. Such download mirrors are often placed in different locations throughout the Internet.

Mobile device—A small, handheld computing devices, typically having a display screen with touch input and/or a miniature keyboard and weighing less than two pounds.

Mobile site—The use of a mobile/temporary facility to serve as a business resumption location. The facility can usually be delivered to any site and can house information technology and staff.

Monitoring policy—Rules outlining or delineating the way in which information about the use of computers, networks, applications and information is captured and interpreted.

Multifactor authentication—A combination of more than one authentication method, such as token and password (or personal identification number [PIN] or token and biometric device).

N

National Institute for Standards and Technology (NIST)—Develops tests, test methods, reference data, proof-of concept implementations, and technical analyses to advance the development and productive use of information technology. NIST is a US government entity that creates mandatory standards that are followed by federal agencies and those doing business with them.

Network basic input/output system (NetBIOS)—A program that allows applications on different computers to communicate within a local area network (LAN).

Network address translation (NAT)—A methodology of modifying network address information in datagram packet headers while they are in transit across a traffic routing device for the purpose of remapping one IP address space into another.

Network interface card (NIC)—A communication card that when inserted into a computer, allows it to communicate with other computers on a network. Most NICs are designed for a particular type of network or protocol.

Network news transfer protocol (NNTP)—Used for the distribution, inquiry, retrieval, and posting of Netnews articles using a reliable stream-based mechanism. For news-reading clients, NNTP enables retrieval of news articles that are stored in a central database, giving subscribers the ability to select only those articles they wish to read (RFC 3977).

Network segmentation—A common technique to implement network security is to segment an organization's network into separate zones that can be separately controlled, monitored and protected.

Network traffic analysis—Identifies patterns in network communications. Traffic analysis does not need to have the actual content of the communication but analyzes where traffic is taking place, when and for how long communications occur and the size of information transferred.

Nonintrusive monitoring—The use of transported probes or traces to assemble information, track traffic and identify vulnerabilities.

Nonrepudiation—The assurance that a party cannot later deny originating data; provision of proof of the integrity and origin of the data and that can be verified by a third party. A digital signature can provide nonrepudiation.

Normalization—The elimination of redundant data.

O

Obfuscation—The deliberate act of creating source or machine code that is difficult for humans to understand.

Open Systems Interconnect (OSI) model—A model for the design of a network. The open systems interconnect (OSI) model defines groups of functionality required to network computers into layers. Each layer implements a standard protocol to implement its functionality. There are seven layers in the OSI model.

Operating system (OS)—A master control program that runs the computer and acts as a scheduler and traffic controller.

Open Web Application Security Project (OWASP)—An open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted.

Outcome measure—Represents the consequences of actions previously taken; often referred to as a lag indicator. Outcome measures frequently focus on results at the end of a time period and characterize historic performance. They are also referred to as a key goal indicator (KGI) and used to indicate whether goals have been met. These can be measured only after the fact and, therefore, are called “lag indicators.”

Outsourcing—A formal agreement with a third party to perform IS or other business functions for an enterprise.

P

Packet—Data unit that is routed from source to destination in a packet-switched network. A packet contains both routing information and data. Transmission Control Protocol/Internet Protocol (TCP/IP) is such a packet-switched network.

Packet filtering—Controlling access to a network by analyzing the attributes of the incoming and outgoing packets and either letting them pass, or denying them, based on a list of rules.

Packet switching—The process of transmitting messages in convenient pieces that can be reassembled at the destination.

Passive response—A response option in intrusion detection in which the system simply reports and records the problem detected, relying on the user to take subsequent action.

Password—A protected, generally computer-encrypted string of characters that authenticate a computer user to the computer system.

Password cracker—A tool that tests the strength of user passwords by searching for passwords that are easy to guess. It repeatedly tries words from specially crafted dictionaries and often also generates thousands (and in some cases, even millions) of permutations of characters, numbers and symbols.

Patch—Fixes to software programming errors and vulnerabilities.

Patch management—An area of systems management that involves acquiring, testing and installing multiple patches (code changes) to an administered computer system in order to maintain up-to-date software and often to address security risk. Patch management tasks include the following: maintaining current knowledge of available patches; deciding what patches are appropriate for particular systems; ensuring that patches are installed properly; testing systems after installation; and documenting all associated procedures, such as specific configurations required. A number of products are available to automate patch management tasks. Patches are sometimes ineffective and can sometimes cause more problems than they fix. Patch management experts suggest that system administrators take simple steps to avoid problems, such as performing backups and testing patches on noncritical systems prior to installations. Patch management can be viewed as part of change management.

Payload—The section of fundamental data in a transmission. In malicious software this refers to the section containing the harmful data/code.

