Security Risk Management and Ethics

Chapter One:
Introduction to Security Risk Management

Textbook : Freund, J., & Jones, J, "*Measuring and managing information risk: A FAIR Approach*", 1st Edition, Butterworth-Heinemann, 2015. ISBN-13: 9780127999326.

Chapter1: Topics

This chapter covers the following topics and concepts:

- What risk is and what its relationship to threat, vulnerability, and loss is.
- What the major components of risk to an IT infrastructure are.
- What risk management is and how it is important to the business.
- What some risk identification techniques are.
- What some risk management techniques are.

Chapter1: Goals

When you complete this chapter, you will be able to:

- Define risk
- Identify the major components of risk
- Describe the relationship between threats and vulnerabilities, and impact
- Define risk management
- Describe risk management's relationship with profitability and survivability
- Explain the relationship between the cost of loss and the cost of risk management

Chapter 1 Goals Cont.,

- Describe how risk is perceived by different roles within an organization
- Identify threats
- List the different categories of threats
- Describe techniques to identify vulnerabilities
- Identify and define risk management techniques

What Is Risk?

- Risk is the likelihood that a loss will occur. Losses occur when

a threat exposes a vulnerability.

- Organizations of all sizes face risks. Some risks are so severe they cause a business to fail. Other risks are minor and can be accepted without another thought.
- Organizations use risk management techniques to identify and differentiate severe risks from minor risks.
- When this is done properly, administrators and managers can intelligently decide what to do about any type of risk.
- Thus, the end result is a decision to avoid, transfer, mitigate, or accept a risk.

What Is Risk? Cont.,

- The common themes of these definitions are threat, vulnerability, and loss.
- Here's a short definition of each of these terms:
  - Threat—A threat is any activity that represents a possible danger.
  - Vulnerability—A vulnerability is a weakness.
  - Loss—A loss results in a compromise to business functions or assets.
- Risks to organizations can result in a loss that negatively affects the business.
- The overall goal is to reduce the losses that can occur from risk.

Classified the Effect of Risks on Businesses

• Organization losses can be categorized in to three levels:

- (1) Business functions

- (2) Business assets

- (3) Driver of business costs

(1) Business functions

- Business functions are the activities a business performs to provide services or sell products.

- If any of these functions are negatively affected by any type of security risks, the organization won't be able to sell as much. The organization will earn less revenue, resulting in an overall loss in terms of customers or profits.

Examples of Business functions and possible risks:

- A Web site sells products on the Internet. If the Web site is attacked and fails, sales are lost.
- Authors write articles that must be submitted by a deadline to be published. If the author's PC becomes infected with a virus, the deadline passes and the article's value is reduced.
- Analysts compile reports used by management to make decisions. Data is gathered from internal servers and Internet sources. If network connectivity fails, analysts won't have access to current data. Management could make decisions based on inaccurate information.

Examples of business Cont.,

• A warehouse application is used for shipping products that have been purchased. It identifies what has been ordered, where the products need to be sent, and where they are located. If the application fails, products aren't shipped on time.

(2) Business assets

• A business asset is anything that has measurable value to a company. If an asset has the potential of losing value, it is at risk.

• Value is defined as the worth of an asset to a business.

• Value can often be expressed in monetary terms, such as $5,000.

• Assets can have both tangible and intangible values.

•The tangible value is the actual cost of the asset.

•The intangible value is value that cannot be measured by cost, such as client confidence.

(2) Business assets Cont..,

Some examples of tangible assets are:

- Computer systems—Servers, desktop PCs, and mobile computers are all tangible assets.
- Network components—Routers, switches, firewalls, and any other components necessary to keep the network running are assets.
- Software applications—Any application that can be installed on a computer system is considered a tangible asset.
- Data—This includes the large-scale databases that are integral to many businesses. It also includes the data used and manipulated by each employee or customer.

(2) Business assets Cont..,

• One of the early steps in risk management is associated with identifying the assets of a company and their associated costs. This data is used to prioritize risks for different assets. Once a risk is prioritized, it becomes easier to identify risk management processes to protect the asset.

Example the effect risk on Business assets

• Imagine that your company sells products via a Web site. The Web site earns $5,000 an hour in revenue. Now, imagine that the Web server hosting the Web site fails and is down for two hours. The costs to repair it total $1,000. What is the tangible loss?

- Lost revenue—$5,000 times two hours 5 $10,000
- Repair costs—$1,000
- Total tangible value—$11,000

Example the effect risk on Business assets Cont..,

The intangible value isn't as easy to calculate but is still very important.

Imagine that several customers tried to make a purchase when the Web site was down. If the same product is available somewhere else, they probably bought the product elsewhere. That lost revenue is the tangible value.

However, if the experience is positive with the other business, where will the customers go the next time they want to purchase this product? It's very possible the other business has just gained new customers and you have lost some.

Example the effect risk on Business assets Cont..,

- The intangible value includes:
- Future lost revenue—Any additional purchases the customers make with the other company is a loss to your company.
- Cost of gaining the customer—A lot of money is invested to attract customers.

Notes:

- It is much easier to sell to a repeat customer than it is to acquire a new customer.
- If you lose a customer, you lose the investment.

Example the effect risk on Business assets Cont..,

- The intangible value includes:

(1) Future lost revenue—Any additional purchases the customers make with the other company is a loss to your company.

(2) Cost of gaining the customer—A lot of money is invested to attract customers. It is much easier to sell to a repeat customer than it is to acquire a new customer. If you lose a customer, you lose the investment.

(3) Customer influence—Customers have friends, families, and business partners. They commonly share their experience with others, especially if the experience is exceptionally positive or negative.

(3) Driver of Business Costs

- Risk is also a driver of business costs. Once risks are identified, steps can be taken to reduce or manage the risk.
- Risks are often managed by implementing countermeasures or controls.
- The costs of managing risk need to be considered in total business costs.
- If too much money is spent on reducing risk, the overall profit is reduced. If too little money is spent on these controls, a loss could result from an easily avoidable threat and/or vulnerability.

(3) Driver of Business Costs Cont…., Profitability Vs Survivability

- Both profitability and survivability must be considered when considering risks.

- Profitability: The ability of a company to make a profit. Profitability is calculated as revenues minus costs.

- Survivability : The ability of a company to survive loss due to a risk. Some losses such as fire can be disastrous and cause the business to fail.

Profitability Vs Survivability Cont.…,

• In terms of profitability, a loss can ruin a business. In terms of survivability, a loss may cause a company never to earn a profit.

• The costs associated with risk management don't contribute directly to revenue gains. Instead, these costs help to ensure that a company can continue to operate even if it incurs a loss.

Profitability Vs Survivability Cont.…,

• In terms of profitability, a loss can ruin a business. In terms of survivability, a loss may cause a company never to earn a profit.

• The costs associated with risk management don't contribute directly to revenue gains. Instead, these costs help to ensure that a company can continue to operate even if it incurs a loss.

Profitability Vs Survivability Cont.…,

• When considering profitability and survivability, you will want to consider the following items:

(1) Out-of-pocket costs—The cost to reduce risks comes from existing funds.

(2) Lost opportunity costs—Money spent to reduce risks can't be spent elsewhere. This may result in lost opportunities if the money could be used for some other purpose.

Profitability Vs Survivability Cont.…,

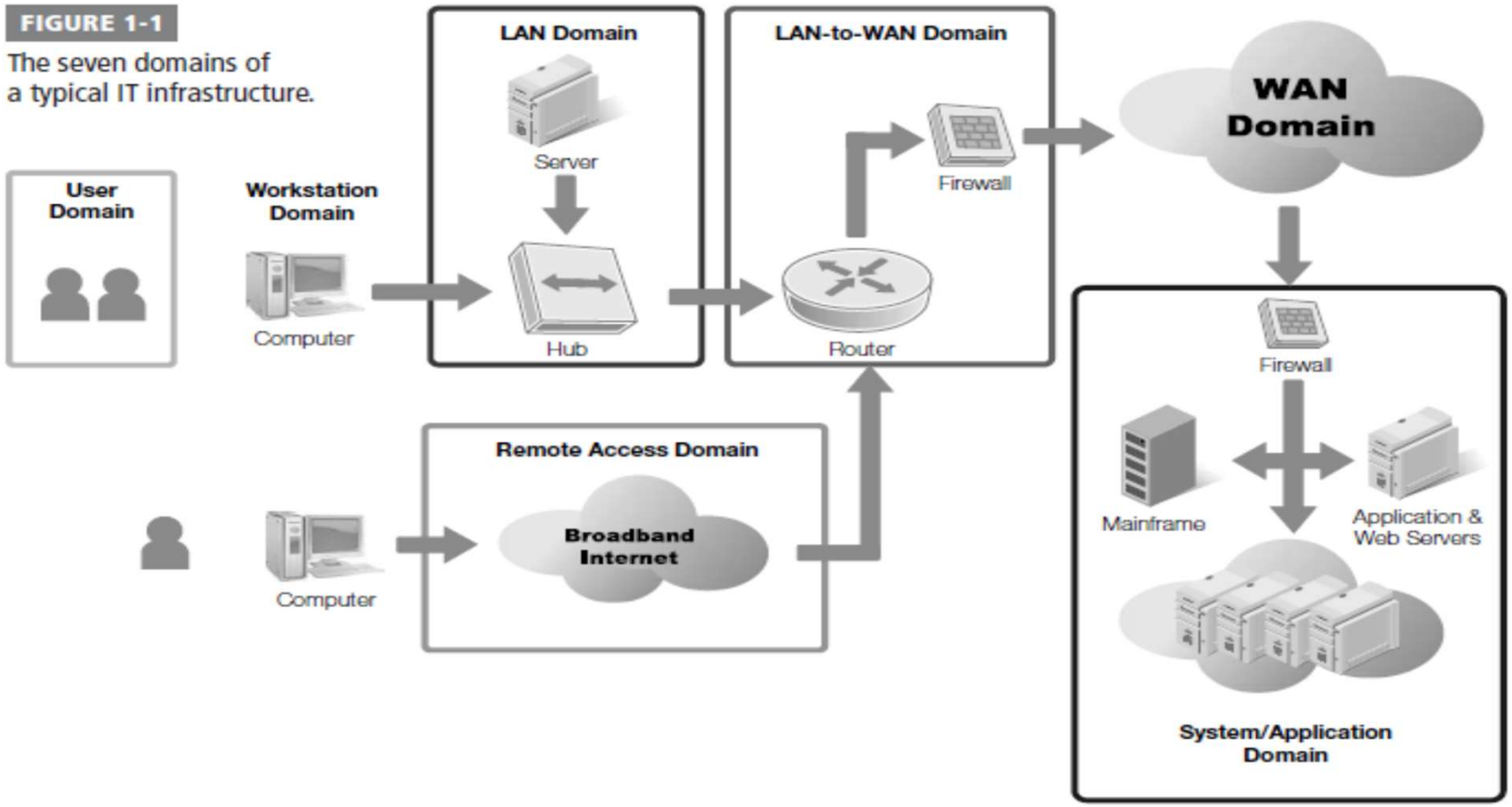
(3) Future costs—Some countermeasures require ongoing or future costs. These costs could be for renewing hardware or software. Future costs can also include the cost of employees to implement the countermeasures.

