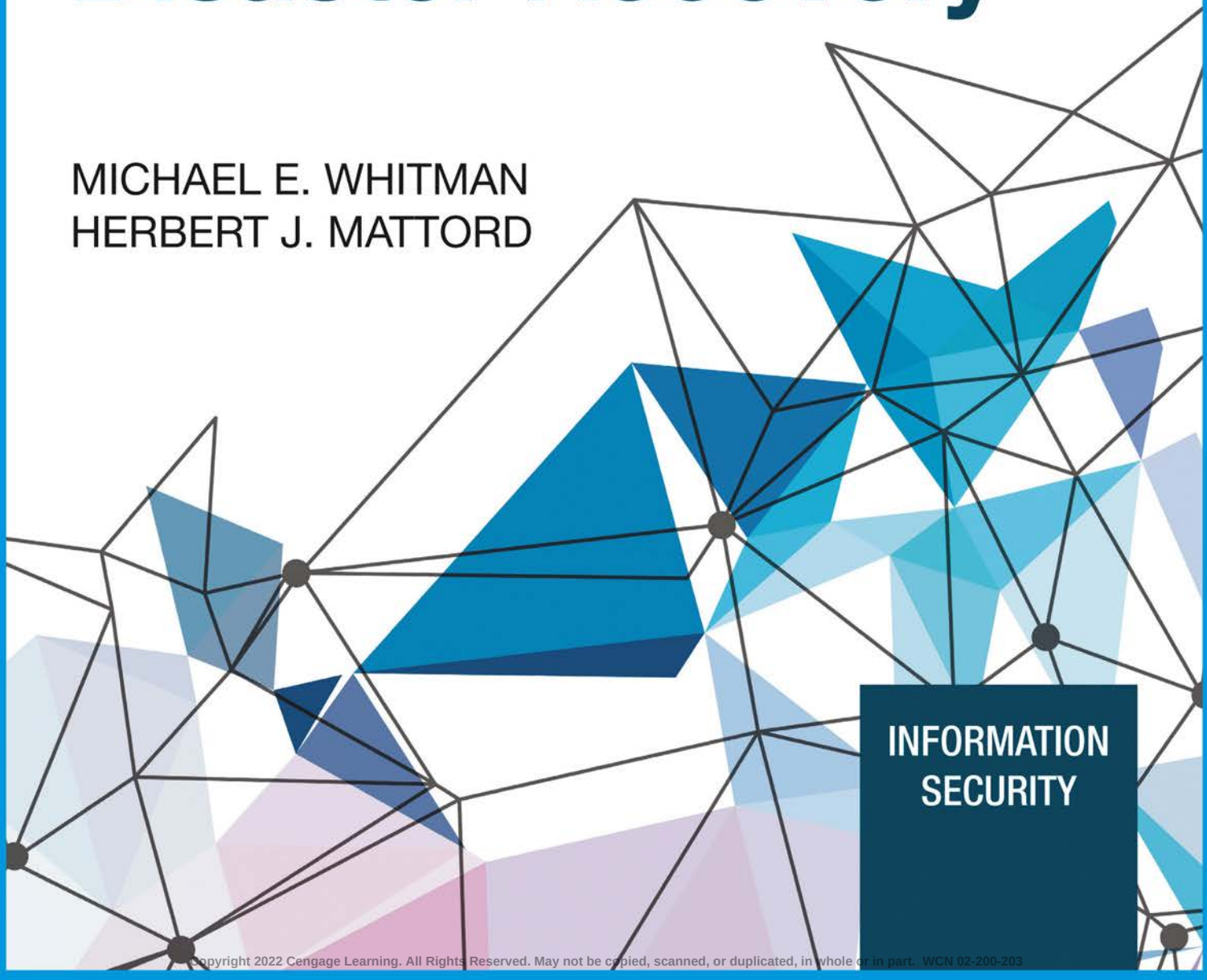
CENGAGE

Third Edition

Principles of Incident Response & Disaster Recovery

MICHAEL E. WHITMAN
HERBERT J. MATTORD



INFORMATION SECURITY

Third Edition

Principles of Incident Response & Disaster Recovery

MICHAEL E. WHITMAN
PH.D., CISM, CISSP
HERBERT J. MATTORD
PH.D., CISM, CISSP

INFORMATION SECURITY

CENGAGE

Australia • Brazil • Canada • Mexico • Singapore • United Kingdom • United States

***Principles of Incident Response & Disaster Recovery*, 3rd Edition**
Michael Whitman and Herbert Mattord

SVP, Higher Education Product Management: Erin Joyner

VP, Product Management: Thais Alencar

Product Team Manager: Kristin McNary

Associate Product Manager: Danielle Klahr

Product Assistant: Tom Benedetto

Director, Learning Design: Rebecca von Gillern

Senior Manager, Learning Design: Leigh Hefferon

Learning Designer: Mary Clyne

Vice President, Marketing – Science, Technology, & Math: Jason Sakos

Senior Marketing Director: Michele McTighe

Marketing Manager: Cassie Cloutier

Product Specialist: Mackenzie Paine

Director, Content Creation: Juliet Steiner

Senior Manager, Content Creation: Patty Stephan

Senior Content Manager: Brooke Greenhouse

Director, Digital Production Services: Krista Kellman

Digital Delivery Lead: Jim Vaughey

Developmental Editor: Dan Seiter

Production Service/Composition: SPi Global

Design Director: Jack Pendleton

Designer: Erin Griffin

Cover image(s): Kolonko/ShutterStock.com

Library of Congress Control Number: 2020917514

ISBN: 978-0-357-50832-9

Loose-leaf Edition:
ISBN: 978-0-357-50833-6

Cengage
200 Pier 4 Boulevard
Boston, MA 02210
USA

Printed in Mexico

Print Number: 01 Print Year: 2020

To Rhonda, Rachel, Alex, and Meghan, thank you for your loving support.

—MEW

To my granddaughters, Julie and Ellie. Always stay strong.

—HJM

BRIEF CONTENTS

TABLE OF CONTENTS

MODULE 4

MODULE 5

MODULE 6

MODULE 7

PREFACE

As global networks expand the interconnection of the world's technically complex infrastructure, communication and computing systems gain added importance. Information security has gained in importance as a professional practice, and it has also emerged as an academic discipline. Ongoing security events, such as malware attacks and successful hacking efforts, have pointed out the weaknesses inherent in unprotected systems and exposed the need for heightened security of these systems. In order to secure technologically advanced systems and networks, both education and the infrastructure to deliver that education are needed to prepare the next generation of information technology and information security professionals to develop a more secure and ethical computing environment. Therefore, improved tools and more sophisticated techniques are needed to prepare students to recognize the threats and vulnerabilities present in existing systems and to design and develop secure systems. Many years have passed since the need for improved information security education was recognized, and as Dr. Ernest McDuffie, Lead of NIST NICE, points out:

> *While there is no doubt that technology has changed the way we live, work, and play, there are very real threats associated with the increased use of technology and our growing dependence on cyberspace. . . .*
>
> *Education can prepare the general public to identify and avoid risks in cyberspace; education will ready the cybersecurity workforce of tomorrow; and education can keep today's cybersecurity professionals at the leading edge of the latest technology and mitigation strategies.*

The need for improvements in information security education is so great that the U.S. National Security Agency (NSA) has established Centers of Academic Excellence in Information Assurance, as described in Presidential Decision Directive 63, "The Policy on Critical Infrastructure Protection" (1998):

> *The goal of the program is to reduce vulnerability in our national information infrastructure by promoting higher education and research in cyber defense and producing professionals with cyber defense expertise.*

Academics who want to focus on delivering skilled undergraduates to the commercial information technology (IT) sector need teaching resources that focus on key topics in the broader area of information security.

APPROACH

This resource provides an overview of contingency operations and its components as well as a thorough treatment of the administration of the planning process for incident response (IR), disaster recovery (DR), and business continuity (BC). It can be used to support course delivery for information security-driven programs targeted at information technology students, as well as IT management and technology management curricula aimed at business or technical management students.

Features

To ensure a successful learning experience, this product includes the following pedagogical features:

- *Module Objectives*—Each module in this book begins with a detailed list of the concepts to be mastered within that module. This list provides you with a quick reference to the contents of the module as well as a useful study aid.
- *Module Scenarios*—Each module opens and closes with a case scenario that follows the same fictional company as it encounters various contingency planning or operational issues. The closing scenario also includes discussion questions to give students and the instructor an opportunity to discuss the issues that underlie the content. New in this edition is an example of an ethical decision that extends the opportunity to discuss the impact of events in the scenario.
- *Boxed Examples*—These supplemental sections, which feature examples not associated with the ongoing case study, are included to illustrate key learning objectives and technical details or extend the coverage of plans and policies.
- *Learning Support*—Each module includes a Module Summary section, definitions of key terms, and a set of open-ended review questions. These are used to reinforce learning of the subject matter presented in the module.
- *Real-World Exercises*—At the end of each module, Real-World Exercises give students the opportunity to examine the contingency planning arena outside the classroom. Using these structured exercises, students can pursue the learning objectives listed at the beginning of each module and deepen their understanding of the text material.
- *Hands-On Projects*—Virtual labs are now available through the MindTap that accompanies *Principles of Incident Response and Disaster Recovery*. These labs have been designed by the authors to help students develop valuable practical skills. They can be accessed in the Practice It folder in MindTap or through the instructor's learning management system (LMS).

New to This Edition

This edition extends the work from the previous edition by adding more detail and examples, specifically in the examination of incident response activities. It continues to track the evolution in approaches and methods that have been developed at NIST. Although the material on disaster recovery, business continuity, and crisis management has not been reduced, the text's focus now follows that of the IT industry in shifting to the prevention, detection, reaction to, and recovery from computer-based incidents and avoidance of threats to the security of information.

Several modules have been reorganized, with a new module on incident detection that has an increased focus on IDPSs, security information and event management systems (SIEMs), and security event correlation.

Structure

The narrative is organized into 12 modules. Appendices and other materials are available with the instructor resources online and in MindTap. Here are summaries of each module's contents:

Module 1, *An Overview of Information Security and Risk Management*, defines the concepts of information security and risk management and explains how they are integral to the management processes used for incident response and contingency planning.

Module 2, *Planning for Organizational Readiness*, focuses on how an organization can plan for and develop processes and staffing appointments needed for successful incident response and contingency plans.

Module 3, *Contingency Strategies for Incident Response, Disaster Recovery, and Business Continuity*, explores the relationships among contingency planning and the subordinate elements of incident response, business resumption, disaster recovery, and business continuity planning. It also explains the techniques used for data and application backup and recovery.

Module 4, *Incident Response: Planning*, expands on the incident response planning process to include processes and activities that are needed as well as the skills and techniques used to develop such plans.

Module 5, *Incident Response: Organizing and Preparing the CSIRT*, presents a detailed explanation of the actions that the CSIRT performs and how they are designed and developed.

Module 6, *Incident Response: Incident Detection Strategies*, describes IR reaction strategies and how they are applied to incidents.

Module 7, *Incident Response: Detection Systems*, describes IDPSs, security information and event management systems (SIEMs), and security event correlation.

Module 8, *Incident Response: Response Strategies*, describes how an organization plans for and executes the recovery process when an incident occurs.

Module 9, *Incident Response: Recovery, Maintenance, and Investigations*, explores how organizations recover from incidents. It also expands on the steps involved in the ongoing maintenance of the IR plan as well as the IT forensics process.

Module 10, *Disaster Recovery*, presents the challenges an organization faces when engaged in disaster recovery and how such challenges are met.

Module 11, *Business Continuity*, covers how organizations ensure continuous operations even when their primary facilities are not available.

Module 12, *Crisis Management in IR, DR, and BC*, covers the role of crisis management and recommends the elements of a plan to prepare for crisis response. The module also covers the key international standards that affect IR, DR, and BC.

Three appendices in the instructor's resources and MindTap present sample BC and crisis management plans and templates.

MINDTAP

MindTap activities for *Principles of Incident Response and Disaster Recovery* are designed to help you master the skills you need in today's workforce. Research shows that employers need critical thinkers, troubleshooters, and creative problem-solvers to stay relevant in this fast-paced, technology-driven world. MindTap helps you achieve this goal with assignments and activities that provide hands-on practice with real-life relevance.

All MindTap activities and assignments are tied to defined learning objectives. Readings with spaced knowledge checks support the course objectives, while hands-on labs provide practice and give you an opportunity to troubleshoot, explore, and try different solutions in a secure sandbox environment. Videos, Review Questions, and Real-World Exercises will help you reinforce your understanding of each module's concepts, and Security for Life assignments will prompt you to explore industry-related news and events.

Use the interactive Flashcards and PowerPoint slides in each module to help you study for exams. Measure how well you have mastered the material by taking the Review Quizzes and completing the Case Exercises at the end of each module. Finally, the Post-Assessment Quiz helps you assess all that you have learned throughout the course, see where you gained deeper knowledge, and identify the skills where you need additional practice!

Instructors can use the content and learning path as they are, or choose how these materials wrap around their own resources. MindTap supplies the analytics and reporting so you can easily see where the class stands in terms of progress, engagement, and completion rates. To learn more about shaping what students see and scheduling when they see it, instructors can go to *www.cengage.com/mindtap/*.

INSTRUCTOR RESOURCES

Instructors can access a robust set of teaching resources tailored to this product at Cengage's Companion Site. An instructor login is required. Please visit *instructor.cengage.com* to request access or log in to your existing account. There, you will find the following instructor-specific resources:

- *Instructor's Manual*—The Instructor's Manual that accompanies this resource includes additional instructional material to assist in class preparation, including suggestions for classroom activities, discussion topics, and additional projects.
- *Solution Files*—The solution files include answers to selected end-of-module materials, including the review questions and some of the hands-on projects.
- *Test Bank*—Cengage Testing, powered by Cognero, is a flexible, online system that allows you to do the following:
  - Author, edit, and manage test bank content from multiple Cengage solutions.
  - Create multiple test versions in an instant.
  - Deliver tests from your LMS, your classroom, or wherever you want.

  The generous question sets developed for this edition include a variety of question types tagged to core learning objectives and narrative topics.
- *PowerPoint Presentations*—This edition includes Microsoft PowerPoint slides for each module. These are included as a teaching aid for classroom presentation. They can also be made available to students on the network for module review, or they can be printed for classroom distribution. Instructors should feel free to add their own slides for additional topics they introduce to the class.
- *Hands-On Projects*—The virtual labs provided with this resource can help students develop practical skills that will be of value as they progress through the course. These author-developed lab projects are available via MindTap or at the Companion Site for LMS integration.
- *Information Security Community Site*—Stay secure with the Information Security Community Site! Connect with students, professors, and professionals from around the world, and stay on top of this ever-changing field.
  - Visit *www.cengage.com/community/infosec*.
  - Download resources such as instructional videos and labs.
  - Ask authors, professors, and students the questions that are on your mind in our Discussion Forums.
  - See up-to-date news, videos, and articles.
  - Read author blogs.
  - Listen to podcasts on the latest information security topics.

AUTHOR TEAM

Long-time college professors and information security professionals Michael Whitman and Herbert Mattord have jointly developed this text and MindTap to merge knowledge from the world of academic study with practical experience from the business world.

Michael Whitman, Ph.D., CISM, CISSP, is the Executive Director of the KSU Institute for Cybersecurity Workforce Development (ICWD, *cyberinstitute.kennesaw.edu*) and a Professor of Information Security and Assurance at Kennesaw State University, Kennesaw, Georgia. Dr. Whitman has over 30 years of experience in higher education, with over 20 years of experience in designing and teaching information security courses. He is an active researcher in information security, fair and responsible use policies, and computer-use ethics. He currently teaches graduate and undergraduate courses in information security and cybersecurity. He has published articles in the top journals in his field, including *Information Systems Research*, *Communications of the ACM*, *Information and Management*, *Journal of International Business Studies*, and *Journal of Computer Information Systems*. Under Dr. Whitman's leadership, Kennesaw State University has been recognized by the National Security Agency and the Department of Homeland Security as a National Center of Academic Excellence in Information Assurance/Cyber Defense Education four times. Dr. Whitman is also the coauthor of *Principles of Information Security*; *Management of Information Security*; *Readings and Cases in the Management*

of Information Security; *Readings and Cases in Information Security: Law and Ethics*; *The Hands-On Information Security Lab Manual*; *Roadmap to the Management of Information Security for IT and Information Security Professionals*; *Guide to Firewalls and VPNs*; *Guide to Firewalls and Network Security*; and *Guide to Network Security*, all published by Course Technology (now Cengage). Prior to his career in academia, Dr. Whitman was an officer in the United States Army.

Herbert Mattord, Ph.D., CISM, CISSP, completed 24 years of IT industry experience as an application developer, database administrator, project manager, and information security practitioner before joining the faculty of Kennesaw State University in 2002. Dr. Mattord is a Professor of Information Security and Assurance and the Director of Undergraduate Education and Outreach at the ICWD. During his career as an IT practitioner, Dr. Mattord has been an adjunct professor at Kennesaw State University; Southern Polytechnic State University in Marietta, Georgia; Austin Community College in Austin, Texas; and Texas State University: San Marcos. He currently teaches undergraduate and graduate courses in information security and cybersecurity. He was formerly the manager of corporate information technology security at Georgia-Pacific Corporation, where much of the practical knowledge found in this text was acquired. Professor Mattord is also the coauthor of *Principles of Information Security*; *Management of Information Security*; *Readings and Cases in the Management of Information Security*; *Readings and Cases in Information Security: Law and Ethics*; *The Hands-On Information Security Lab Manual*; *Roadmap to the Management of Information Security for IT and Information Security Professionals*; *Guide to Firewalls and VPNs*; *Guide to Firewalls and Network Security*; and *Guide to Network Security*, all published by Course Technology (now Cengage).

ACKNOWLEDGMENTS

The authors would like to thank their families for their support and understanding for the many hours dedicated to this project—hours taken in many cases from family activities.

Reviewers

We are indebted to the following individuals for their contributions of perceptive feedback on the initial proposal, the project outline, and individual learning modules:

- Paul Witman, California Lutheran University
- Humayun Zafar, Kennesaw State University
- Randall Reid, University of West Florida

Special Thanks

The authors wish to thank the editorial and production teams at Cengage. Their diligent and professional efforts greatly enhanced the final product:

- Danielle Klahr, Associate Product Manager
- Amy Savino, Senior Product Manager
- Mary Clyne, Learning Designer
- Brooke Greenhouse, Senior Content Manager
- Dan Seiter, Developmental Editor

In addition, several professional and commercial organizations and individuals have aided the development of the text and MindTap by providing information and inspiration, and the authors wish to acknowledge their contributions:

- Bernstein Crisis Management
- Continuity Central
- Information Systems Security Associations

- Institute for Crisis Management
- National Institute of Standards and Technology
- Oracle, Inc.
- Purdue University
- Rothstein Associates, Inc.
- SunGard
- Our colleagues in the Department of Information Systems and the Michael J. Coles College of Business, Kennesaw State University

Our Commitment

The authors are committed to serving the needs of the adopters and readers. We would be pleased and honored to receive feedback on the textbook, MindTap, and supporting materials. You can contact us through Cengage.

MODULE 1

AN OVERVIEW OF INFORMATION SECURITY AND RISK MANAGEMENT

Upon completion of this material, you should be able to:

1. Define and explain information security
2. Describe the role of information security policy in the organization
3. Identify and explain the basic concepts and phases of risk management

An ounce of prevention is worth a pound of cure.

— Benjamin Franklin

Opening Scenario

Paul Alexander and his boss, Amanda Wilson, were sitting in Amanda's office discussing the coming year's budget when they heard a commotion in the hall. Hearing his name mentioned, Paul stuck his head out the door and saw Jonathon Jasper ("JJ" to his friends) walking quickly toward him.

"Paul!" JJ called again, relieved to see Paul waiting in Amanda's office. "Hi, Amanda," JJ said, then, looking at Paul, he added, "We have a problem." JJ was one of the systems administrators at Hierarchical Access LTD (HAL), a Georgia-based cloud services firm.

Paul stepped out into the hall, closing Amanda's door behind him. "What's up, JJ?"

"I think we've got someone sniffing around our credentialing services platform," JJ replied. "I just looked at the log files, and there is an unusual number of failed login attempts on accounts that normally just don't have that many, like yours!"

Paul answered, "Sounds like we need to investigate," then paused a moment.

"That system is configured to allow off-premises VPN access," he finally said to JJ. "Are there corresponding entries in the reverse proxy server or the VPN logs?"

JJ shook his head "no."

Paul sighed. "Which means it must be internal."

"Yeah, that's why it's a problem," JJ replied. "We haven't gotten this kind of thing since we partitioned the credentialing platform. It's got to be someone in-house."

JJ looked exasperated. "And after all that time I spent conducting awareness training!"

"Don't worry just yet," Paul told him. "Let me make a few calls, and then we'll go from there. Grab your incident response plan and meet me in the conference room in 10 minutes. Grab Tina in network operations on the way; she's on call for today."

contingency planning (CP)

The actions taken by senior management to specify the organization's efforts and actions if an adverse event becomes an incident or disaster. This planning includes incident response, disaster recovery, business continuity, and crisis management efforts, as well as preparatory business impact analysis.

security

A state of being secure and free from danger or harm. Also, the actions taken to make someone or something secure.

INTRODUCTION

This book is about being prepared for the unexpected—being ready for events such as incidents and disasters. We call this **contingency planning (CP)**, and the sad fact is that most organizations don't incorporate it into their day-to-day business activities, so they are often not well prepared to offer the proper response to a disaster or security incident. By December 2019, Internet World Stats estimated that there were over 4.5 billion people online, representing well over half of the world's 7.8 billion population.[1] Each one of those online users is a potential threat to any online system. The vast majority of Internet users will not intentionally probe, monitor, attack, or attempt to access an organization's information without authorization; however, that potential does exist. If even less than one-tenth of 1 percent of online users make the effort, the result would be over four and a half *million* potential attackers.

In the weeks that followed the September 11, 2001 attacks in New York, Pennsylvania, and Washington D.C., the media reported on the disastrous losses that various organizations were suffering. Still, many organizations were able to continue conducting business. Why? They were prepared for unexpected events. The cataclysm in 2001 was not the first attack on the World Trade Center (WTC). On February 26, 1993, a car bomb exploded beneath one of the WTC towers, killing 6 and injuring over 1,000. The attack was limited in its devastation only because the attackers weren't able to acquire all the components for a coordinated bomb and cyanide gas attack.[2]

Still, this attack was a wake-up call for the hundreds of organizations that conducted business in the WTC. Many began asking, "What would we have done if the attack had been more successful?" As a direct result, many of the organizations occupying the WTC on September 11 had developed contingency plans. Although thousands of people lost their lives in the attack, many were able to evacuate, and many organizations were prepared to resume their businesses in the aftermath of the devastation.

In a Forrester survey called "The State of Disaster Recovery Preparedness," only about 55 percent of respondents were either prepared or very prepared to recover their data center in the event of a disaster or site failure, and only 54 percent had a formal enterprise disaster recovery program.[3] According to the Syncsort State of Resilience Report, "Nearly half of businesses experienced a failure requiring a high availability/disaster recovery solution to resume operations. 35% lost a few minutes to an hour of data, 28% lost a few hours and 31% lost a day or more."[4] According to the U.S. Federal Emergency Management Agency, between 40 and 60 percent of small businesses affected by a disaster either never reopen or go out of business following the event.[5] Thus, having a disaster recovery and business continuity plan is vital to sustaining operations when catastrophes strike. Considering the risks, it is imperative that management teams create, implement, train, and rehearse test plans to deal with incidents and disasters. For this reason, the importance of information security and contingency planning has been steadily growing and is now taken more seriously by senior management and boards of directors.

Before we can discuss contingency planning in detail, we must introduce some critical concepts, of which contingency planning is an integral part. The first of these, which serves as the overall disciplinary umbrella, is information security. This term refers to many interlinked programs and activities that work together to ensure the confidentiality, integrity, and availability of the information used by organizations. This includes steps to ensure the protection of organizational information systems, specifically during incidents and disasters. Because information security is a complex subject that includes risk management as well as information security policy, it is important to have an overview of that broad field and an understanding of these major components. That is the purpose of this first module. Contingency planning is an important element of information security, but before management can plan for contingencies, it should have an overall strategic plan for information security in place, including risk management processes to guide the appropriate managerial and technical controls.

This module serves as an overview of information security, with special consideration given to risk management and the role that contingency planning plays in (1) information security in general and (2) risk management in particular.

AN OVERVIEW OF INFORMATION SECURITY

In general, **security** means being free from danger. To be secure in this context is to be protected from the risk of loss, damage, unwanted modification, or other hazards. Achieving an appropriate level of security for an organization depends on the implementation of a multilayered system that works to protect information assets from harm, unwanted

access, and modification. Security is often achieved by means of several strategies undertaken simultaneously or used in combination. Many of those strategies will focus on specific areas of security, but they also have many elements in common. It is the role of management to ensure that each strategy is properly planned, organized, staffed, directed, and controlled.

These efforts contribute to the information security program as a whole. This textbook derives its definition of information security from the standards published by the Committee on National Security Systems (CNSS), chaired by the U.S. Secretary of Defense. **Information security (InfoSec)** focuses on the protection of information and the characteristics that give it value, such as confidentiality, integrity, and availability. These characteristics, known as the **C.I.A. triad**, include the technology that stores, processes, and transmits information through a variety of protection mechanisms such as policy, training and awareness programs, and technology. This definition is illustrated in Figure 1-1.

Information assets have the characteristics of **confidentiality** when only the people, agents, or computer systems with the rights and privileges to access them are able to do so. Information assets have **integrity** when they are not exposed (while being stored, processed, or transmitted) to corruption, damage, destruction, or other disruption of their authentic states; in other words, the information is whole, complete, and uncorrupted. Finally, information assets have **availability** when authorized users, agents, or computer systems are able to access them in the specified format without interference or obstruction. In other words, the information is there when it is needed, it comes from an authentic source, and it is in the format expected.

information security (InfoSec)
Protection of the confidentiality, integrity, and availability of information assets, whether in storage, processing, or transmission, via the application of policy, education, training and awareness, and technology.

C.I.A. triad
The industry standard for computer security since the development of the mainframe. The standard is based on three characteristics that describe the utility of information: confidentiality, integrity, and availability.

confidentiality
An attribute of information that describes how data is protected from disclosure or exposure to unauthorized individuals or systems.

integrity
An attribute of information that describes how data is whole, complete, and uncorrupted.

availability
An attribute of information that describes how data is accessible and correctly formatted for use without interference or obstruction.

Key Information Security Concepts

This book uses many terms and concepts that are essential to a discussion of information security. Some of these terms are illustrated in Figure 1-2; all are covered in greater detail in this and subsequent modules.

- ***Access***—A subject or object's ability to use, manipulate, modify, or affect another subject or object. Authorized users have legal access to a system, whereas hackers must gain illegal access to a system. Access controls regulate this ability.
- ***Asset***—The organizational resource that is being protected. An asset can be logical, such as a Web site, software information, or data. An asset can also be physical, such as a person, a computer system, hardware, or other tangible objects. Assets, particularly information assets, are the focus of what security efforts are attempting to protect.

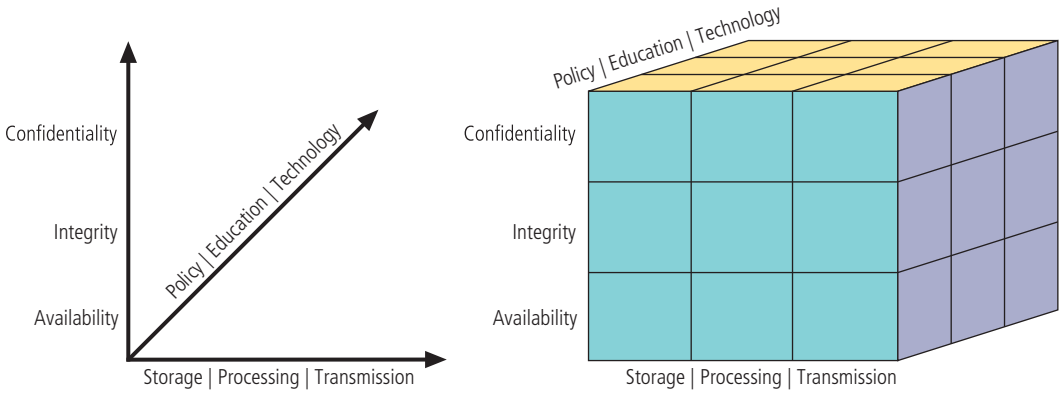


Figure 1-1 CNSS security model[6]

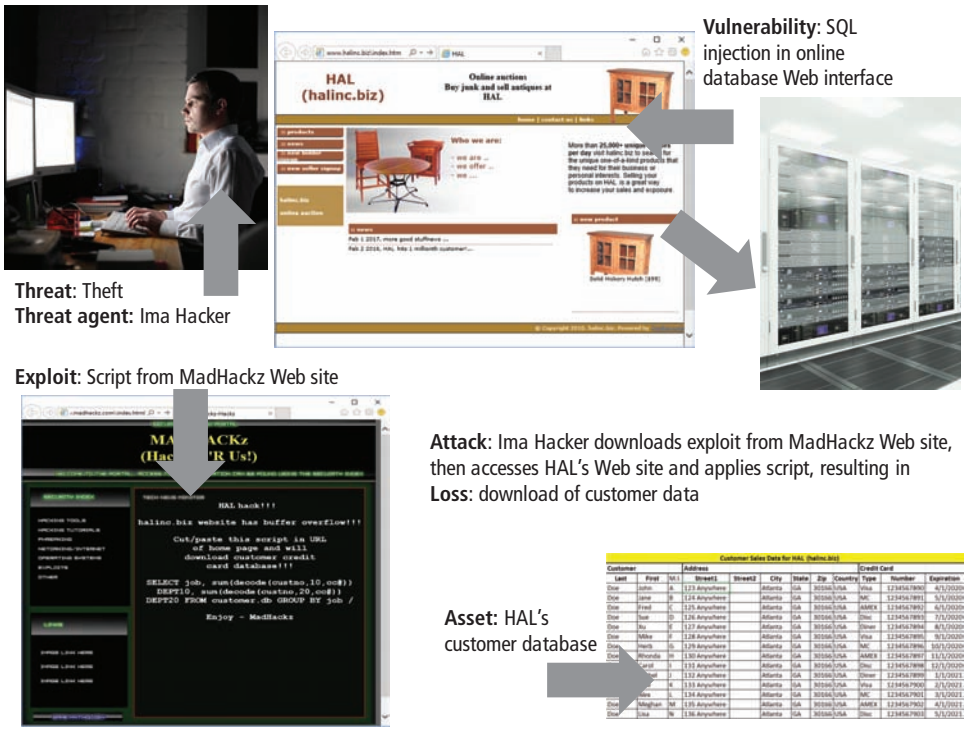


Figure 1-2 Key concepts in information security

Source: The photo at top left is from © iStock.com/TommL. The photo at top right is from © iStock.com/nerminmuminovic.

- ***Attack***—An intentional or unintentional act that can damage or otherwise compromise information and the systems that support it. Attacks can be active or passive, intentional or unintentional, and direct or indirect. Someone who purposefully copies valuable data to re-sell commits an *active attack*, while a person who casually reads sensitive information not intended for his or her use is committing a *passive attack*. A hacker attempting to break into an information system is an *intentional attack*, while a lightning strike that causes a building fire is an *unintentional attack*. A *direct attack* is perpetrated by a hacker using a PC to break into a system, but an *indirect attack* is a hacker compromising a system in order to use it only to attack other systems—for example, as part of a botnet (slang for robot network). This group of compromised computers, running software of the attacker's choosing, can operate autonomously or under the attacker's direct control to attack systems and steal user information or conduct distributed denial-of-service attacks. Direct attacks originate from the threat itself. Indirect attacks originate from a compromised system or resource that is malfunctioning or working under the control of a threat.
- ***Control, safeguard, or countermeasure***—Security mechanisms, policies, or procedures that can successfully counter attacks, reduce risk, resolve vulnerabilities, and otherwise improve security within an organization. The various levels and types of controls are discussed more fully in the following modules.
- ***Exploit***—A technique used to compromise a system. This term can be a verb or a noun. Threat agents may attempt to exploit a system or other information asset by using it illegally for their personal gain. Or, an exploit can be a documented process to take advantage of a vulnerability or exposure, usually in software, that is either inherent in the software or created by the attacker. Exploits make use of existing software tools or custom-made software components.
- ***Exposure***—A condition or state of being exposed; in information security, exposure exists when a vulnerability is known to an attacker.
- ***Loss***—In this context, a single instance of an information asset that suffers damage or destruction, unintended or unauthorized modification or disclosure, or denial of use. As one example, when an organization's information is stolen, it has suffered a loss.
- ***Risk***—The probability of an unwanted occurrence, such as an adverse event or loss. Organizations must minimize risk to match their risk appetite—the quantity and nature of the risk they are willing to accept.

- ***Subjects and objects of attack***—A computer can be either the subject of an attack—an agent entity used to conduct the attack—or the object of an attack: the target entity. A computer can also be both the subject and object of an attack. For example, it can be compromised by an attack (object) and then used to attack other systems (subject).
- ***Threat***—Any event or circumstance that has the potential to adversely affect operations and assets. The term *threat source* is commonly used interchangeably with the more generic term *threat*. The two terms are technically distinct, but to simplify the discussion, the text will continue to use the term *threat* to describe threat sources.
- ***Threat agent***—The specific instance or a component of a threat. For example, the threat source of *trespass or espionage* is a category of potential danger to information assets, while an *external professional hacker* (like Kevin Mitnick, who was convicted of hacking into phone systems) is a specific threat agent. A lightning strike, hailstorm, or tornado is a threat agent that is part of the threat source known as *acts of God/acts of nature*.
- ***Threat event***—An intentional or unintentional act that can damage or otherwise compromise information and the systems that support it. An example of a threat event might be damage caused by a storm. This term is commonly used interchangeably with the term *attack*.
- ***Threat source***—A category of objects, people, or other entities that represents the origin of danger to an asset—in other words, a category of threat agents. Threat sources are always present and can be purposeful or undirected. For example, threat agent *hackers*, as part of the threat source *acts of trespass or espionage*, purposely threaten unprotected information systems, while threat agent *severe storms*, as part of the threat source *acts of God/acts of nature*, incidentally threaten buildings and their contents.
- ***Vulnerability***—A potential weakness in an asset or its defensive control system(s). Some examples of vulnerabilities are a flaw in a software package, an unprotected system port, and an unlocked door. Some well-known vulnerabilities have been examined, documented, and published; others remain latent (or undiscovered).

The 12 Categories of Threats

Table 1-1 shows 12 general categories of threats that represent a clear and present danger to an organization's people, information, and systems. Each organization must prioritize the threats it faces based on the particular security situation in which it operates, its organizational strategy regarding risk, and the exposure levels of its assets. You may notice that many of the examples in the table could be listed in more than one category. For example, a theft performed by a hacker falls into the category of *theft*, but it can also be considered an example of *espionage or trespass* as the hacker illegally accesses the information. The theft may also be accompanied by defacement actions to delay discovery, qualifying it for the category of *sabotage or vandalism*.

Table 1-1 The 12 Categories of Threats to Information Security[7]

Category of Threat	Attack Examples
Compromises to intellectual property	Piracy, copyright infringement
Deviations in quality of service	Internet service provider (ISP), power, or WAN service problems
Espionage or trespass	Unauthorized access and/or data collection
Forces of nature	Fire, floods, earthquakes, lightning
Human error or failure	Accidents, employee mistakes
Information extortion	Blackmail, information disclosure
Sabotage or vandalism	Destruction of systems or information
Software attacks	Viruses, worms, macros, denial of service
Technical hardware failures or errors	Equipment failure
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies
Theft	Illegal confiscation of equipment or information

intellectual property (IP)
Original ideas and inventions created, owned, and controlled by a particular person or organization; IP includes the representation of original ideas.

software piracy
The unauthorized duplication, installation, or distribution of copyrighted computer software, which is a violation of intellectual property.

availability disruption
A reduced level of service in an element of the critical infrastructure.

service level agreement (SLA)
A document or part of a document that specifies the expected level of service from a service provider. An SLA usually contains provisions for minimum acceptable availability and penalties or remediation procedures for downtime.

noise
The presence of additional and disruptive signals in network communications or electrical power delivery.

faults
Short-term interruptions in electrical power availability.

spikes
Short-term increases in electrical power availability, also known as swells.

surges
Long-term increases in electrical power availability.

sags
Short-term decreases in electrical power availability.

brownouts
Long-term decreases in the quality of electrical power availability.

Compromises to Intellectual Property

Many organizations create or support the development of **intellectual property (IP)** as part of their business operations. Intellectual property can be trade secrets, proprietary processes, copyrights, trademarks, and patents. IP is protected by copyright and other laws, carries the expectation of proper attribution or credit to its source, and potentially requires the acquisition of permission for its use, as specified in those laws. For example, the use of a song in a movie or a photo in a publication may require a specific payment or royalty. The unauthorized appropriation of IP constitutes a threat to information security.

Employees may have access privileges to the various types of IP owned by the organization, including purchased and developed software and organizational information. Many employees typically need to use IP to conduct day-to-day business. Compromises to IP typically occur in two primary areas:

- *Software piracy*—Organizations often purchase or lease the IP of other organizations, and must abide by purchase or licensing agreements for its fair and responsible use. The most common IP breach is the unlawful use or duplication of software-based intellectual property, more commonly known as **software piracy**. Many individuals and organizations do not purchase software as mandated by the owner's license agreements.
- *Copyright protection and user registration*—A number of technical mechanisms—digital watermarks, embedded code, copyright or activation codes, and even the intentional placement of bad sectors on software media—have been used to enforce copyright laws. The most common tool is a unique software registration code in combination with an end-user license agreement (EULA) that is usually displayed during the installation of new software, requiring users to indicate that they have read and agree to conditions of the software's use.

Deviations in Quality of Service

An organization's information system depends on the successful operation of many interdependent support systems, including power grids, data and telecommunications networks, utilities, parts suppliers, service vendors, and even janitorial staff and garbage haulers. Any of these support systems can be interrupted by severe weather, employee illnesses, or other unforeseen events. Deviations in quality of service can result from accidents such as a backhoe taking out an ISP's fiber-optic link or other accidents or disruptions. The backup provider may be online and in service but may be able to supply only a fraction of the bandwidth the organization needs for full service. This degradation of service is a form of **availability disruption**. Irregularities in Internet service, communications, and power supplies can dramatically affect the availability of information and systems. Some of the subcategories of this threat include the following:

- *Internet service issues*—In organizations that rely heavily on the Internet and the Web to support continued operations, ISP failures can considerably undermine the availability of information. When an organization places its Web servers in the care of a Web hosting provider, that provider assumes responsibility for all Internet services and for the hardware and operating system software used to operate the Web site. These Web hosting services are usually arranged with a **service level agreement (SLA)**.

- *Communications and other service provider issues*—Other utility services can affect organizations as well. Among these are telephone, water, wastewater, trash pickup, cable television, natural or propane gas, and custodial services.
- *Power irregularities*—Irregularities from power utilities are common and can lead to fluctuations such as power excesses, power shortages, and power losses. These fluctuations can pose problems for organizations that provide inadequately conditioned power for their information systems equipment. When power voltage levels vary from normal, expected levels, such as during a blackout, brownout, fault, **noise**, spike, surge, or sag, an organization's sensitive electronic equipment—especially networking equipment, computers, and computer-based systems, which are vulnerable to fluctuations—can be easily damaged or destroyed. Most good uninterruptible power supplies (UPS) can protect against **faults**, **spikes**, **surges**, **sags**, and even **brownouts** and **blackouts** of limited duration.

Espionage or Trespass

Espionage or **trespass** is a well-known and broad category of electronic and human activities that can breach the confidentiality of information. When an unauthorized person gains access to information an organization is trying to protect, the act is categorized as espionage or trespass. Attackers can use many different methods to access the information stored in an information system. Some forms of espionage are relatively low tech. One example, called **shoulder surfing**, is used in public or semipublic settings when people gather information they are not authorized to have. Another is *dumpster diving*, where adversaries rummage in refuse for valuable information. Acts of trespass can lead to unauthorized real or virtual actions that enable information gatherers to enter premises or systems without permission. Sound principles of authentication and authorization can help organizations protect valuable information and systems. These control methods and technologies employ multiple layers or factors to protect against unauthorized access and trespass.

The classic perpetrator of information espionage or trespass is the **hacker**, who spends long hours examining the types and structures of targeted systems and uses skill, guile, and/or fraud to attempt to bypass controls placed on information owned by someone else. Most hackers are grouped into two general categories—the *expert hacker* and the *novice hacker*. The **expert hacker** is usually a master of several programming languages, networking protocols, and operating systems, and exhibits a mastery of the technical environment of the chosen targeted system. A new category of expert hackers has emerged over the last decade. The **professional hacker** seeks to conduct attacks for personal benefit or the benefit of an employer, which is typically a crime organization or government-sponsored operation. The professional hacker should not be confused with the **penetration tester**, who has authorization from an organization to test its information systems and network defense and is expected to provide detailed reports of the findings. **Novice hackers** have little or no real expertise of their own but rely upon the skills of expert hackers, who often become dissatisfied with attacking systems directly and turn their attention to writing software. These programs are automated exploits that allow novice hackers to act as **script kiddies**, *mouse monkeys*, or **packet monkeys**.

After an attacker gains access to a system, the next step is to increase his or her privileges (**privilege escalation**). While most accounts associated with a system have only rudimentary "use" permissions and capabilities, the attacker needs administrative or "root" privileges.

blackouts
Long-term interruptions (outages) in electrical power availability.

trespass
Unauthorized entry into the real or virtual property of another party.

shoulder surfing
The direct, covert observation of individual information or system use.

hacker
A person who accesses systems and information without authorization and often illegally.

expert hacker
A hacker who uses an extensive knowledge of the inner workings of computer hardware and software to gain unauthorized access to systems and information. Also known as elite hackers, expert hackers often create automated exploits, scripts, and tools used by other hackers.

professional hacker
A hacker who conducts attacks for personal financial benefit or for a crime organization or foreign government. Not to be confused with a penetration tester.

penetration tester
An information security professional with authorization to attempt to gain system access in an effort to identify and recommend resolutions for vulnerabilities in those systems.

novice hackers
Relatively unskilled hackers who use the work of expert hackers to perform attacks. Also known as neophytes, n00bs, or newbies. This category of hackers includes script kiddies and packet monkeys.

script kiddies
Hackers of limited skill who use expertly written software to attack a system. Script kiddies are also known as skids, skiddies, or script bunnies.

packet monkeys
Script kiddies who use automated exploits to engage in denial-of-service attacks.

privilege escalation
The unauthorized modification of an authorized or unauthorized system user account to gain advanced access and control over system resources.

brute force password attack
An attempt to guess a password by trying every possible combination of characters and numbers in it.

dictionary password attack
A variation of the brute force password attack that attempts to narrow the range of possible passwords by using a list of common passwords and possibly including attempts based on the target's personal information.

rainbow table
A table of hash values and their corresponding plaintext values that can be used to look up password values if an attacker is able to steal a system's encrypted password file.

Password Attacks Password attacks fall under the category of espionage or trespass, just as lock-picking falls under breaking and entering. Attempting to guess or reverse-calculate a password is often called *password cracking*. There are a number of alternative approaches to password cracking:

- *Brute force*—The application of computing and network resources to try every possible password combination is called a **brute force password attack**.
- *Dictionary attacks*—The **dictionary password attack**, or simply dictionary attack, is a variation of the brute force attack that narrows the field using a dictionary of common passwords and includes information related to the target user, such as names of relatives or pets, and familiar numbers such as phone numbers, addresses, and even Social Security numbers.
- *Rainbow tables*—A far more sophisticated and potentially much faster password attack is possible if the attacker can gain access to an encrypted password file, such as the Security Account Manager (SAM) data file. These files can be quickly searched against a repository of possible encryption values (the **rainbow table**), and the corresponding plaintext value can be located.
- *Social engineering password attacks*—Using an approach commonly referred to as *pretexting*, attackers posing as an organization's IT professionals may attempt to gain access to systems information by contacting low-level employees and offering to help with their computer issues.

Forces of Nature

Forces of nature, sometimes called *Acts of God* or *force majeure*, can present some of the most dangerous threats because they usually occur with little warning and are beyond the control of people. Some typical force of nature attacks include the following:

- *Fire*—The ignition of combustible material; damage can also be caused by smoke from fires or by water from sprinkler systems or firefighters.
- *Flood*—Water overflowing into an area that is normally dry, causing direct damage, and subsequent indirect damage from high humidity and moisture.
- *Earthquake*—A sudden movement of the earth's crust caused by volcanic activity or the release of stress accumulated along geologic faults.
- *Lightning*—An abrupt, discontinuous, natural electric discharge in the atmosphere, which can cause direct damage through an electrical surge or indirect damage from fires. Damage from lightning can usually be prevented with specialized lightning rods and by installing special electrical circuit protectors.
- *Landslide or mudslide*—The downward slide of a mass of earth and rock. Landslides or mudslides also disrupt operations by interfering with access to buildings.
- *Tornados or severe windstorms*—Violent wind effects in which air moves at destructively high speeds, causing direct damage and indirect damage from thrown debris. A tornado is a rotating column of whirling air that can be more than a mile wide. Wind shear is a much smaller and more linear wind effect, but it can have similarly devastating consequences.
- *Hurricanes, typhoons, and tropical depressions*—Severe tropical storms that commonly originate at sea and move to land, bringing excessive rainfall, flooding, and high winds.
- *Tsunami*—A very large ocean wave caused by an underwater earthquake or volcanic eruption; it can reach miles inland as it crashes into landmasses.
- *Electrostatic discharge (ESD)*—Also known as static electricity, and usually little more than a nuisance. However, an employee walking across a carpet on a cool, dry day can generate up to 12,000 volts of electricity, and sensitive electronics can suffer damage from as little as 10 volts.
- *Dust contamination*—Can dramatically reduce the effectiveness of cooling mechanisms and potentially cause components to overheat. Specialized optical technology, such as CD or DVD drives, can suffer failures due to excessive dust contamination inside systems.

Human Error or Failure

This category includes acts performed without intent or malicious purpose or in ignorance by an authorized user. When people use information systems, mistakes happen. Errors also happen when people fail to follow the established policy.

Human error or failure often can be prevented with training, ongoing awareness activities, and controls. These controls range from simple activities, such as requiring the user to type a critical command twice, to more complex procedures, such as verifying commands by a second party. Some common types of human error include the following:

- *Social engineering*—There are several **social engineering** techniques, which usually involve a perpetrator posing as a person who is higher in the organizational hierarchy than the victim.
- *Advance-fee fraud*—Another social engineering attack called the **advance-fee fraud (AFF)** involves schemes often using the names of legitimate companies, such as the Nigerian National Petroleum Company, to solicit information with the promise of large sums of money from a bank, government agency, long-lost relative, lottery, or other organization.
- *Phishing*—Some attacks are sent by e-mail and may involve schemes attempting to convince users that a valid organization needs their information. **Phishing** attacks use two primary techniques, often in combination with one another: URL manipulation and Web site forgery. In URL manipulation, attackers send an HTML–embedded e-mail message or a hyperlink whose HTML code opens a forged Web site. In Web forgery, the attacker copies the HTML code from a legitimate Web site and then modifies key elements.
- *Spear phishing*—While normal phishing attacks target as many recipients as possible, **spear phishing** involves an attacker sending a targeted message that appears to be from an employer, a colleague, or some other legitimate correspondent to a small group or even one person.
- *Pretexting*—**Pretexting**, sometimes referred to as phone phishing, is a pure social engineering attack in which the attacker calls a potential victim on the telephone and pretends to be an authority figure in order to gain access to private or confidential information.

Information Extortion

Information extortion, also known as *cyberextortion*, is common in the theft of credit card numbers. It involves the theft of information followed by a request for payment to the information's owner, with the threat of public release unless a demand is met. Recent information extortion attacks have involved specialized forms of malware known as **ransomware**. This attack is usually implemented with malware that is run on the victim's system as a result of phishing or spear-phishing attacks. (See the following section on software attacks.) The result is that the user's data is encrypted. Paying the adversary a ransom in a digital currency may or may not result in the victim receiving the encryption key to recover the data, which is why the U.S. Federal Bureau of Investigation (FBI) recommends not paying the ransom.[8]

In late 2015, ransomware took on a new level of danger. Prior to that time, organizations could reasonably assume that systems attacked by ransomware could be safely restored from backups, losing only hours or, at worst, days of data. In 2015, persistent and delayed ransomware attacks like those from Locky and Crypto were distributed that would either specifically target backups or remain dormant longer than had been previously seen, allowing the malware itself to be backed up with the rest of the organizations' data.[9] When the attack was triggered and the organizations' systems and data were locked up, recovery from backups only re-installed the ransomware.

social engineering

The process of using social skills to convince people to reveal access credentials or other valuable information to an attacker.

advance-fee fraud (AFF)

A form of social engineering, typically conducted via e-mail, in which an organization or some third party indicates that the recipient is due an exorbitant amount of money and needs only a small advance fee or personal banking information to facilitate the transfer. This may also involve prepayment for services with a payment larger than required; the overpayment is returned and then the initial payment is repudiated.

phishing

A form of social engineering in which the attacker provides what appears to be a legitimate communication (usually e-mail), but it contains hidden or embedded code that redirects the reply to a third-party site in an effort to extract personal or confidential information.

spear phishing

Any highly targeted phishing attack.

pretexting

A form of social engineering in which the attacker pretends to be an authority figure who needs information to confirm the target's identity, but the real object is to trick the target into revealing confidential information. Pretexting is commonly performed by telephone.

information extortion

The act of an attacker or trusted insider who steals information from a computer system and demands compensation for its return or for an agreement not to disclose the information. Also known as cyberextortion.

ransomware

Computer software specifically designed to identify and encrypt valuable information in a victim's system in order to extort payment for the key needed to unlock the encryption.