Penetration testing—A live test of the effectiveness of security defenses through mimicking the actions of real-life attackers.

Personal identification number (PIN)—A type of password (i.e., a secret number assigned to an individual) that, in conjunction with some means of identifying the individual, serves to verify the authenticity of the individual. PINs have been adopted by financial institutions as the primary means of verifying customers in an electronic funds transfer (EFT) system.

Phishing—This is a type of electronic mail (email) attack that attempts to convince a user that the originator is genuine, but with the intention of obtaining information for use in social engineering. Phishing attacks may take the form of masquerading as a lottery organization advising the recipient or the user's bank of a large win; in either case, the intent is to obtain account and personal identification number (PIN) details. Alternative attacks may seek to obtain apparently innocuous business information, which may be used in another form of active attack.

Plain old telephone service (POTS)—A wired telecommunications system.

Platform as a Service (PaaS)—Offers the capability to deploy onto the cloud infrastructure customer- created or -acquired applications that are created using programming languages and tools supported by the provider.

Policy—Generally, a document that records a high-level principle or course of action that has been decided on.

The intended purpose is to influence and guide both present and future decision making to be in line with the philosophy, objectives and strategic plans established by the enterprise's management teams.

In addition to policy content, policies need to describe the consequences of failing to comply with the policy, the means for handling exceptions, and the manner in which compliance with the policy will be checked and measured.

Port (Port number)—A process or application- specific software element serving as a communication end point for the Transport Layer IP protocols (UDP and TCP).

Port scanning—The act of probing a system to identify open ports.

Prime number—A natural number greater than 1 that can only be divided by 1 and itself.

Principle of least privilege/access—Controls used to allow the least privilege access needed to complete a task.

Privacy—Freedom from unauthorized intrusion or disclosure of information about an individual.

Probe—Inspect a network or system to find weak spots.

Procedure—A document containing a detailed description of the steps necessary to perform specific operations in conformance with applicable standards. Procedures are defined as part of processes.

Protocol—The rules by which a network operates and controls the flow and priority of transmissions.

Proxy server—A server that acts on behalf of a user. Typical proxies accept a connection from a user, make a decision as to whether the user or client IP address is permitted to use the proxy, perhaps perform additional authentication, and complete a connection to a remote destination on behalf of the user.

Public key encryption—A cryptographic system that uses two keys: one is a public key, which is known to everyone, and the second is a private or secret key, which is only known to the recipient of the message. See also Asymmetric Key.

Public key infrastructure (PKI)—A series of processes and technologies for the association of cryptographic keys with the entity to whom those keys were issued.

Public switched telephone network (PSTN)—A communications system that sets up a dedicated channel (or circuit) between two points for the duration of the transmission.

R

Ransomware—Malware that restricts access to the compromised systems until a ransom demand is satisfied.

Reciprocal agreement—Emergency processing agreement between two or more enterprises with similar equipment or applications. Typically, participants of a reciprocal agreement promise to provide processing time to each other when an emergency arises.

Recovery—The phase in the incident response plan that ensures that affected systems or services are restored to a condition specified in the service delivery objectives (SDOs) or business continuity plan (BCP).

Recovery action—Execution of a response or task according to a written procedure.

Recovery point objective (RPO)—Determined based on the acceptable data loss in case of a disruption of operations.

It indicates the earliest point in time that is acceptable to recover the data. The RPO effectively quantifies the permissible amount of data loss in case of interruption.

Recovery time objective (RTO)—The amount of time allowed for the recovery of a business function or resource after a disaster occurs.

Redundant site—A recovery strategy involving the duplication of key IT components, including data or other key business processes, whereby fast recovery can take place.

Registered ports—Registered ports--1024 through 49151: Listed by the IANA and on most systems can be used by ordinary user processes or programs executed by ordinary users.

Registration authority (RA)—The individual institution that validates an entity's proof of identity and ownership of a key pair.

Regulation—Rules or laws defined and enforced by an authority to regulate conduct.

Regulatory requirements—Rules or laws that regulate conduct and that the enterprise must obey to become compliant.

Remediation—After vulnerabilities are identified and assessed, appropriate remediation can take place to mitigate or eliminate the vulnerability.

Remote access (RAS)—Refers to any combination of hardware and software to enable the remote access to tools or information that typically reside on a network of IT devices.

Originally coined by Microsoft when referring to their built-in NT remote access tools, RAS was a service provided by Windows NT which allowed most of the services that would be available on a network to be accessed over a modem link. Over the years, many vendors have provided both hardware and software solutions to gain remote access to various types of networked information. In fact, most modern routers include a basic RAS capability that can be enabled for any dial-up interface.

Removable media—Any type of storage device that can be removed from the system while is running.