(4) Client/stakeholder confidence—The value of client and stakeholder confidence is also important. If risks aren't addressed, clients or stakeholders may lose confidence when a threat exploits a vulnerability, resulting in a significant loss to the company.

Example the risk on Driver of Business Costs

- Consider antivirus software. The cost to install antivirus software on every computer in the organization can be quite high. Every dollar spent reduces the overall profit, and antivirus software doesn't have the potential to add any profit.
- However, what's the alternative? If antivirus software is not installed, every system represents a significant risk. If any system becomes infected, a virus could release a worm as a payload and infect the entire network. Databases could be corrupted. Data on file servers could be erased. Email servers could crash. The entire business could grind to a halt. If this happens too often or for too long the business could fail.

What Are the Major Components of Risk to an IT Infrastructure?



Seven Domains of a Typical IT Infrastructure

- There are a lot of similarities between different IT organizations.
- For example, any IT organization will have users and computers.

There are seven domains of a typical IT infrastructure.

- Figure 1.1 shows the seven domains of a typical IT infrastructure.

- When considering risk management, you can examine each of these domains separately. Each domain represents a possible target for an attacker.

Seven Domains of a Typical IT Infrastructure Cont.…,

- Some attackers have the skills and aptitudes to con users so they focus on the User Domain. Other attackers may be experts in specific applications so they focus on the System/Application Domain.
- An attacker only needs to be able to exploit vulnerabilities in one domain of the seven domains.
- However, a business must provide protection in each of the domains. A weakness in any one of the domains can be exploited by an attacker even if the other six domains have no vulnerabilities.

(1) Risk on the User Domain

- The User Domain includes people. They can be users, employees, contractors, or consultants. The old phrase that a chain is only as strong as its weakest link applies to IT security too. People are often the weakest link in IT security.
- Business could have the strongest technical and physical security available. However, if personnel don't understand the value of security, the security can be bypassed. For example, technical security can require strong, complex passwords that can't be easily cracked.
- However, a social engineer can convince an employee to give up the password. This called "Social Engineering".

(1) Risk on the User Domain Cont.…,

- Some users assume that no one will ever think of looking at the sticky note under their keyboard.

- Users can visit risky Web sites, and download and execute infected software. They may unknowingly bring viruses from home via universal serial bus (USB) thumb drives. When they plug in the USB drive the work computer becomes infected. This in turn can infect other computers and the entire network.

(1) Risk on the User Domain Cont.…, Example of Social Engineering

Demystifying Social Engineering

Social engineering is a common technique used to trick people into revealing sensitive information. Leonardo DiCaprio played Frank Abagnale in the movie *Catch Me If You Can*, which demonstrated the power of social engineering. A social engineer doesn't just say "give me your secrets." Instead, the attacker uses techniques such as flattery and conning.

A common technique used in vulnerability assessments is to ask employees to give their user name and password. The request may come in the form of an e-mail, a phone call, or even person-to-person.

One common method used in vulnerability assessments is to send an e-mail requesting a user name and password. The e-mail is modified so that it looks as if it's coming from an executive. The e-mail adds a sense of urgency and may include a reference to an important project. From the user's perspective here's what they receive:

From: CEO

Subj: Project upgrade

All,

The XYZ project is at risk of falling behind. As you know this is integral to our success in the coming year. We're having a problem with user authentication. We think it's because passwords may have special characters that aren't recognized.

I need everyone to reply to this e-mail with your user name and password. We must complete this test today so please respond as soon as you receive this e-mail.

Thanks for your assistance.

When employees are trained to protect their password, they usually recognize the risks and don't reply. However, it has been shown that when employees aren't trained, as many as 70 percent of the employees may respond.

(2) Risk on Workstation Domain

- The workstation is the end user's computer. The workstation is susceptible to malicious software, also known as malware.
- The workstation is vulnerable if it is not kept up to date with recent patches.
- If antivirus software isn't installed, the workstation is also vulnerable.
- If a system is infected, the malware can cause significant harm. Some malware infects a single system.
- Other malware releases worm components that can spread across the network.
- Antivirus companies regularly update virus definitions as new malware is discovered.

(2) Risk on Workstation Domain Cont.,

- In addition to installing the antivirus software, companies must also update software regularly with new definitions. If the antivirus software is installed and up to date, the likelihood of a system becoming infected is reduced.
- Bugs and vulnerabilities are constantly being discovered in operating systems and applications. Some of the bugs are harmless. Others represent significant risks.
- Microsoft and other software vendors regularly release patches and fixes that can be applied. When systems are kept updated, these fixes help keep the systems protected. When systems aren't updated, the threats can become significant.

(3) Risk on LAN Domain

- The LAN Domain is the area that is inside the firewall. It can be a few systems connected together in a small home office network. It can also be a large network with thousands of computers.
- Each individual device on the network must be protected or all devices can be at risk.
- Network devices such as hubs, switches, and routers are used to connect the systems together on the local area network (LAN). The internal LAN is generally considered a trusted zone. Data transferred within the LAN isn't protected as thoroughly as if it were sent outside the LAN.
- As an example, sniffing attacks occur when an attacker uses a protocol analyzer to capture data packets.

(3) Risk on LAN Domain Cont.,

- A protocol analyzer is also known as a sniffer. An experienced attacker can read the actual data within these packets.
- If hubs are used instead of switches, there is an increased risk of sniffing attacks. An attacker can plug into any port in the building and potentially capture valuable data.
- If switches are used instead of hubs, the attacker must have physical access to the switch to capture the same amount of data. Most organizations protect network devices in server rooms or wiring closets.
- NOTE : Many organizations outlaw the use of hubs within the LAN. Switches are more expensive. However, they reduce the risk of sniffing attacks.

(4) Risk on LAN-to-WAN Domain

- The LAN-to-WAN Domain connects the local area network to the wide area network (WAN). The LAN Domain is considered a trusted zone since it is controlled by a company.
- The WAN Domain is considered an untrusted zone because it is not controlled and is accessible by attackers.
- The area between the trusted and untrusted zones is protected with one or more firewalls. This is also called the boundary, or the edge.
- Security here is referred to as boundary protection or edge protection.

(4) Risk on LAN-to-WAN Domain Cont.

- The public side of the boundary is often connected to the Internet and has public Internet Protocol (IP) addresses. These IP addresses are accessible from anywhere in the world, and attackers are constantly probing public IP addresses.

- They look for vulnerabilities and when one is found, they pounce.

- A high level of security is required to keep the LAN-to--WAN Domain safe.

(5) Risk on Remote Access Domain

- Mobile workers often need access to the private LAN when they are away from the company.
- Remote access is used to grant mobile workers this access.
- Remote access can be granted via direct dialup connections or using a virtual private network (VPN) connection.
- A VPN provides access to a private network over a public network.
- The public network used by VPNs is most commonly the Internet. Since the Internet is largely untrusted and has known attackers, remote access represents a risk.

(5) Risk on Remote Access Domain Cont.,

- Attackers can access unprotected connections. They can also try to break into the remote access servers. Using a VPN is an example of a control to lessen the risk. But VPNs have their vulnerabilities, too.

- Vulnerabilities exist at two stages of the VPN connection:

(1) The first stage is authentication. Authentication is when the user provides credentials to prove identity. If these credentials can be discovered, the attacker can later use them to impersonate the user.

(2) The second stage is when data is passed between the user and the server. If the data is sent in clear text, an attacker can capture and read the data.

(5) Risk on Remote Access Domain Cont.,

NOTE:

VPN connections use tunneling protocols to reduce the risk of data being captured. A tunneling protocol will encrypt the traffic sent over the network. This makes it more difficult for attackers to capture and read data.

(6) Risk on WAN Domain

- For many businesses, the WAN is the Internet. However, a business can also lease semiprivate lines from private telecommunications companies.
- These lines are semiprivate because they are rarely leased and used by only a single company. Instead, they are shared with other unknown companies.
- As mentioned in the LAN-to-WAN Domain, the Internet is an untrusted zone. Any host on the Internet with a public IP address is at significant risk of attack.

(6) Risk on WAN Domain Cont.,

- Moreover, it is fully expected that any host on the Internet will be attacked.
- Semiprivate lines aren't as easily accessible as the Internet. However, a company rarely knows who else is sharing the lines.
- These leased lines require the same level of security provided to any host in the WAN Domain.
- A significant amount of security is required to keep hosts in the WAN Domain safe.

(7) Risk on System/Application Domain

- The System/Application Domain refers to servers that host server level applications.
- Mail servers receive and send email for clients. Database servers host databases that are accessed by users, applications, or other servers.
- Domain Name System (DNS) servers provide names to IP addresses for clients.
- You should always protect servers using best practices: Remove unneeded services and protocols. Change default passwords.
- Regularly patch and update the server systems. Enable local firewalls.

(7) Risk on System/Application Domain

- One of the challenges with servers in the System/Application Domain is that the knowledge becomes specialized. People tend to focus on areas of specialty.

- For example, common security issues with an email server would likely be known only by technicians who regularly work with the email servers.
- NOTE:

You should lock down a server using the specific security requirements needed by the hosted application. An e-mail server requires one set of protections while a database server requires a different set.

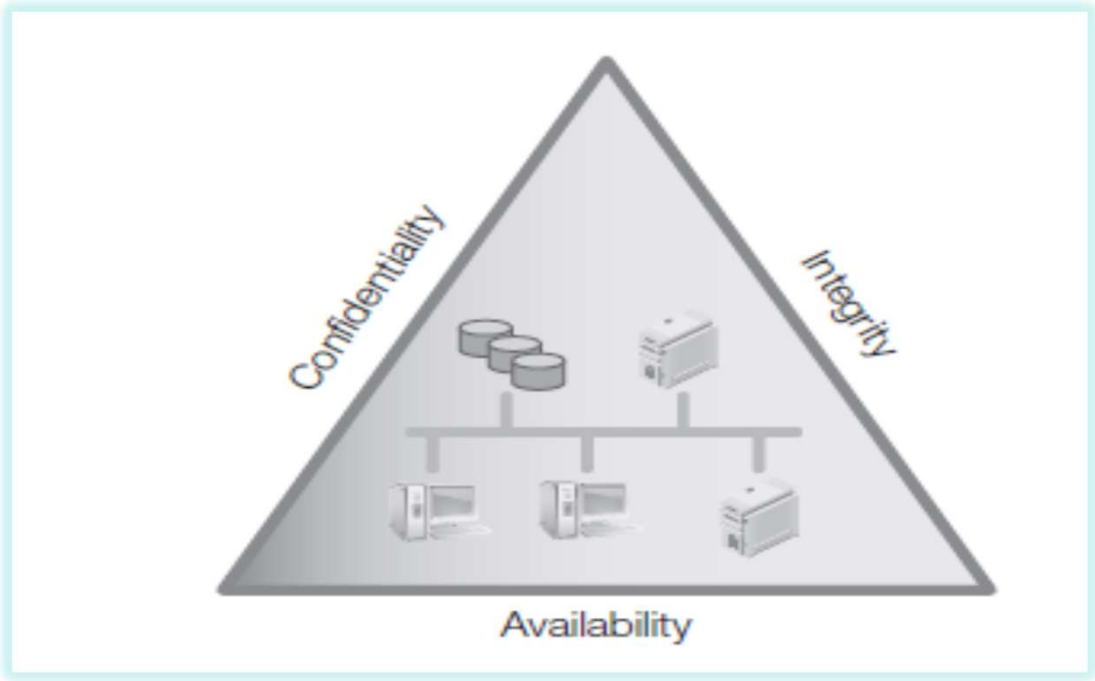
Threats, Vulnerabilities, and Impact

- When a threat exploits a vulnerability it results in a loss. The impact identifies the severity of the loss.
- A threat is any circumstance or event with the potential to cause a loss. You can also think of a threat as any activity that represents a possible danger. Threats are always present and cannot be eliminated, but they may be controlled.
- Threats have independent probabilities of occurring that often are unaffected by an organizational action. As an example, an attacker may be an expert in attacking Web servers hosted on Apache. There is very little a company can do to stop this attacker from trying to attack. However, a company can reduce or eliminate vulnerabilities to reduce the attacker's chance of success.

Threats, Vulnerabilities, and Impact

- Threats are attempts to exploit vulnerabilities that result in the loss of confidentiality, integrity, or availability of a business asset.
- The protection of confidentiality, integrity, and availability are common security objectives for information systems.
- Figure 1.2 shows these three security objectives as a protective triangle. If any side of the triangle is breached or fails, security fails.
- In other words, risks to confidentiality, integrity, or availability represent potential loss to an organization. Because of this, a significant amount of risk management is focused on protecting these resources.

Threats, Vulnerabilities, and Impact Cont.,



Threats, Vulnerabilities, and Impact Cont.,

- Confidentiality—Preventing unauthorized disclosure of information. Data should be available only to authorized users. Loss of confidentiality occurs when data is accessed by someone who should not have access to it. Data is protected using access controls and encryption technologies.
- Integrity—Ensuring data or an IT system is not modified or destroyed. If data is modified or destroyed, it loses its value to the company. Hashing is often used to ensure integrity.
- Availability—Ensuring data and services are available when needed. IT systems are commonly protected using fault tolerance and redundancy techniques. Backups are used to ensure the data is retained even if an entire building is destroyed.

Threats, Vulnerabilities, and Impact Cont.,

- A vulnerability is a weakness. It could be a procedural, technical, or administrative weakness.
- It could be a weakness in physical security, technical security, or operational security.
- It's only when an attacker is able to exploit the vulnerability that a loss to an asset occurs.
- Vulnerabilities may exist because they've never been corrected. They can also exist if security is weakened either intentionally or unintentionally.
- Example: Consider a locked door used to protect a server room. A technician could intentionally unlock it to make it easier to access. If the door doesn't shut tight on its own, it could accidentally be left open. Either way, the server room becomes vulnerable.

Threats, Vulnerabilities, and Impact Cont.,

- The impact is the amount of the loss. The loss can be expressed in monetary terms, such as $5,000.
- The value of hardware and software is often easy to determine. If a laptop is stolen, you can use the purchase value or the replacement value.
- However, some losses aren't easy to determine. If that same laptop held data, the value of the data is hard to estimate.
- Descriptive terms instead of monetary terms can be used to describe the impact.
- You can describe losses in relative terms such as high, medium, or low. As an example, NIST SP 80030 suggests the following impact terms:

Threats, Vulnerabilities, and Impact Cont.,

(1) High impact—If a threat exploits the vulnerability it may:

- Result in the costly loss of major assets or resources.
- Significantly violate, harm, or impede an organization's mission, reputation, or interest.
- Or, result in human death or serious injury.

(2) Medium impact—If a threat exploits the vulnerability it may:

- Result in the costly loss of assets or resources.
- Violate, harm, or impede an organization's mission, reputation, or interest.
- Or, result in human injury.

(3) Low impact—If a threat exploits the vulnerability it may:

- Result in the loss of some assets or resources.
- Or, noticeably affect an organization's mission, reputation, or interest.

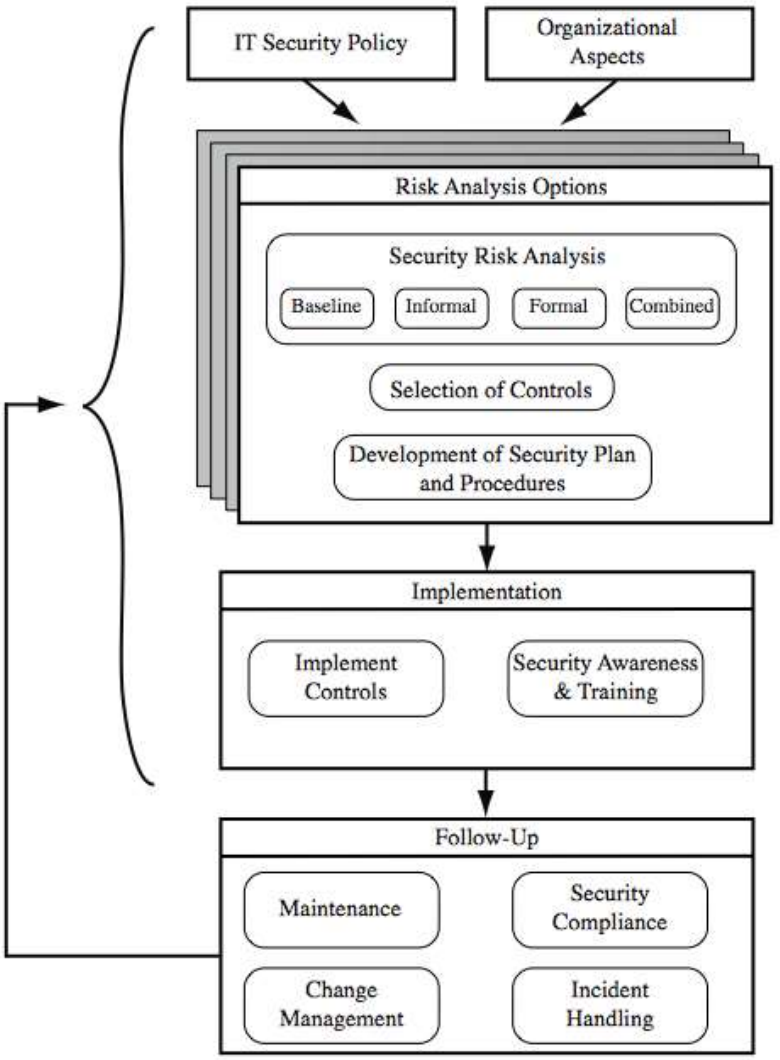
IT Security Management

- **IT Security Management:** a process used to achieve and maintain appropriate levels of confidentiality, integrity, availability, accountability, authenticity and reliability. IT security management functions include:
  - Organizational IT security objectives, strategies and policies
  - Determining organizational IT security requirements
  - Identifying and analyzing security threats to IT assets
  - Identifying and analyzing risks
  - Specifying appropriate safeguards
  - Monitoring the implementation and operation of safeguards
  - Developing and implement a security awareness program
  - Detecting and reacting to incidents

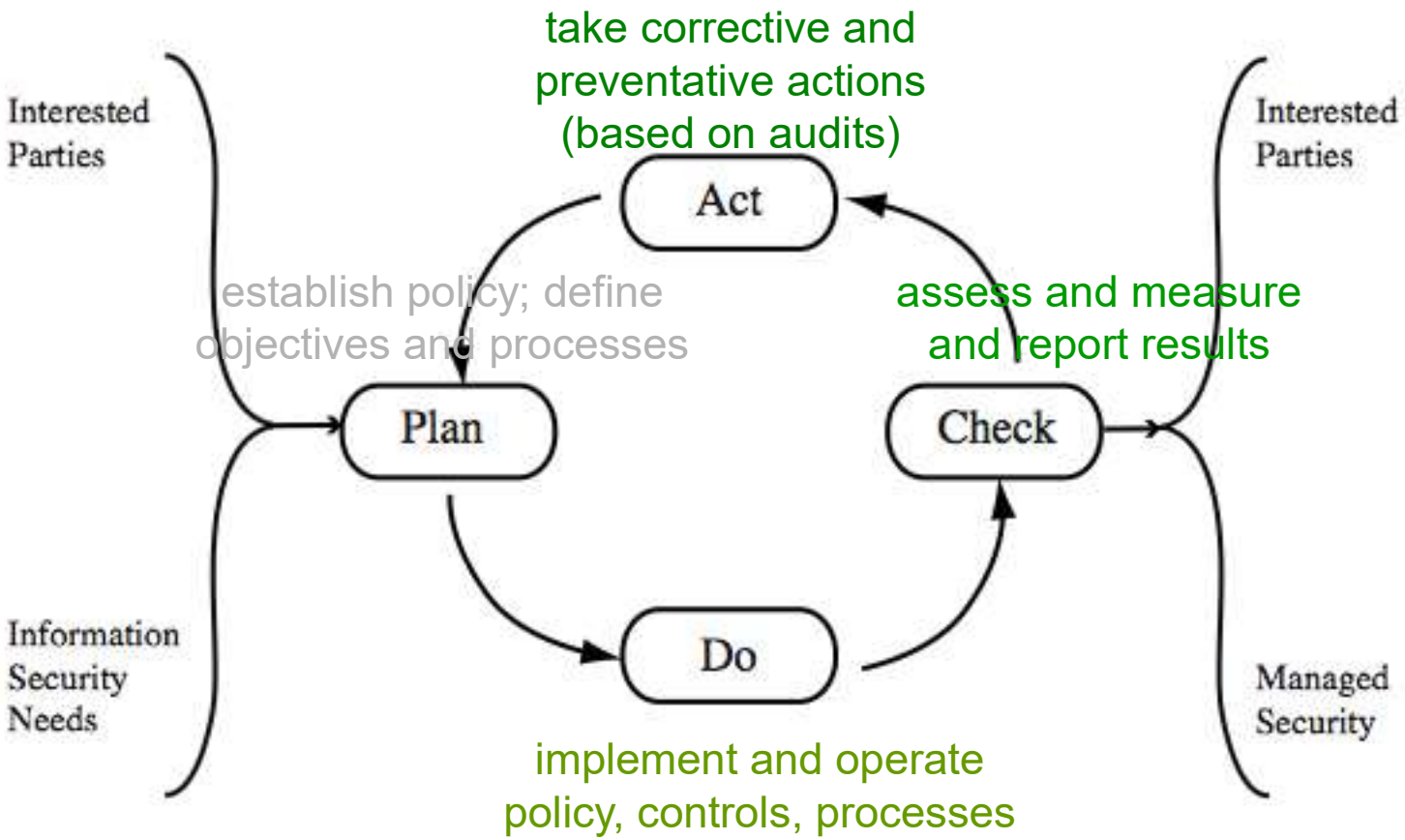
ISO 27000 Security Standards

ISO27000	a proposed standard which will define the vocabulary and definitions used in the 27000 family of standards.
ISO27001	defines the information security management system specification and requirements against which organizations are formally certified. It replaces the older Australian and British national standards AS7799.2 and BS7799.2.
ISO27002 (ISO17799)	currently published and better known as ISO17799, this standard specifies a code of practice detailing a comprehensive set of information security control objectives and a menu of best-practice security controls. It replaces the older Australian and British national standards AS7799.1 and BS7799.1.
ISO27003	a proposed standard containing ***implementation guidance*** on the use of the 27000 series of standards following the "Plan-Do-Check-Act" process quality cycle. Publication is proposed for late 2008.
ISO27004	a draft standard on information security ***management measurement*** to help organizations measure and report the effectiveness of their information security management systems. It will address both the security management processes and controls. Publication is proposed for 2007.
ISO27005	a proposed standard on information ***security risk management***. It will replace the recently released British national standard BS7799.3. Publication is proposed for 2008/9.
ISO13335	provides guidance on the ***management of IT security***. This standard comprises a number of parts. Part 1 defines concepts and models for information and communications technology security management. Part 2, currently in draft, will provide operational guidance on ICT security. These replace the older series of 5 technical reports ISO/IEC TR 13335 parts 1-5.

IT Security Management Process



Plan - Do - Check – Act (Deming Cycle)



Organizational Context and Security Policy

- First examine organization's IT security:
  - Objectives - wanted IT security outcomes
  - Strategies - how to meet objectives
  - Policies - identify what needs to be done
- Maintained and updated regularly
  - Using periodic security reviews
  - Reflect changing technical/risk environments

Security Policy: Topics to Cover

- Needs to address:
  - Scope and purpose including relation of objectives to business, legal, regulatory requirements
  - IT security requirements
  - Assignment of responsibilities
  - Risk management approach
  - Security awareness and training
  - General personnel issues and any legal sanctions
  - Integration of security into systems development
  - Information classification scheme
  - Contingency and business continuity planning
  - Incident detection and handling processes
  - How when policy reviewed, and change control to it

Management Support

- IT security policy must be supported by senior management
- Need IT security officer
  - To provide consistent overall supervision
  - Manage process
  - Handle incidents
- Large organizations needs IT security officers on major projects/teams
  - Manage process within their areas

Security Risk Assessment

- Critical component of process
  - else may have vulnerabilities or waste money
- Ideally examine every asset vs risk
  - not feasible in practice
- Choose one of possible alternatives based on organization's resources and risk profile
  - Baseline
  - Informal
  - Formal
  - Combined

Baseline Approach

- Use “industry best practice”
  - Easy, cheap, can be replicated
  - But gives no special consideration to org
  - May give too much or too little security
- Implement safeguards against most common threats
- Baseline recommendations and checklist documents available from various bodies
- Alone only suitable for small organizations

Informal Approach

- Conduct informal, pragmatic risk analysis on organization's IT systems
- Exploits knowledge and expertise of analyst
- Fairly quick and cheap
- Does address some org specific issues
- Some risks may be incorrectly assessed
- Skewed by analysts views, varies over time
- Suitable for small to medium sized orgs

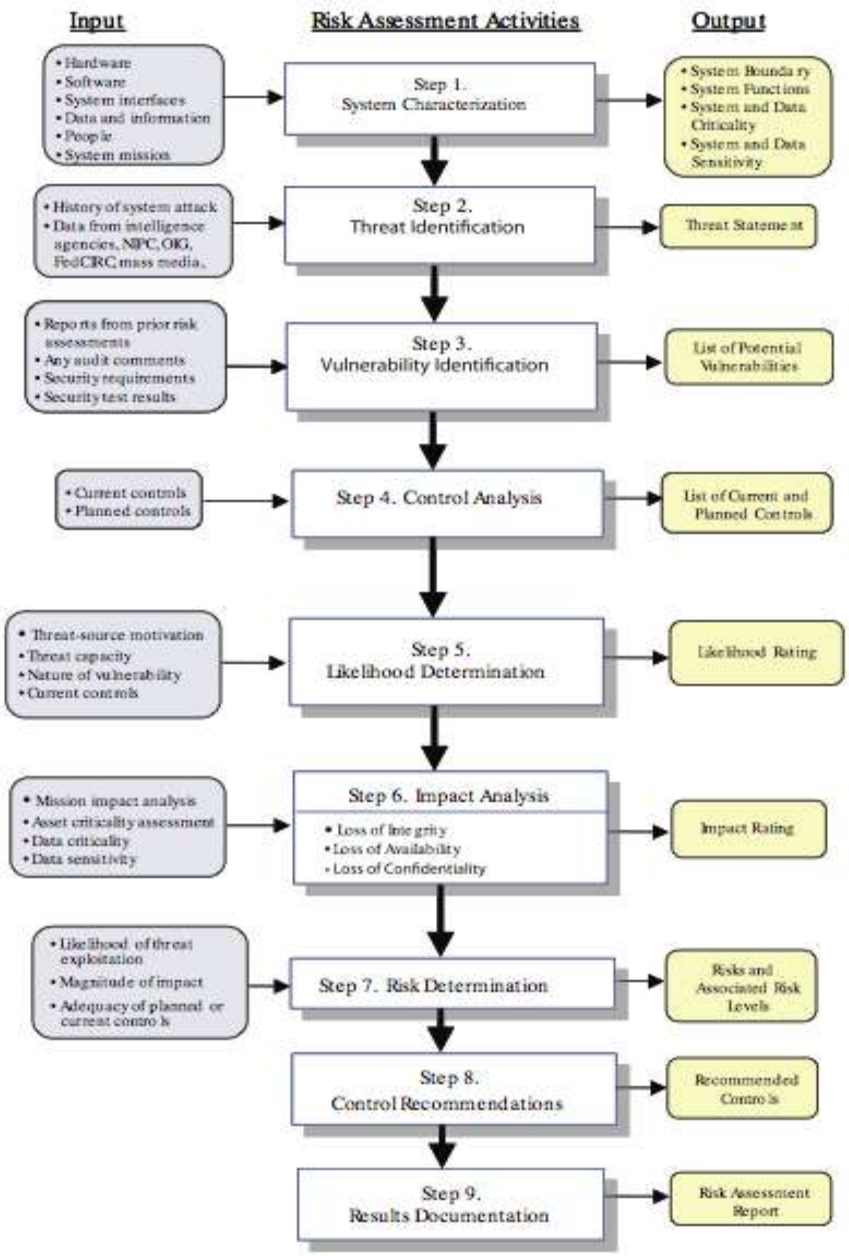
Detailed Risk Analysis

- Most comprehensive alternative
- Assess using formal structured process
  - With a number of stages
  - Identify likelihood of risk and consequences
  - Hence have confidence controls appropriate
- Costly and slow, requires expert analysts
- May be a legal requirement to use
- Suitable for large organizations with IT systems critical to their business objectives

Combined Approach

- Combines elements of other approaches
  - Initial baseline on all systems
  - Informal analysis to identify critical risks
  - Formal assessment on these systems
  - Iterated and extended over time
- Better use of time and money resources
- Better security earlier that evolves
- May miss some risks early
- Recommended alternative for most orgs

Detailed Risk Analysis Process



Establish Context

- Determine broad risk exposure of org
  - Related to wider political/social environment
  - Legal and regulatory constraints
- Specify organization's risk *appetite*
- Set boundaries of risk assessment
  - Partly on risk assessment approach used
- Decide on risk assessment criteria used

Asset Identification

- Identify assets
  - "anything which needs to be protected"
  - of value to organization to meet its objectives
  - tangible or intangible
  - in practice try to identify significant assets
- Draw on expertise of people in relevant areas of organization to identify key assets
  - identify and interview such personnel
  - see checklists in various standards

Terminology

asset: anything that has value to the organization

threat: a potential cause of an unwanted incident which may result in harm to a system or organization

vulnerability: a weakness in an asset or group of assets which can be exploited by a threat

risk: the potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets.

Threat Identification

- To identify threats or risks to assets asK
  - who or what could cause it harm?
  - how could this occur?
- Threats are anything that hinders or prevents an asset providing appropriate levels of the key security services:
  - confidentiality, integrity, availability, accountability, authenticity and reliability
- Assets may have multiple threats

Threat Sources

- Threats may be
  - natural “acts of god”
  - man-made and either accidental or deliberate
- Should consider human attackers
  - motivation
  - capability
  - resources
  - probability of attack
  - deterrence
- Any previous history of attack on org

Threat Identification

- Depends on risk assessors experience
- Uses variety of sources
  - natural threat chance from insurance stats
  - lists of potential threats in standards, IT security surveys, info from governments
  - tailored to organization's environment
  - and any vulnerabilities in its IT systems

Vulnerability Identification

- Identify exploitable flaws or weaknesses in organization's IT systems or processes
- Hence determine applicability and significance of threat to organization
- Need combination of threat and vulnerability to create a risk to an asset
- Again can use lists of potential vulnerabilities in standards etc

Analyze Risks

- Specify likelihood of occurrence of each identified threat to asset given existing controls
  - management, operational, technical processes and procedures to reduce exposure of org to some risks
- Specify consequence should threat occur
- Hence derive overall risk rating for each threat

  risk = probability threat occurs x cost to organization
- In practice very hard to determine exactly
- Use qualitative not quantitative, ratings for each
- Aim to order resulting risks in order to treat them

Determine Likelihood

Rating	Likelihood Description	Expanded Definition
1	**Rare**	May occur only in exceptional circumstances and may deemed as “unlucky” or very unlikely.
2	**Unlikely**	Could occur at some time but not expected given current controls, circumstances, and recent events.
3	**Possible**	Might occur at some time, but just as likely as not. It may be difficult to control its occurrence due to external influences.
4	**Likely**	Will probably occur in some circumstance and one should not be surprised if it occurred.
5	**Almost Certain**	Is expected to occur in most circumstances and certainly sooner or later.

Determine Consequence

Rating	Consequence	Expanded Definition
1	**Insignificant**	Generally a result of a minor security breach in a single area. Impact is likely to last less than several days and requires only minor expenditure to rectify.
2	**Minor**	Result of a security breach in one or two areas. Impact is likely to last less than a week, but can be dealt with at the segment or project level without management intervention. Can generally be rectified within project or team resources.
3	**Moderate**	Limited systemic (and possibly ongoing) security breaches. Impact is likely to last ***up to 2 weeks*** and generally requires management intervention. Will have ongoing compliance costs to overcome.
4	**Major**	Ongoing systemic security breach. Impact will likely last ***4-8 weeks*** and require significant management intervention and resources to overcome, and compliance costs are expected to be substantial. Loss of business or organizational outcomes is possible, but not expected, especially if this is a once off.
5	**Catastrophic**	Major systemic security breach. Impact will last for ***3 months or more*** and senior management will be required to intervene for the duration of the event to overcome shortcomings. Compliance costs are expected to be very substantial. Substantial public or political debate about, and loss of confidence in, the organization is likely. Possible criminal or disciplinary action is likely.
6	**Doomsday**	Multiple instances of major systemic security breaches. Impact duration cannot be determined and senior management will be required to place the company under voluntary administration or other form of major restructuring. Criminal proceedings against senior management is expected, and substantial loss of business and failure to meet organizational objectives is unavoidable.

Determine Resultant Risk

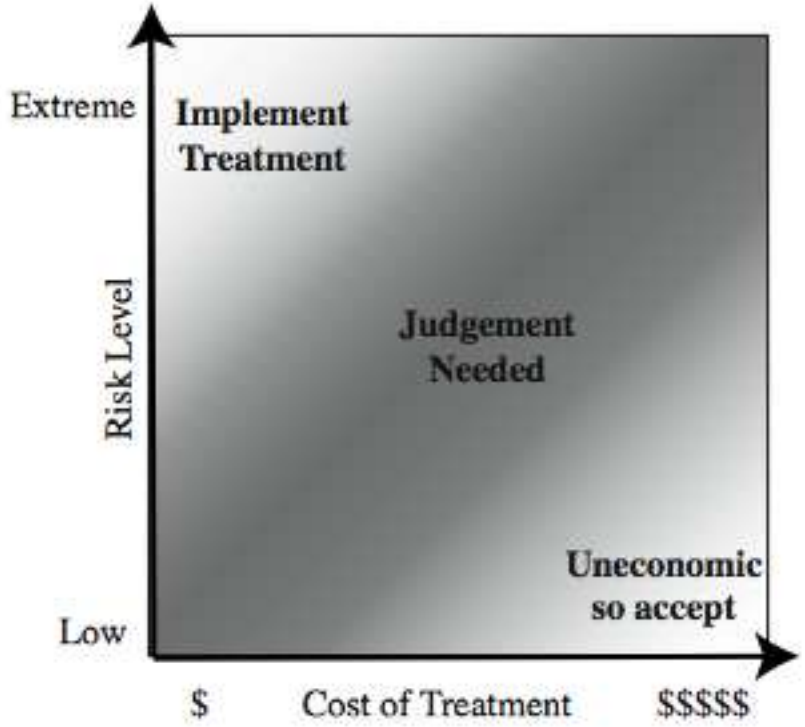
Likelihood	Consequences					
	Doomsday	**Catastrophic**	**Major**	**Moderate**	**Minor**	**Insignificant**
Almost Certain	E	E	E	E	H	H
Likely	E	E	E	H	H	M
Possible	E	E	E	H	M	L
Unlikely	E	E	H	M	L	L
Rare	E	H	H	M	L	L

Risk Level	Description
Extreme (E)	Will require detailed r esearch and management planning at an executive/director level. Ongoing planning and monitoring will be required with regular reviews. Substantial adjustment of controls to manage the risk are expected, with costs possibly exceeding original forecasts.
High (H)	Requires management attention, but management and planning can be left to senior project or team leaders. Ongoing planning and monitoring with regular reviews are likely, though adjustment of controls are likely to be met from within existing resources
Medium (M)	Can be managed by existing specific monitoring and response procedures. Management by employees is suitable with appropriate monitoring and reviews.
Low (L)	Can be managed through routine procedures.

Document in Risk Register and Evaluate Risks

Asset	Threat/ Vulnerability	Existing Controls	Likelihood	Consequence	Level of Risk	Risk Priority
Internet Router	Outside Hacker attack	Admin password only	Possible	Moderate	High	1
Destruction of Data Center	Accidental Fire or Flood	None (no disaster recovery plan)	Unlikely	Major	High	2

Risk Treatment



Risk Treatment Alternatives

- **Risk acceptance**: *accept risk (perhaps because of excessive cost of risk treatment)*
- **Risk avoidance**: *do not proceed with the activity that causes the risk (loss of convenience)*
- **Risk transfer**: buy insurance; outsource
- **Reduce consequence**: *modify the uses of an asset to reduce risk impact (e.g., offsite backup)*
- **Reduce likelihood**: *implement suitable controls*

Case Study: Silver Star Mines

- Fictional operation of global mining company
- Large IT infrastructure
  - both common and specific software
  - some directly relates to health & safety
  - formerly isolated systems now networked
- Decided on combined approach
- Mining industry less risky end of spectrum
- Management accepts moderate or low risk

Assets

- Reliability and integrity of SCADA nodes and net
- Integrity of stored file and database information
- Availability, integrity of financial system
- Availability, integrity of procurement system
- Availability, integrity of maintenance/production system
- Availability, integrity and confidentiality of mail services

Threats & Vulnerabilities

- Unauthorized modification of control system
- Corruption, theft, loss of info
- Attacks/errors affecting procurement system
- Attacks/errors affecting financial system
- Attacks/errors affecting mail system
- Attacks/errors maintenance/production affecting system

Risk Register

Asset	Threat/ Vulnerability	Existing Controls	Likelihood	Consequence	Level of Risk	Risk Priority
Reliability and integrity of the SCADA nodes and network	Unauthorized modification of control system	layered firewalls & servers	Rare	Major	High	1
Integrity of stored file and database information	Corruption, theft, loss of info	firewall, policies	Possible	Major	Extreme	2
Availability and integrity of Financial System	Attacks/errors affecting system	firewall, policies	Possible	Moderate	High	3
Availability and integrity of Procurement System	Attacks/errors affecting system	firewall, policies	Possible	Moderate	High	4
Availability and integrity of Maintenance/ Production System	Attacks/errors affecting system	firewall, policies	Possible	Minor	Medium	5
Availability, integrity and confidentiality of mail services	Attacks/errors affecting system	firewall, ext mail gateway	Almost Certain	Minor	High	6

Summary

- Detailed need to perform risk assessment as part of IT security management process
- Relevant security standards
- Presented risk assessment alternatives
- Detailed risk assessment process involves
  - Context including asset identification
  - Identify threats, vulnerabilities, risks
  - Analyse and evaluate risks
- Silver Star Mines case study

Security Risk Management and Ethics

Chapter Two: Security Risk Management

Textbook : Freund, J., & Jones, J, "Measuring and managing information risk: A FAIR Approach", 1st Edition, Butterworth-Heinemann, 2015. ISBN-13: 9780127999326.

Chapter2: Topics

This chapter covers the following topics and concepts:

- What risk management is and how it is important to the business.
- What some risk identification techniques are.
- What some risk management techniques are.

Chapter2: Goals

When you complete this chapter, you will be able to:

- Define risk management
- Describe risk management techniques
- Describe risk identification techniques
- Explain the relationship between the cost of loss and the cost of risk management
- Explain the risk management lifecycle

Risk Management and Its Importance to the Organization

- Risk management is the practice of identifying, assessing, controlling, and mitigating risks.
- Threats and vulnerabilities are key drivers of risk.
- Identifying the threats and vulnerabilities that are relevant to the organization is an important step.
- You can then take action to reduce potential losses from these risks.
- It's important to realize that risk management isn't intended to be risk elimination.
- That isn't a reasonable goal. Instead, risk management attempts to identify the risks that can be minimized and implement controls to do so.

Risk Management and Its Importance to the Organization Cont.,

- Risk management includes several elements:

(1) Risk assessment—Risk management starts with a risk assessment or risk analysis.

There are multiple steps to a risk assessment:

- Identify the IT assets of an organization and their value. This can include data, hardware, software, services, and the IT infrastructure.
- Identify threats and vulnerabilities to these assets. Prioritize the threats and vulnerabilities.
- Identify the likelihood a vulnerability will be exploited by a threat. These are your risks.
- Identify the impact of a risk. Risks with higher impacts should be addressed first.

Risk Management and Its Importance to the Organization Cont.,

(2) identify risks to manage—You can choose to avoid, transfer, mitigate, or accept risks. The decision is often based on the likelihood of the risk occurring, and the impact it will have if it occurs.

(3) Selection of controls—After you have identified what risks to address, you can identify and select control methods. Control methods are also referred to as countermeasures. Controls are primarily focused on reducing vulnerabilities and impact.

Risk Management and Its Importance to the Organization Cont.,

(4) Implementation and testing of controls—Once the controls are implemented, you can test them to ensure they provide the expected protection.

(5) Evaluation of controls—Risk management is an ongoing process. You should regularly evaluate implemented controls to determine if they still provide the expected protection. Evaluation is often done by performing regular vulnerability assessments.

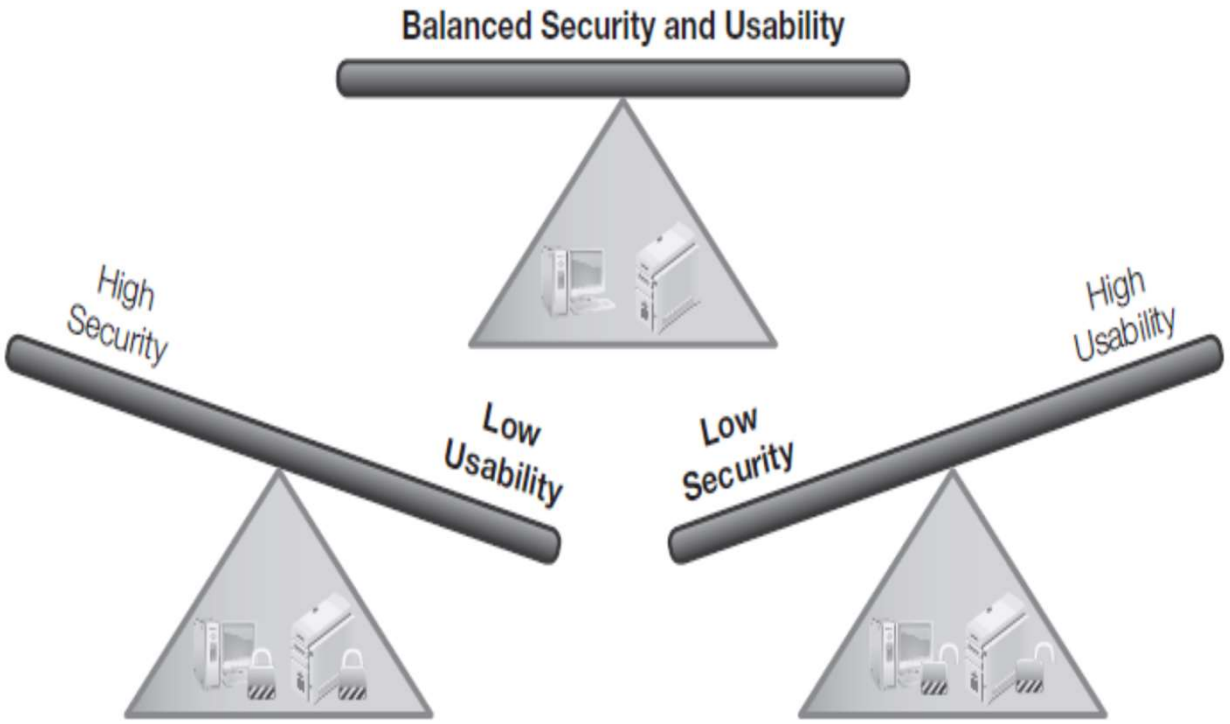
Role-Based Perceptions of Risk

- Ideally, all personnel within an organization will readily understand the threat to a company's health if risk is not managed.
- Unfortunately, risks and risk management are often perceived quite differently.
- One of the challenges with effective risk management is achieving a proper balance between security and usability.
- Consider Figure 1.3. In the diagram on the left, the computers are completely locked down with a high level of security. Users are unable to use them to adequately perform their job. On the right, the computers are easy to use but security is neglected. In the middle, a balance between the two has been achieved.

Role-Based Perceptions of Risk

FIGURE 1-3

Balancing security and usability in an organization.



Role-Based Perceptions of Risk Cont.,

- It is common for individuals in the followings roles to have different perceptions of risk:

(1) Management— Management is concerned mostly with profitability and survivability. Since attacks can result in loss of confidentiality, integrity, or availability, management is willing to spend money to mitigate risks. However, their view of the risk is based on the costs of the risk and the costs of the controls. Management needs accurate facts to make decisions on which controls to implement to protect company assets.

Role-Based Perceptions of Risk Cont.,

(2) System administrator—Administrators are responsible for protecting the IT systems. When they understand the risks, they often want to lock systems down as tight as possible. Administrators are often highly technical individuals. System administrators sometimes lose sight of the need to balance security costs with profitability.

Role-Based Perceptions of Risk Cont.,

(3) Tier 1 administrator—Tier 1 administrators are the first line of defense for IT support (thus the "tier 1" part of the name). When a user needs assistance, a tier 1 administrator is often called. They may be more concerned with usability than security or profitability. These administrators are given limited administrative permissions. They often view the security controls as hindrances to perform their job and don't always recognize the importance of the controls. For example, the need to use a change management process isn't always understood. A well-meaning technician may bypass a change management process to solve one problem but unintentionally create another problem. These unapproved changes can result in business losses.

Role-Based Perceptions of Risk Cont.,

(4) Developer—Some companies have in-house application developers. They write applications that can be used in-house or sold. Many developers have adopted a secure computing mindset. They realize that security needs to be included from the design stage all the way to the release stage. When developers haven't adopted a security mindset, they often try to patch security holes at the end of the development cycle. This patching mindset rarely addresses all problems, resulting in the release of vulnerable software.

Role-Based Perceptions of Risk Cont.,

(5) End user—End users simply want the computer to work for them. They are most concerned with usability. They often don't understand the reason for the security controls and restrictions. Instead, security is viewed as an inconvenience. Well-meaning users often try to circumvent controls so they can accomplish their job. For example, USB thumb drives often transport viruses without the user's knowledge. Companies frequently implement policies restricting the use of thumb drives. When a user needs to transfer a fi le from one computer to another, the USB thumb drive can be tempting.

Risk Identification Techniques

- You learned about risk and losses earlier in chapter 1. Risk is the likelihood that a loss will occur. Losses occur when a threat exposes a vulnerability.

- In order to identify risks, you'll need to take three steps:
- Step One: Identify threats
- Step Two: Identify vulnerabilities
- Step Three: Estimate the likelihood of a threat exploiting a vulnerability

Step One: Identifying Threats

- "Threat identification" is the process of creating a list of threats. This list attempts to identify all the possible threats to an organization. This is no small task. The list can be extensive.
- A threat is any circumstance or event with the potential to cause a loss. Said another way, it is any activity that represents a possible danger.
- The loss or danger is directly related to one of the following:

(1) Loss of confidentiality—Someone sees your password or a company's "secret formula."

(2) Loss of integrity—An e-mail message is modified in transit, a virus infects a file, or someone makes unauthorized changes to a Web site.

(3) Loss of availability—An e-mail server is down and no one has e-mail access, or a file server is down so data files aren't available.

Step One: Identifying Threats Cont..,

Threats are often considered in the following categories:

(1) External or internal—External threats are outside the boundary of the organization. They can also be thought of as risks that are outside the control of the organization. Internal threats are within the boundary of the organization. They could be related to employees or other personnel who have access to company resources. Internal threats can be related to any hardware or software controlled by the business.

Step One: Identifying Threats Cont..,

(2) Natural or man-made—Natural threats are often related to weather such as hurricanes, tornadoes, and ice storms. Earthquakes and tsunamis are also natural threats. A human or manmade threat is any threat from a person. Any attempt to sabotage resources is a man made threat. Fire could be manmade or natural depending on how the fire is started.

Step One: Identifying Threats Cont..,

(3) Intentional or accidental—Any deliberate attempt to compromise confidentiality, integrity, or availability is intentional. Employee mistakes or user error are accidental threats. A faulty application that corrupts data could be considered accidental. One method used to identify threats is through a brainstorming session. In a brainstorming session, participants throw out anything that pops into their heads. All ideas are written down without any evaluation. This creative process helps bring up ideas that may be missed when a problem is only analyzed logically.

Step One: Identifying Threats Cont..,

Some examples of threats to an organization include:

- An unauthorized employee trying to access data
- Any type of malware
- An attacker defacing a Web site
- Any DoS or DDoS attack
- An external attacker trying to access data
- Any loss of data
- Any loss of services
- A social engineer tricking an employee into revealing a secret
- Earthquakes, floods, or hurricanes
- A lightning strike
- Electrical, heating, or air conditioning outages
- Fires

Step Two: Identifying Vulnerabilities

- You learned earlier that a vulnerability is a weakness. When a threat occurs, if there is a vulnerability the weakness is apparent. However, before threats occur, you'll have to dig a little to identify the weaknesses. Luckily, most organizations have a lot of sources which can help you.
- Some of the sources you can use are:

(1) System logs—Many types of logs can be used to identify threats. Audit logs can determine if users are accessing sensitive data. Firewall logs can identify traffic that is trying to breach the network. Firewall logs can also identify computers taken over by malware and acting as zombies. DNS logs can identify unauthorized transfer of data.

Step Two: Identifying Vulnerabilities Cont....,

(2) Trouble reports—Most companies use databases to document trouble calls. These databases can contain a wealth of information. With a little bit of analysis, you can use them to identify trends and weaknesses.

(3) Prior events—Previous security incidents are excellent sources of data. As evidence of risks which already occurred, they help justify controls. They show the problems that have occurred and can show trends. Ideally, weaknesses from a security incident will be resolved right after the incident. In practice, employees are sometimes eager to put the incident behind them and forget it as soon as possible. Even if documentation doesn't exist on the incident, a few key questions can uncover the details.

Step Two: Identifying Vulnerabilities Cont....,

(4) Incident response teams—Some companies have incident response teams. These teams will investigate all the security incidents within the company. You can interview team members and get a wealth of information. These teams are often eager to help reduce risks.

(5) Audits—Many organizations are regularly audited. Systems and processes are checked to verify a company complies with existing rules and laws. At the completion of an audit, a report is created. These reports list findings which directly relate to weaknesses.

(6) Certification and accreditation records—Several standards exist to examine and certify IT systems. If the system meets the standards, the IT system can be accredited. The entire process includes detailed documentation. This documentation can be reviewed to identify existing and potential weaknesses.

Step Three: Estimate the likelihood of a threat exploiting a vulnerability Using the Seven Domains of a Typical IT Infrastructure

- Another way of identifying weaknesses is by examining the seven domains of a typical IT infrastructure.
- The following list gives you some examples in each of these domains:

(1) User Domain—Social engineering represents a big vulnerability. Sally gets a call. “Hi. This is Bob from the help desk. We’ve identified a virus on your computer.” Bob then attempts to walk Sally though a long detailed process and then says “Why don’t I just fix this for you? You can get back to work. All I need is your password.”

Step Three: Estimate the likelihood of a threat Cont.,

(2) Workstation Domain—Computers that aren't patched can be exploited. If they don't have antivirus software they can become infected.

(3) LaN Domain—Any data on the network that is not secured with appropriate access controls is vulnerable. Weak passwords can be cracked. Permissions that aren't assigned properly allow unauthorized access.

(4) LaN-to-WaN Domain—If users are allowed to visit malicious Web sites, they can mistakenly download malicious software. Firewalls with unnecessary ports open allow access to the internal network from the Internet.

Step Three: Estimate the likelihood of a threat Cont.,

(5) WaN Domain—Any public-facing server is susceptible to DoS and DDoS attacks. A File Transfer Protocol (FTP) server that allows anonymous uploads can host Warez from black-hat hackers.

(6) Remote access Domain—Remote users may be infected with a virus but not know it. When they connect to the internal network via remote access, the virus can infect the network.

(7) System/application Domain—Database servers can be subject to SQL injection attacks. In a SQL injection attack, the attacker can read the entire database. SQL injection attacks can also modify data in the database.

Pairing Threats with Vulnerabilities

- One of the most important steps when identifying risks is to pair the threats with vulnerabilities.
- Threats are matched to existing vulnerabilities to determine the likelihood of a risk.
- The "Identifying Threats" section listed several threats. Table 1-2 takes a few of those threats and matches them to vulnerabilities to identify possible losses.

The following formula is often used when pairing threats with vulnerabilities.

$$\text{Risk} = \text{Threat} \times \text{Vulnerability}$$

Example of Pairing Threats with Vulnerabilities

THREAT	VULNERABILITY	IMPACT
An unauthorized employee tries to access data hosted on a server.	The organization doesn't use authentication and access controls.	The possible loss would depend on the sensitivity of the data and how it's used. For example, if the unauthorized employee accessed salary data and freely shared it, this could impact morale and productivity.
Any type of malicious software, such as viruses or worms, enters the network.	Antivirus software doesn't detect the virus.	The virus could be installed on systems. Viruses typically result in loss of confidentiality, integrity, or availability.
An attacker modifies or defaces a Web site.	The Web site isn't protected.	Depending on how the attacker modifies the Web site, the credibility of the company could be affected.
A social engineer tricks an employee into revealing a password.	Users aren't adequately trained.	Passwords could be revealed. An attacker who obtains a password could take control of the user's account.

Risk Management Techniques

- After risks have been identified, you need to decide what you want to do about them.
- Risk management can be thought of as handling risk.
- It's important to realize that risk management is not risk elimination.
- A business that doesn't take any risks doesn't stay in business long. • The ultimate goal of risk management is to protect the organization.
- It helps ensure a business can continue to operate and earn a profit.
- When deciding how to handle a risk you can choose to avoid, transfer, mitigate, or accept the risk. These techniques are explained in the following slides.

Risk Management Techniques Cont....,

Risk management includes several techniques. They include:

(1) Avoidance

(2) Transfer

(3) Mitigation

(4) Acceptance

(1) Avoidance

• One of the ways you manage risk is by simply avoiding it. The primary reason to avoid a risk is that the impact of the risk outweighs the benefit of the asset.

• An organization can avoid risk by:

(1) Eliminating the source of the risk—The company can stop the risky activity. For example, a company may have a wireless network that is vulnerable to attacks. The risk could be avoided by removing the wireless network. This can be done if the wireless network isn't an important asset in the company.

(1) Avoidance Cont.,

(2) Eliminating the exposure of assets to the risk—The company can move the asset. For example, a data center could be at risk because it is located where earthquakes are common. It could be moved to an earthquake-free zone to eliminate this risk. The cost to move the data center will be high. However, if the risk is unacceptable and the value of the data center is higher it makes sense.

(2) Transfer

- You can transfer risk by shifting responsibility to another party. This is most commonly done by purchasing insurance.
- It can also be done by outsourcing the activity.

(1) Insurance—You purchase insurance to protect your company from a loss. If a loss occurs, the insurance covers it. Many types of insurance are available, including fire insurance.

(2) Outsourcing the activity—For example, your company may want to host a Web site on the Internet. The company can host the Web site with a Web hosting provider. Your company and the provider can agree on who assumes responsibility for security, backups, and availability.

(3) Mitigation

- You reduce risk by reducing vulnerabilities, and risk mitigation is the primary strategy in this process.
- Risk mitigation is also known as reduction or treatment.
- You reduce vulnerabilities by implementing controls or countermeasures. The cost of a control should not exceed the benefit. Determining costs and benefits often requires a cost benefit analysis.
- Some examples of mitigation steps are:

(1) Alter the physical environment—Replace hubs with switches. Locate servers in locked server rooms.

(2) Change procedures—Implement a backup plan. Store a copy of backups offsite, and test the backups.

(3) Mitigation Cont.,

(3) Add fault tolerance—Use Redundant Array of Independent Disks (RAID) for important data stored on disks. Use failover clusters to protect servers.

(4) Modify the technical environment—Increase security on the firewalls. Add intrusion detection systems. Keep antivirus software up to date.

(5) Train employees—Train technical personnel on how to implement controls. Train end users on social engineering tactics.

(3) Mitigation Cont.,

- Often the goal is not to eliminate the risk but instead, to make it too expensive for the attacker.
- Consider the following two formulas.

(1) Attacker's cost < attacker's gain—When this is true, it is appealing to the attacker.

(2)Attacker's cost > attacker's gain—When this is true, the attacker is less likely to pursue the attack.

- Example: Cryptography is one of the ways to increase the attacker's cost. If your company sends data across the network in clear text, it can be captured and analyzed. If the company encrypts the data, an attacker must decrypt it before analyzing it. The goal of the encryption isn't to make it impossible to decrypt the data. Instead, the goal is to make it too expensive or too time consuming for the attacker to crack it.

(4) Acceptance

- You can also choose to accept a risk. A company can evaluate a risk, understand the potential loss, and choose to accept it.
- This is commonly done when the cost of the control outweighs the potential loss.
- For example, consider the following scenario: A company hosts a Web server used for ecommerce. The Web server generates about $1,000 per month in revenue. The server could be protected using a failover cluster. However, estimates indicate that a failover cluster will cost approximately $10,000. If the server goes down, it may be down for only one or two hours, which equates to less than $3. (Revenue per hour = $1,000*12*365/24 = $1.37.)

- The decision to accept a loss becomes easier if you have evaluated the costs against the benefits, which is known as a "cost benefit analysis." A cost benefit analysis is useful when choosing any of the techniques to manage risk.

Cost-Benefit Analysis

- Any organization must perform a cost-benefit analysis (CBA) to help determine which controls or countermeasures to implement.
- If the benefits outweigh the costs, the control is often selected. A CBA compares the business impact with the cost to implement a control.
- For example, the loss of data on a file server may represent the loss of $1 million worth of research. Implementing a backup plan to ensure the availability of the data may cost $10,000. In other words, you would spend $10,000 to save $1 million. This makes sense.

Cost-Benefit Analysis Cont.,

- A CBA starts by gathering data to identify the costs of the controls and benefits gained if they are implemented.

(1) Cost of the control—This includes the purchase costs plus the operational costs over the lifetime of the control.

(2) Projected benefits—This includes the potential benefits gained from implementing the control. You identify these benefits by examining the costs of the loss and how much the loss will be reduced if the control is implemented.

Cost-Benefit Analysis Cont.,

- A control doesn't always eliminate the loss. Instead, the control reduces it.
- For example, annual losses for a current risk may average $100,000. If a control is implemented, these losses may be reduced to $10,000. The benefit of the control is $90,000.
- You can use the following formula to determine if the control should be used:

Loss before control - loss after control = cost of control

- Imagine the company lost $100,000 last year without any controls implemented. You estimate you'll lose $10,000 a year if the control is implemented. The cost of the control is estimated at $10,000.

Cost-Benefit Analysis Cont.,

- The formula is:

$100,000 - $10,000 (cost of control) - $10,000 (expected residual loss) = $80,000.

- One of the biggest challenges when performing a CBA is getting accurate data. While current losses are often easily available, future costs and benefits need to be estimated. Costs are often underestimated. Benefits are often overestimated.

- The immediate costs of a control are often available. However, the ongoing costs are sometimes hidden. Some of the hidden costs may be:

  - Costs to train employees
  - Costs for ongoing maintenance
  - Software and hardware renewal costs

- If the costs outweigh the benefits, the control may not be implemented. Instead, the risk could be accepted, transferred or avoided.

(7) Risk on System/Application Domain

- The System/Application Domain refers to servers that host server level applications.
- Mail servers receive and send email for clients. Database servers host databases that are accessed by users, applications, or other servers.
- Domain Name System (DNS) servers provide names to IP addresses for clients.
- You should always protect servers using best practices: Remove unneeded services and protocols. Change default passwords.
- Regularly patch and update the server systems. Enable local firewalls.

(7) Risk on System/Application Domain

• One of the challenges with servers in the System/Application Domain is that the knowledge becomes specialized. People tend to focus on areas of specialty.

• For example, common security issues with an email server would likely be known only by technicians who regularly work with the email servers.

• NOTE:

You should lock down a server using the specific security requirements needed by the hosted application. An e-mail server requires one set of protections while a database server requires a different set.

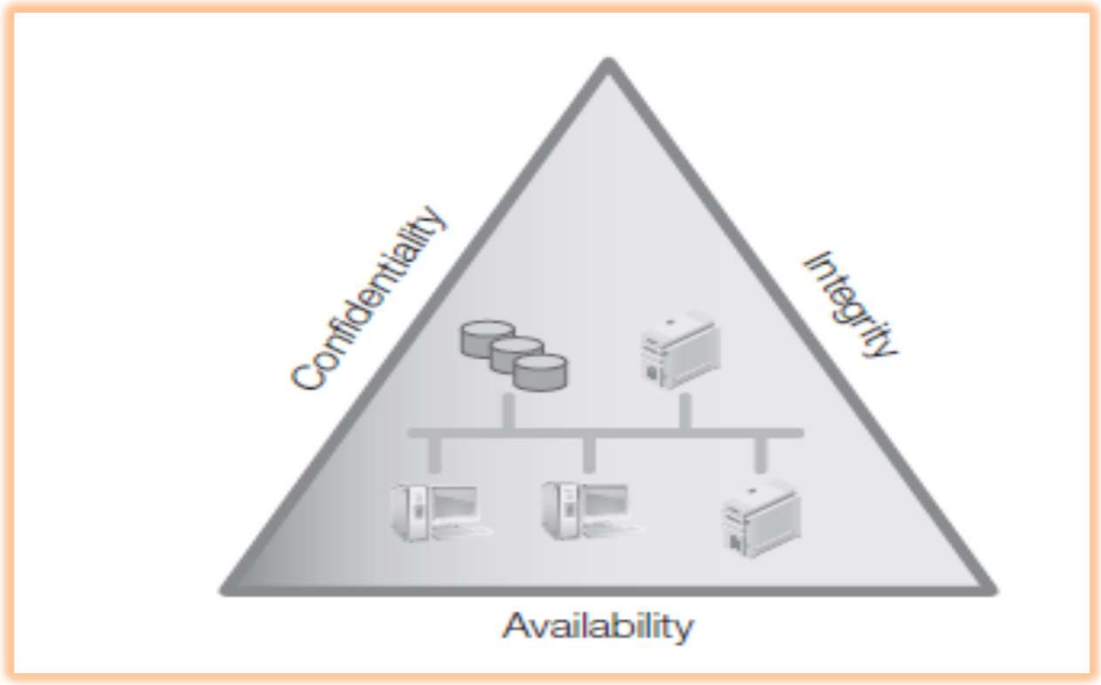
Threats, Vulnerabilities, and Impact

- When a threat exploits a vulnerability it results in a loss. The impact identifies the severity of the loss.
- A threat is any circumstance or event with the potential to cause a loss. You can also think of a threat as any activity that represents a possible danger. Threats are always present and cannot be eliminated, but they may be controlled.
- Threats have independent probabilities of occurring that often are unaffected by an organizational action. As an example, an attacker may be an expert in attacking Web servers hosted on Apache. There is very little a company can do to stop this attacker from trying to attack. However, a company can reduce or eliminate vulnerabilities to reduce the attacker's chance of success.

Threats, Vulnerabilities, and Impact

- Threats are attempts to exploit vulnerabilities that result in the loss of confidentiality, integrity, or availability of a business asset.
- The protection of confidentiality, integrity, and availability are common security objectives for information systems.
- Figure 1.2 shows these three security objectives as a protective triangle. If any side of the triangle is breached or fails, security fails.
- In other words, risks to confidentiality, integrity, or availability represent potential loss to an organization. Because of this, a significant amount of risk management is focused on protecting these resources.

Threats, Vulnerabilities, and Impact Cont.,



Threats, Vulnerabilities, and Impact Cont.,

- Confidentiality—Preventing unauthorized disclosure of information. Data should be available only to authorized users. Loss of confidentiality occurs when data is accessed by someone who should not have access to it. Data is protected using access controls and encryption technologies.
- Integrity—Ensuring data or an IT system is not modified or destroyed. If data is modified or destroyed, it loses its value to the company. