# 

# **Chapter 1**

**An Overview of Information Security and Risk Management**

|  |
| --- |
| **At a Glance** |

#### Instructor’s Manual Table of Contents

* Overview
* Objectives
* Teaching Tips
* Quick Quizzes
* Class Discussion Topics
* Additional Projects
* Additional Resources
* Key Terms

|  |
| --- |
| Lecture Notes |

# **Overview**

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 chapter 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.

# **Objectives**

* Define and explain information security
* Identify and explain the basic concepts of risk management
* List and discuss the components of contingency planning
* Describe the role of information security policy in the development of contingency plans

# **Teaching Tips**

**Introduction**

1. Begin the course by explaining that this text is about being prepared for the unexpected, being ready for such events as incidents and disasters. We call this contingency planning, and the sad fact is that most organizations do not incorporate it into their day-to-day business activities.
2. Discuss the effects that the September 11, 2001 attacks in New York, Pennsylvania and Washington D.C. had on contingency planning.

1. Introduce the term **information security**.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | Most people have never thought seriously about dealing with a major disaster. Pose these questions to students to raise their awareness of the need for disaster planning: If you knew that your company was going to burn to the ground tonight, what would you choose to take out of the building? Do you have an evacuation “hot list”? How long would it be before you could be up and running again in a new location? |

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | To learn more about information system risk management, visit: <http://www.sans.org/reading_room/whitepapers/auditing/introduction-information-system-risk-management_1204> |

**Information Security**

1. Introduce the terms **C.I.A. triangle**, **confidentiality**, **integrity**, and **availability**. Use Figure 1-1 to aid the discussion.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | There is a distinction between data and information, although the specifics are not agreed upon by everyone. It is generally accepted that data refers to raw facts, while information is data in a usable form, usually following some processing and interpretation. When talking about the value of a company’s information assets, this distinction becomes more important. |

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | Point out the importance of protecting information at all times, and in all places. Discuss the incident in which some of Bank of America’s backup tapes containing credit card information were lost in transit from one facility to another. |

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | To learn more about the C.I.A. triangle, visit: <http://it.med.miami.edu/x904.xml> |

**Key Information Security Concepts**

1. Introduce the terms **threat**, **asset**, **attack**, **threat-agent**, **vulnerability**, **well-known vulnerabilities**, **exploit**, **control**, **safeguard**, and **countermeasure**.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | Ask students to discuss how an employee might be considered a vulnerability. |

1. Use Table 1-1 to discuss the following threats to information security:

* **Trespass**: Point out that the classic perpetrator of deliberate acts of espionage or trespass is the hacker.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | DefCon is an annual convention of hackers that is held to share vulnerabilities and exploits. |

* **Software Attacks**: Introduce the terms **virus**, **worm**, **backdoor and trap door**, **polymorphism**, **propagation vectors**, and **malware hoaxes**.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | Most students will be familiar with these terms, but may not understand the differences between them. |

* **Human Error or Failure**: Discuss the difference between human error and failure.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | Human error or failure can result in catastrophic events. The immediate cause of the Chernobyl nuclear reactor disaster was a mismanaged electrical engineering experiment conducted by engineers with no knowledge of reactor physics. [www.pbs.org/wgbh/pages/frontline/shows/reaction/readings/chernobyl.html](http://www.pbs.org/wgbh/pages/frontline/shows/reaction/readings/chernobyl.html) |

* **Theft**: Introduce the terms **competitive intelligence** and **espionage**.
* **Compromises to Intellectual Property**: Discuss the risks involved in “bring your own device” (or BYOD) systems.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | To learn about some famous cases of corporate espionage, visit: <http://images.businessweek.com/slideshows/20110919/famous-cases-of-corporate-espionage#slide2> |

* **Sabotage or Vandalism**: Introduce the term **cyberterrorist**.
* **Technical Software Failures or Errors**: Introduce the term **trap door** and discuss its security implications.
* **Technical Hardware Failures or Errors**: Point out that technical hardware failures or errors occur when a manufacturer distributes equipment containing a known or unknown flaw.
* **Forces of Nature**: Discuss the reasons why these threats are considered the most dangerous.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | See the following site for lessons learned from the Japanese earthquake, tsunami, and nuclear disaster: <http://www.pkfindia.in/Value%20Adds/Lessons%20from%20the%20disasters%20in%20Japan.pdf> |

* **Deviations in Quality of Service by Service Providers**: Note that Internet service, communications, and power irregularities can dramatically affect the availability of information and systems.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | Ask students to discuss the impact the total loss of telephone communications (both landlines and cell phones) would have on their companies. |

* **Technological Obsolescence**: Point out that IT professionals play a large role in the identification of obsolescence.
* **Information Extortion**: Note that extortion is common in credit card number theft.
* **Other Threats Listings**: Use Table 1-2 to discuss computer crime.

**Quick Quiz 1**

1. Objects, persons, or other entities that pose a potential risk of loss to an asset are called \_\_\_\_.

Answer: threats

1. Name the three critical elements of the C.I.A. triangle.

Answer: confidentiality, integrity, and availability

1. A targeted solution to misuse a specific vulnerability is called a(n) \_\_\_\_.

Answer: exploit

1. \_\_\_\_ is the protection of the confidentiality, integrity, and availability of information, whether in storage, during processing, or in transmission.

Answer: Information security (InfoSec)

**Overview of Risk Management**

1. Introduce the terms **risk identification** and **risk control**. Use Figure 1-2 to aid the discussion.
2. Introduce the term **risk management**.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | Without a formal approach to risk management, a company is highly likely to be unable to mitigate the impact of a major incident. |

**Know Yourself**

1. Point out that just because you have a control in place to protect an asset does not necessarily mean that the asset is protected.

**Know the Enemy**

1. Note that it is essential that all stakeholders conduct periodic management reviews.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | Point out the importance of including all departments within the company in this process, as people in different areas of activities will have unique insights into various aspects of threats and control strategies. |

**Risk Identification**

1. Use Figure 1-3 to discuss the components of risk identification.
2. The following topics should also be discussed:

* **Asset Identification and Value Assessment**: Discuss information asset classification and information asset evaluation.
* **Data Classification and Management**: Introduce the terms **security clearance** and **need to know**.
* **Threat Identification:** Introduce the term **threat assessment**.
* **Vulnerability Identification**: Note that the process of listing vulnerabilities works best when groups of people with diverse backgrounds work iteratively in a series of brainstorming sessions.

**Risk Assessment**

1. Risk assessment assigns a risk rating or score to each information asset. Note that although this number does not mean anything in absolute terms, it is useful in gauging the relative risk to each vulnerable information asset and facilitates the development of comparative ratings later in the risk control process. Use Figure 1-4 to aid the discussion.
2. The following topics should also be discussed:

* **Likelihood**: Point out that in risk assessment, you assign a numeric value to the likelihood of a vulnerability being successfully exploited.
* **Valuation of Information Assets**: Explain that it is impossible to know everything about each vulnerability, such as how likely it is to occur or how great an impact a successful attack would have.
* **Risk Determination**: Discuss the definition of risk.
* **Qualitative Risk Management**: Introduce the term **residual risk**.
* **Identify Possible Controls**: Discuss the three general categories of controls, according to the CNSS model: policies, programs (education and training), and technologies.

**Risk Control Strategies**

1. Explain that once the project team for information security development has created the ranked vulnerability worksheet, it must choose one of the following five approaches for controlling the risks that result from the vulnerabilities:

* **Defense**: Note that there are three common methods of risk defense: defense through application of policy, defense through application of training and education programs, and defense through application of technology.
* **Transference**: This approach attempts to shift the risk to other assets, other processes, or other organizations.
* **Mitigation**: This approach attempts to reduce the impact caused by the exploitation of vulnerability through planning and preparation.
* **Acceptance**: This approach chooses to do nothing to protect the information asset. Instead, it accepts the outcome of its potential exploitation.
* **Termination:** Note that sometimes, the cost of protecting an asset outweighs its value.

**Quick Quiz 2**

1. \_\_\_\_ is the process of examining, documenting, and assessing the security posture of an organization’s information technology and the risks it faces.

Answer: Risk identification

1. \_\_\_\_ is the process of applying controls to reduce the risks to an organization’s data and information systems.

Answer: Risk control

1. The process of assigning a risk rating or score to an information asset is called \_\_\_\_.

Answer: risk assessment

1. \_\_\_\_ is the risk that remains to the information asset even after the existing control has been applied.

Answer: Residual risk

**Contingency Planning and Its Components**

1. Introduce the term **contingency plan**.

**Business Impact Analysis**

1. Note that business impact analysis is a crucial component of the initial planning stages, as it provides detailed scenarios of the potential impact each attack could have on the organization.

**Incident Response Plan**

1. Introduce the term **incident**.
2. Explain that in the event of a serious virus or worm outbreak, the IR plan may be used to assess the likelihood of imminent damage and to inform key decision makers in the various communities of interest.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | Stress the importance of doing damage control without obliterating the forensic evidence. Because decisions made in the heat of the crisis are rarely well thought out, creating and rehearsing a plan in advance of an incident is critical. |

**Disaster Recovery Plan**

1. Note that in many regards, the DR plan is an extension to the IR plan that covers disastrous events.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | Ensure that students understand the distinction between the Incident Response Plan and the Disaster Recovery Plan. |

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | Sudden loss of key personnel, especially high-level management, is another type of “disaster” that requires advance planning, particularly when the loss is due to death. |

**Business Continuity Plan**

1. Discuss the difference between a business continuity plan and a business resumption plan.

**Contingency Planning Timeline**

1. Use Figures 1-5 and 1-6 to review the steps involved in contingency planning.
2. Use Figure 1-7 and Table 1-4 to discuss the seven steps involved in NIST SP 800-34, Revision 1.
3. Use Figure 1-8 to illustrate how the various plans referenced in SP 800-34 relate to one another.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | Formal training for all personnel involved in the detection and recovery processes should occur on a regular basis to ensure that actions to be taken are well known and practiced. |

**Role of Information Security Policy in Developing Contingency Plans**

1. Emphasize that quality security programs begin and end with policy.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | Without clearly defined and enforced policies in place, the effectiveness of a contingency plan will be seriously compromised. The organization also may be exposing itself to legal liabilities. |

**Key Policy Definitions**

1. Introduce the terms **policy**, **standards**, **de facto standards**, and **de jure standards**. Use Figure 1-9 to aid the discussion.
2. Introduce the terms **mission**, **vision**, **strategic planning**, and **information security policy**.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | Many students will be familiar with the concept of missions, as early Web site construction tools asked for a mission statement as part of the process of creating a company Web site. |

**Enterprise Information Security Policy**

1. Note that the EISP guides the development, implementation, and management of the security program. It contains the requirements to be met by the information security blueprint or framework.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | Stress the fact that policy must not only define the actions and expectations, but must also define the consequences of failure to follow the policy. Policy without enforcement will have limited impact. |

**Issue-Specific Security Policy**

1. Discuss the three approaches to creating and managing ISSPs.
2. Table 1-5 shows a sample ISSP. Note that this can be used as a template to enable an organization to address all the key points of such a policy.
3. Briefly discuss each of the following areas presented in Table 1-5:

* Statement of Policy
* Authorized Access and Usage of Equipment
* Prohibited Usage of Equipment
* Systems Management
* Violations of Policy
* Policy Review and Modification
* Limitations of Liability

**Systems-Specific Policy**

1. Explain that SysSPs can be organized into two groups:

* Access control lists (ACLs)
* Configuration rules

1. The following topics should also be discussed:

* **ACL Policies**: ACLs allow a configuration to set restrictions for a particular user, computer, time, duration—even a particular file.
* **Rule Policies**: Many security systems require specific configuration scripts that tell the systems what actions to perform on each set of information they process.

**Policy Management**

1. Point out that policies are living documents that must be nurtured, given that they are constantly changing and growing. They must be properly disseminated (distributed, read, understood, and agreed to) and managed.

**Quick Quiz 3**

1. A(n) \_\_\_\_ is used to anticipate, react to, and recover from events that threaten the security of information and information assets in the organization.

Answer: contingency plan

1. A(n) \_\_\_\_ is a document that describes how, in the event of a disaster, critical business functions will continue at an alternate location while the organization recovers its ability to function at the primary site—as supported by the DR plan.

Answer: business continuity plan (BC plan)

1. \_\_\_\_ is the process of moving the organization toward its vision.

Answer: Strategic planning

1. A(n) \_\_\_\_ is a plan or course of action used by an organization to convey instructions from its senior management to those who make decisions, take actions, and perform other duties on behalf of the organization.

Answer: policy

# **Class Discussion Topics**

1. Does your company (or school) have a current disaster recovery plan? What are some of the activities involved in it? Do you feel confident that your company (or school) is prepared to survive a major disaster? Why or why not?
2. Has your company (or school) been the target of a network or system intrusion? What information was targeted? Was the attack successful? If so, what changes has your company (or school) made to ensure that this vulnerability has been controlled?

# **Additional Projects**

1. Select a major organization that was located in the Hurricane Katrina disaster area. Research their experiences and prepare a report detailing the unexpected challenges the organization encountered in returning their operations to normal. Give suggestions on what might be added to the organization’s contingency plan to mitigate those unexpected challenges.

Prepare a comparison chart for disasters caused by major forces of nature (hurricane, tornado, earthquake, flood, and fire). List specific aspects of the incident response plan and the disaster recovery plan that would be different depending on the type of disaster.

# **Additional Resources**

1. Discussion of the actual causes of the Chernobyl nuclear reactor disaster:

[www.pbs.org/wgbh/pages/frontline/shows/reaction/readings/chernobyl.html](http://www.pbs.org/wgbh/pages/frontline/shows/reaction/readings/chernobyl.html)

1. Cyberterrorism: <http://www.huffingtonpost.com/dorian-de-wind/cyberterrorism-a-grave_b_2867430.html>
2. Cyberterrorism: <http://www.washingtonpost.com/blogs/post-partisan/wp/2013/03/29/is-the-u-s-prepared-for-cyberterrorism/>

**Key Terms**

* **Acceptance**: a risk control strategy in which you understand the consequences and accept the risk without controls or mitigation
* **Asset**: an organizational resource that is being protected
* **Attack**: an intentional or unintentional attempt to cause damage or otherwise compromise information
* **Availability**: enables authorized users or systems to access information without interference or obstruction, in the required format
* **Avoidance**: a risk control strategy in which you apply safeguards that eliminate or reduce the remaining uncontrolled risks
* **Business continuity plan** (**BCP**): expresses how to ensure that critical business functions continue at an alternate location after a catastrophic incident or disaster
* **Business impact analysis** (**BIA**): investigation and assessment of the impact of attacks
* **Business resumption plan** (**BRP**): merges the Disaster Recovery Plan and Business Continuity Plan into a single process
* **C.I.A. triangle**: the three most critical characteristics of information used within information systems: confidentiality, integrity, and availability
* **Confidentiality**:when disclosure or exposure to unauthorized individuals or systems is prevented
* **Contingency plan**: a plan to anticipate, react to, and recover from events that threaten assets; focuses on steps required to restore normal operations
* **Control**, **safeguard**, or **countermeasure**: security mechanisms, policies, or procedures to successfully counter attacks, reduce risk, resolve vulnerabilities and improve security
* **Cyberterrorist**: hacks systems to conduct terrorist activities through network or Internet pathways
* **De facto standard**: informal standard
* **De jure standard**: formal standard
* **Disaster recovery plan** (**DRP**): deals with preparation for and recovery from a natural or man-made disaster
* **Enterprise information security policy** (**EISP**): an executive-level document that contains the requirements for all security efforts that must be met
* **Exploit**: illegal use of a system or information asset, or a targeted solution to misuse a specific hole or vulnerability
* **Hacker**: uses software to gain access to information illegally
* **Incident response plan** (**IRP**): deals with the identification, classification, response, and recovery from an incident
* **Incident**: any clearly identified attack on assets
* **Information security** (**InfoSec**): the protection of the confidentiality, integrity, and availability of information in storage, during processing or in transmission
* **Information security policy**: provides rules for the protection of information assets
* **Integrity**: prevention of corruption, damage, destruction, or other disruption of information
* **Intellectual property (IP)**: The ownership of ideas and control over the tangibles or virtual representation of those ideas
* **Issue-specific security policy** (**ISSP**): addresses specific areas of technology
* **Likelihood**: the probability that a specific vulnerability within an organization will be successfully attacked
* **Malware**: malicious code or malicious software components designed to damage, destroy, or deny service to the target system
* **Mission**: a written statement of an organization’s purpose
* **Mitigation**: a risk control strategy in which you reduce the impact of a vulnerability in the event that it is exploited
* **Need to know**: before someone can access a specific set of data, the need-to-know requirement must be met. This extra level of protection ensures that the confidentiality of information is properly maintained
* **Policy**: an organizational law that dictates acceptable and unacceptable behavior, and defines penalties for violations
* **Residual risk**: risk that remains after a control has been applied
* **Risk assessment**: assigns a risk rating or score to each information asset
* **Risk control**: the process of applying controls to reduce the risks to data and information systems
* **Risk identification**: the process of examining and documenting the security posture of an organization’s information technology
* **Risk management**: a formal process of identifying and controlling risks to an organization’s information assets
* **Security clearance**: a means of classifying personnel with respect to information security, resulting in various levels of access to confidential materials
* **Standard**: detailed statement of what must be done to comply with policy
* **Strategic planning**: process of moving the organization toward its vision
* **Systems-specific security policies** (**SysSPs**): standards and procedures to be used when configuring or maintaining systems
* **Termination**: Removal of the asset or function from the environment that represents risk
* **Threat assessment**: each of the threat categories must be assessed regarding its potential to endanger the organization
* **Threat**: a category of objects, persons, or other entities that pose a potential risk of loss to an asset
* **Threat-agent**: a specific and identifiable instance of a general threat
* **Transference**: an approach that attempts to shift the risk to other assets, other processes, or other organizations
* **Vision**: written statement about organization’s goals
* **Vulnerability**: a weakness or fault in the protection mechanisms for information assets
* **Well-known vulnerabilities**: vulnerabilities that have been examined, documented, and published