Repeaters—A physical layer device that regenerates and propagates electrical signals between two network segments. Repeaters receive signals from one network segment and amplify (regenerate) the signal to compensate for signals (analog or digital) distorted by transmission loss due to reduction of signal strength during transmission (i.e., attenuation).

Replay—The ability to copy a message or stream of messages between two parties and replay (retransmit) them to one or more of the parties.

Residual risk—The remaining risk after management has implemented a risk response.

Resilience—The ability of a system or network to resist failure or to recover quickly from any disruption, usually with minimal recognizable effect.

Return on investment (ROI)—A measure of operating performance and efficiency, computed in its simplest form by dividing net income by the total investment over the period being considered.

Return-oriented attacks—An exploit technique in which the attacker uses control of the call stack to indirectly execute cherry-picked machine instructions immediately prior to the return instruction in subroutines within the existing program code.

Risk—The combination of the probability of an event and its consequence (ISO/IEC 73).

Risk acceptance—If the risk is within the enterprise's risk tolerance or if the cost of otherwise mitigating the risk is higher than the potential loss, the enterprise can assume the risk and absorb any losses.

Risk assessment—A process used to identify and evaluate risk and its potential effects. Risk assessments are used to identify those items or areas that present the highest risk, vulnerability or exposure to the enterprise for inclusion in the IS annual audit plan. Risk assessments are also used to manage the project delivery and project benefit risk.

Risk avoidance—The process for systematically avoiding risk, constituting one approach to managing risk.

Risk management—The coordinated activities to direct and control an enterprise with regard to risk. In the International Standard, the term “control” is used as a synonym for “measure.” (ISO/IEC Guide 73:2002)

One of the governance objectives. Entails recognizing risk; assessing the impact and likelihood of that risk; and developing strategies, such as avoiding the risk, reducing the negative effect of the risk and/or transferring the risk, to manage it within the context of the enterprise's risk appetite. (COBIT 5)

Risk mitigation—The management of risk through the use of countermeasures and controls.

Risk reduction—The implementation of controls or countermeasures to reduce the likelihood or impact of a risk to a level within the organization's risk tolerance.

Risk tolerance—The acceptable level of variation that management is willing to allow for any particular risk as the enterprise pursues its objectives.

Risk transfer—The process of assigning risk to another enterprise, usually through the purchase of an insurance policy or by outsourcing the service.

Risk treatment—The process of selection and implementation of measures to modify risk (ISO/IEC Guide 73:2002).

Root cause analysis—A process of diagnosis to establish the origins of events, which can be used for learning from consequences, typically from errors and problems.

Rootkit—A software suite designed to aid an intruder in gaining unauthorized administrative access to a computer system.

Router—A networking device that can send (route) data packets from one local area network (LAN) or wide area network (WAN) to another, based on addressing at the network layer (Layer 3) in the open systems interconnection (OSI) model. Networks connected by routers can use different or similar networking protocols. Routers usually are capable of filtering packets based on parameters, such as source addresses, destination addresses, protocol and network applications (ports).

RSA—A public key cryptosystem developed by R. Rivest, A. Shamir and L. Adleman used for both encryption and digital signatures. The RSA has two different keys, the public encryption key and the secret decryption key. The strength of the RSA depends on the difficulty of the prime number factorization. For applications with high-level security, the number of the decryption key bits should be greater than 512 bits.

S

Safeguard—A practice, procedure or mechanism that reduces risk.

Secure Electronic Transaction (SET)—A standard that will ensure that credit card and associated payment order information travels safely and securely between the various involved parties on the Internet.

Secure Multipurpose Internet Mail Extensions (S/MIME)—Provides cryptographic security services for electronic messaging applications: authentication, message integrity and nonrepudiation of origin (using digital signatures) and privacy and data security (using encryption) to provide a consistent way to send and receive MIME data (RFC 2311).

Secure Socket Layer (SSL)—A protocol that is used to transmit private documents through the Internet. The SSL protocol uses a private key to encrypt the data that are to be transferred through the SSL connection.

Secure Hypertext transfer protocol (S/HTTP)—An application layer protocol, S/HTTP transmits individual messages or pages securely between a web client and server by establishing an SSL-type connection.

Secure Shell (SSH)—Network protocol that uses cryptography to secure communication, remote command line login and remote command execution between two networked computers.

Security as a Service (SecaaS)—The next generation of managed security services dedicated to the delivery, over the Internet, of specialized information-security services.

Security metrics—A standard of measurement used in management of security-related activities.

Security perimeter—The boundary that defines the area of security concern and security policy coverage.

Segmentation—Network segmentation is the process of logically grouping network assets, resources, and applications together into compartmentalized areas that have no trust of each other.

Segregation/separation of duties (SoD)—A basic internal control that prevents or detects errors and irregularities by assigning to separate individuals the responsibility for initiating and recording transactions and for the custody of assets. Segregation/ separation of duties is commonly used in large IT organizations so that no single person is in a position to introduce fraudulent or malicious code without detection.

Sensitivity—A measure of the impact that improper disclosure of information may have on an enterprise.

Service delivery objective (SDO)—Directly related to the business needs, SDO is the level of services to be reached during the alternate process mode until the normal situation is restored.

Service level agreement (SLA)—An agreement, preferably documented, between a service provider and the customer(s)/user(s) that defines minimum performance targets for a service and how they will be measured.

Simple mail transfer protocol (SMTP)—The standard electronic mail (email) protocol on the Internet.

Single factor authentication (SFA)—Authentication process that requires only the user ID and password to grant access.

Smart card—A small electronic device that contains electronic memory, and possibly an embedded integrated circuit. Smart cards can be used for a number of purposes including the storage of digital certificates or digital cash, or they can be used as a token to authenticate users.

Sniffing—The process by which data traversing a network are captured or monitored.

Social engineering—An attack based on deceiving users or administrators at the target site into revealing confidential or sensitive information.

Software as a Service (SaaS)—Offers the capability to use the provider's applications running on cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email).

Source routing specification—A transmission technique where the sender of a packet can specify the route that packet should follow through the network.

Spam—Computer-generated messages sent as unsolicited advertising.

Spear phishing—An attack where social engineering techniques are used to masquerade as a trusted party to obtain important information such as passwords from the victim.

Spoofing—Faking the sending address of a transmission in order to gain illegal entry into a secure system.

Spyware—Software whose purpose is to monitor a computer user's actions (e.g., web sites visited) and report these actions to a third party, without the informed consent of that machine's owner or legitimate user. A particularly malicious form of spyware is software that monitors keystrokes to obtain passwords or otherwise gathers sensitive information such as credit card numbers, which it then transmits to a malicious third party. The term has also come to refer more broadly to software that subverts the computer's operation for the benefit of a third party.

SQL injection—Results from failure of the application to appropriately validate input. When specially crafted user-controlled input consisting of SQL syntax is used without proper validation as part of SQL queries, it is possible to glean information from the database in ways not envisaged during application design. (MITRE)

Stateful inspection—A firewall architecture that tracks each connection traversing all interfaces of the firewall and makes sure they are valid.

Statutory requirements—Laws created by government institutions.

Supervisory control and data acquisition (SCADA)—Systems used to control and monitor industrial and manufacturing processes, and utility facilities.

Switches—Typically associated as a data link layer device, switches enable local area network (LAN) segments to be created and interconnected, which has the added benefit of reducing collision domains in Ethernet-based networks.

Symmetric key encryption—System in which a different key (or set of keys) is used by each pair of trading partners to ensure that no one else can read their messages. The same key is used for encryption and decryption. See also Private Key Cryptosystem.

System development lifecycle (SDLC)—The phases deployed in the development or acquisition of a software system. SDLC is an approach used to plan, design, develop, test and implement an application system or a major modification to an application system. Typical phases of SDLC include the feasibility study, requirements study, requirements definition, detailed design, programming, testing, installation and postimplementation review, but not the service delivery or benefits realization activities.

System hardening—A process to eliminate as many security risks as possible by removing all nonessential software programs, protocols, services and utilities from the system.

T

Tangible asset—Any assets that has physical form.

Target—Person or asset selected as the aim of an attack.

Telnet—Network protocol used to enable remote access to a server computer. Commands typed are run on the remote server.

Threat—Anything (e.g., object, substance, human) that is capable of acting against an asset in a manner that can result in harm. A potential cause of an unwanted incident (ISO/IEC 13335).

Threat agent—Methods and things used to exploit a vulnerability. Examples include determination, capability, motive and resources.

Threat analysis/assessment—An evaluation of the type, scope and nature of events or actions that can result in adverse consequences; identification of the threats that exist against enterprise assets. The threat analysis usually defines the level of threat and the likelihood of it materializing.

Threat event—Any event during which a threat element/actor acts against an asset in a manner that has the potential to directly result in harm.

Threat vector—The path or route used by the adversary to gain access to the target.

Time lines—Chronological graphs where events related to an incident can be mapped to look for relationships in complex cases. Time lines can provide simplified visualization for presentation to management and other nontechnical audiences.

Token—A device that is used to authenticate a user, typically in addition to a username and password. A token is usually a device the size of a credit card that displays a pseudo random number that changes every few minutes.

Topology—The physical layout of how computers are linked together. Examples of topology include ring, star and bus.

Total cost of ownership (TCO)—Includes the original cost of the computer plus the cost of: software, hardware and software upgrades, maintenance, technical support, training, and certain activities performed by users.

Transmission control protocol (TCP)—A connection-based Internet protocol that supports reliable data transfer connections. Packet data are verified using checksums and retransmitted if they are missing or corrupted. The application plays no part in validating the transfer.

Transmission control protocol/Internet protocol (TCP/IP)—Provides the basis for the Internet; a set of communication protocols that encompass media access, packet transport, session communication, file transfer, electronic mail (email), terminal emulation, remote file access and network management.

Transport Layer Security (TLS)—A protocol that provides communications privacy over the Internet. The protocol allows client-server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery (RFC 2246).

Transport Layer Security (TLS) is composed of two layers: the TLS Record Protocol and the TLS Handshake Protocol. The TLS Record Protocol provides connection security with some encryption method such as the Data Encryption Standard (DES). The TLS Record Protocol can also be used without encryption. The TLS Handshake Protocol allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before data is exchanged.

Triple DES (3DES)—A block cipher created from the Data Encryption Standard (DES) cipher by using it three times.

Trojan horse—Purposefully hidden malicious or damaging code within an authorized computer program. Unlike viruses, they do not replicate themselves, but they can be just as destructive to a single computer.

Tunnel—The paths that the encapsulated packets follow in an Internet virtual private network (VPN).

Tunnel mode—Used to protect traffic between different networks when traffic must travel through intermediate or untrusted networks. Tunnel mode encapsulates the entire IP packet with an AH or ESP header and an additional IP header.

Two-factor authentication—The use of two independent mechanisms for authentication, (e.g., requiring a smart card and a password) typically the combination of something you know, are or have.

U

Uncertainty—The difficulty of predicting an outcome due to limited knowledge of all components.

Uniform resource locator (URL)—The string of characters that form a web address.

User Datagram Protocol (UDP)—A connectionless Internet protocol that is designed for network efficiency and speed at the expense of reliability. A data request by the client is served by sending packets without testing to verify whether they actually arrive at the destination, not whether they were corrupted in transit. It is up to the application to determine these factors and request retransmissions.

User interface impersonation—Can be a pop-up ad that impersonates a system dialog, an ad that impersonates a system warning, or an ad that impersonates an application user interface in a mobile device.

User mode—Used for the execution of normal system activities.

User provisioning—A process to create, modify, disable and delete user accounts and their profiles across IT infrastructure and business applications.

V

Value—The relative worth or importance of an investment for an enterprise, as perceived by its key stakeholders, expressed as total life cycle benefits net of related costs, adjusted for risk and (in the case of financial value) the time value of money.

Vertical defense in depth—Controls are placed at different system layers – hardware, operating system, application, database or user levels.

Virtual local area network (VLAN)—Logical segmentation of a LAN into different broadcast domains. A VLAN is set up by configuring ports on a switch, so devices attached to these ports may communicate as if they were attached to the same physical network segment, although the devices are located on different LAN segments. A VLAN is based on logical rather than physical connections.

Virtual private network (VPN)—A secure private network that uses the public telecommunications infrastructure to transmit data. In contrast to a much more expensive system of owned or leased lines that can only be used by one company, VPNs are used by enterprises for both extranets and wide areas of intranets. Using encryption and authentication, a VPN encrypts all data that pass between two Internet points, maintaining privacy and security.

Virtual private network (VPN) concentrator—A system used to establish VPN tunnels and handle large numbers of simultaneous connections. This system provides authentication, authorization and accounting services.

Virtualization—The process of adding a “guest application” and data onto a “virtual server,” recognizing that the guest application will ultimately part company from this physical server.

Virus—A program with the ability to reproduce by modifying other programs to include a copy of itself. A virus may contain destructive code that can move into multiple programs, data files or devices on a system and spread through multiple systems in a network.

Virus signature file—The file of virus patterns that are compared with existing files to determine whether they are infected with a virus or worm.

Voice over Internet Protocol (VoIP)—Also called IP Telephony, Internet Telephony and Broadband Phone, a technology that makes it possible to have a voice conversation over the Internet or over any dedicated Internet Protocol (IP) network instead of over dedicated voice transmission lines.

Volatile data—Data that changes frequently and can be lost when the system’s power is shut down.

Vulnerability—A weakness in the design, implementation, operation or internal control of a process that could expose the system to adverse threats from threat events.

Vulnerability analysis/assessment—A process of identifying and classifying vulnerabilities.

Vulnerability scanning—An automated process to proactively identify security weaknesses in a network or individual system.

W

Warm site—Similar to a hot site but not fully equipped with all of the necessary hardware needed for recovery.

Web hosting—The business of providing the equipment and services required to host and maintain files for one or more web sites and provide fast Internet connections to those sites. Most hosting is “shared,” which means that web sites of multiple companies are on the same server to share/reduce costs.

Web server—Using the client-server model and the World Wide Web’s HyperText Transfer Protocol (HTTP), Web Server is a software program that serves web pages to users.

Well-known ports—0 through 1023: Controlled and assigned by the Internet Assigned Numbers Authority (IANA), and on most systems can be used only by system (or root) processes or by programs executed by privileged users. The assigned ports use the first portion of the possible port numbers. Initially, these assigned ports were in the range 0-255. Currently, the range for assigned ports managed by the IANA has been expanded to the range 0-1023.

Wide area network (WAN)—A computer network connecting different remote locations that may range from short distances, such as a floor or building, to extremely long transmissions that encompass a large region or several countries.

Wi-Fi protected access (WPA)—A class of systems used to secure wireless (Wi-Fi) computer networks. WPA was created in response to several serious weaknesses that researchers found in the previous system, Wired Equivalent Privacy (WEP). WPA implements the majority of the IEEE 802.11i standard, and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared. WPA is designed to work with all wireless network interface cards, but not necessarily with first generation wireless access points. WPA2 implements the full standard, but will not work with some older network cards. Both provide good security with two significant issues. First, either WPA or WPA2 must be enabled and chosen in preference to WEP; WEP is usually presented as the first security choice in most installation instructions. Second, in the “personal” mode, the most likely choice for homes and small offices, a pass phrase is required that, for full security, must be longer than the typical six to eight character passwords users are taught to employ.

Wi-Fi protected access II (WPA2)—Wireless security protocol that supports 802.11i encryption standards to provide greater security. This protocol uses Advanced Encryption Standards (AES) and Temporal Key Integrity Protocol (TKIP) for stronger encryption.

Wired equivalent privacy (WEP)—A scheme that is part of the IEEE 802.11 wireless networking standard to secure IEEE 802.11 wireless networks (also known as Wi-Fi networks). Because a wireless network broadcasts messages using radio, it is particularly susceptible to eavesdropping. WEP was intended to provide comparable confidentiality to a traditional wired network (in particular, it does not protect users of the network from each other), hence the name. Several serious weaknesses were identified by cryptanalysts, and WEP was superseded by Wi-Fi Protected Access (WPA) in 2003, and then by the full IEEE 802.11i standard (also known as WPA2) in 2004. Despite the weaknesses, WEP provides a level of security that can deter casual snooping.

Wireless local area network (WLAN)—Two or more systems networked using a wireless distribution method.

Worm—A programmed network attack in which a self-replicating program does not attach itself to programs, but rather spreads independently of users’ action.

Write blocker—A device that allows the acquisition of information on a drive without creating the possibility of accidentally damaging the drive.

Write protect—The use of hardware or software to prevent data to be overwritten or deleted.

Z

Zero-day exploit—A vulnerability that is exploited before the software creator/vendor is even aware of its existence.

APPENDIX C—KNOWLEDGE CHECK ANSWERS

SECTION 1—KNOWLEDGE CHECK

1. Three common controls used to protect the availability of information are: [a]
 - a. Redundancy, backups and access controls.
 - b. Encryption, file permissions and access controls.
 - c. Access controls, logging and digital signatures.
 - d. Hashes, logging and backups.
2. Select all that apply. Governance has several goals, including: [a, b, c, e]
 - a. Providing strategic direction.
 - b. Ensuring that objectives are achieved.
 - c. Verifying that organizational resources are being used appropriately.
 - d. Directing and monitoring security activities.
 - e. Ascertaining whether risk is being managed properly.
3. Choose three. According to the NIST framework, which of the following are considered key functions necessary for the protection of digital assets? [b, d, e]
 - a. Encrypt
 - b. Protect
 - c. Investigate
 - d. Recover
 - e. Identify
4. Which of the following is the best definition for cybersecurity? [d]
 - a. The process by which an organization manages cybersecurity risk to an acceptable level
 - b. The protection of information from unauthorized access or disclosure
 - c. The protection of paper documents, digital and intellectual property, and verbal or visual communications
 - d. Protecting information assets by addressing threats to information that is processed, stored or transported by interworked information systems
5. Which of the following cybersecurity roles is charged with the duty of managing incidents and remediation? [c]
 - a. Board of directors
 - b. Executive committee
 - c. Cybersecurity management
 - d. Cybersecurity practitioners

SECTION 2—KNOWLEDGE CHECK

1. The core duty of cybersecurity is to identify, respond and manage risk to an organization's digital assets.
2. A(n) threat is anything capable of acting against an asset in a manner that can cause harm.
3. A(n) asset is something of value worth protecting.
4. A(n) vulnerability is a weakness in the design, implementation, operation or internal controls in a process that could be exploited to violate the system security.
5. The path or route used to gain access to the target asset is known as a(n) attack vector.
6. In an attack, the container that delivers the exploit to the target is called a(n) payload.
7. Policies communicate required and prohibited activities and behaviors.
8. Rootkit is a class of malware that hides the existence of other malware by modifying the underlying operating system.
9. Procedures provide details on how to comply with policies and standards.
10. Guidelines contain step-by-step instructions to carry out procedures.

11. Malware, also called malicious code, is software designed to gain access to targeted computer systems, steal information or disrupt computer operations.
12. Standards are used to interpret policies in specific situations.
13. Patches are solutions to software programming and coding errors.
14. Identity management includes many components such as directory services, authentication and authorization services, and user management capabilities such as provisioning and deprovisioning.

SECTION 3—KNOWLEDGE CHECK

1. Select all that apply. The Internet perimeter should: [a, b, d, e]
 - a. Detect and block traffic from infected internal end points.
 - b. Eliminate threats such as email spam, viruses and worms.
 - c. Format, encrypt and compress data.
 - d. Control user traffic bound toward the Internet.
 - e. Monitor and detect network ports for rogue activity.
2. The layer of the OSI model ensures that data are transferred reliably in the correct sequence, and the layer coordinates and manages user connections. [b]
 - a. Presentation, data link
 - b. Transport, session
 - c. Physical, application
 - d. Data link, network
3. Choose three. There key benefits of the DMZ system are: [b, c, e]
 - a. DMZs are based on logical rather than physical connections.
 - b. An intruder must penetrate three separate devices.
 - c. Private network addresses are not disclosed to the Internet.
 - d. Excellent performance and scalability as Internet usage grows.
 - e. Internal systems do not have direct access to the Internet.
4. Which of the following best states the role of encryption within an overall cybersecurity program? [d]
 - a. Encryption is the primary means of securing digital assets.
 - b. Encryption depends upon shared secrets and is therefore an unreliable means of control.
 - c. A program's encryption elements should be handled by a third-party cryptologist.
 - d. Encryption is an essential but incomplete form of access control.
5. The number and types of layers needed for defense in depth are a function of: [a]
 - a. Asset value, criticality, reliability of each control and degree of exposure.
 - b. Threat agents, governance, compliance and mobile device policy.
 - c. Network configuration, navigation controls, user interface and VPN traffic.
 - d. Isolation, segmentation, internal controls and external controls.

SECTION 4—KNOWLEDGE CHECK

1. Put the steps of the penetration testing phase into the correct order. [d, b, a, c]
 - a. Attack
 - b. Discovery
 - c. Reporting
 - d. Planning
2. System hardening should implement the principle of or . [b]
 - a. Governance, compliance
 - b. Least privilege, access control
 - c. Stateful inspection, remote access
 - d. Vulnerability assessment, risk mitigation
3. Select all that apply. Which of the following are considered functional areas of network management as defined by ISO? [a, b, d, e]
 - a. Accounting management
 - b. Fault management
 - c. Firewall management
 - d. Performance management
 - e. Security management
4. Virtualization involves: [b]
 - a. The creation of a layer between physical and logical access controls.
 - b. Multiple guests coexisting on the same server in isolation of one another.
 - c. Simultaneous use of kernel mode and user mode.
 - d. DNS interrogation, WHOIS queries and network sniffing.
5. Vulnerability management begins with an understanding of cybersecurity assets and their locations, which can be accomplished by: [c]
 - a. Vulnerability scanning.
 - b. Penetration testing.
 - c. Maintaining an asset inventory.
 - d. Using command line tools.

SECTION 5—KNOWLEDGE CHECK

1. Arrange the steps of the incident response process into the correct order. [d, e, b, a, c]
 - a. Mitigation and recovery
 - b. Investigation
 - c. Postincident analysis
 - d. Preparation
 - e. Detection and analysis
2. Which element of an incident response plan involves obtaining and preserving evidence? [c]
 - a. Preparation
 - b. Identification
 - c. Containment
 - d. Eradication

3. Select three. The chain of custody contains information regarding: [b, d, e]
 - a. Disaster recovery objectives, resources and personnel.
 - b. Who had access to the evidence, in chronological order.
 - c. Labor, union and privacy regulations.
 - d. Proof that the analysis is based on copies identical to the original evidence.
 - e. The procedures followed in working with the evidence.

4. NIST defines a(n) as a “violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.” [d]
 - a. Disaster
 - b. Event
 - c. Threat
 - d. Incident

5. Select all that apply. A business impact analysis (BIA) should identify: [b, c, d]
 - a. The circumstances under which a disaster should be declared.
 - b. The estimated probability of the identified threats actually occurring.
 - c. The efficiency and effectiveness of existing risk mitigation controls.
 - d. A list of potential vulnerabilities, dangers and/or threats.
 - e. Which types of data backups (full, incremental and differential) will be used.

SECTION 6—KNOWLEDGE CHECK

1. _____ is defined as “a model for enabling convenient, on-demand network access to a shared pool of configurable resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management or service provider interaction.” [b]
 - a. Software as a Service (SaaS)
 - b. Cloud computing
 - c. Big data
 - d. Platform as a Service (PaaS)

2. Select all that apply. Which of the following statements about advanced persistent threats (APTs) are true? [a, b, c]
 - a. APTs typically originate from sources such as organized crime groups, activists or governments.
 - b. APTs use obfuscation techniques that help them remain undiscovered for months or even years.
 - c. APTs are often long-term, multi-phase projects with a focus on reconnaissance.
 - d. The APT attack cycle begins with target penetration and collection of sensitive information.
 - e. Although they are often associated with APTs, intelligence agencies are rarely the perpetrators of APT attacks.

3. Smart devices, BYOD strategies and freely available applications and services are all examples of: [a]
 - a. The reorientation of technologies and services designed around the individual end user.
 - b. The primacy of external threats to business enterprises in today’s threat landscape.
 - c. The stubborn persistence of traditional communication methods.
 - d. The application layer’s susceptibility to APTs and zero-day exploits.

4. Choose three. Which types of risk are typically associated with mobile devices? [a, c, d]
- a. Organizational risk
 - b. Compliance risk
 - c. Technical risk
 - d. Physical risk
 - e. Transactional risk
5. Which three elements of the current threat landscape have provided increased levels of access and connectivity, and therefore increased opportunities for cybercrime? [d]
- a. Text messaging, Bluetooth technology and SIM cards
 - b. Web applications, botnets and primary malware
 - c. Financial gains, intellectual property and politics
 - d. Cloud computing, social media and mobile computing

Page intentionally left blank

APPENDIX D—ADDITIONAL RESOURCES

1. Anderson, Kent, “A Business Model for Information Security,” *ISACA® Journal*, Vol. 3, 2008
2. Encurve, LLC, *Risk Management Concepts Presentation*, 2013
3. ENISA, *ENISA Threat Landscape 2013—Overview of Current and Emerging Cyber-Threats*, December 2013
4. ISACA, *Advanced Persistent Threats: How to Manage the Risk to Your Business*, USA, 2013
5. ISACA, *CISA Review Manual 2014*, USA
6. ISACA, *COBIT 5 for Information Security*, USA, 2012
7. ISACA, *CRISC Review Manual 2014*, USA
8. ISACA, *Responding to Targeted Cyberattacks*, USA, 2013
9. ISACA, *Securing Mobile Devices Using COBIT 5 for Information Security*, USA, 2012
10. ISACA, “Top Business/Security Issues Survey Results,” USA, 2011
11. Khan, Kamal, “Introduction to Voice-over IP Technology,” *ISACA Journal*, Volume 2, 2005, www.isaca.org/Journal/Past-Issues/2005/Volume-2/Pages/Introduction-to-Voice-over-IP-Technology1.aspx
12. Mandia, Kevin, Matt Pepe, Chris Prosis, *Incident Response & Computer Forensics*, 2nd Edition, McGraw Hill/Osborne, USA, 2003
13. McKemmish, D. Rodney. *Computer and Intrusion Forensics*, Artech House, USA, 2003
14. MITRE, *Common Attack Pattern Enumeration and Classification (CAPEC)*, February 2014, <http://capec.mitre.org/>
15. Moody, Robert “Ports and Port Scanning: An Introduction”, *ISACA Journal*, Volume 4, 2001, www.isaca.org/Journal/Past-Issues/2001/Volume-5/Pages/Ports-and-Port-Scanning-An-Introduction.aspx
16. National Institute of Standards and Technology (NIST), *Special Publication 800-30, Revision 1*, Guide for Conducting Risk Assessments, USA, September 2012
17. Open Web Application Security Project (OWASP). *OWASP Top 10*, 2013, www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
18. Schultz, E.E., Brown, D.S., and Longstaff, T.A.; *Responding to Computer Security Incidents: Guidelines for Incident Handling*, Lawrence Livermore National Lab., USA, 1990
19. The 2013 Global Information Security Workforce Study, 2014, www.isc2cares.org/Workforcestudy

Page intentionally left blank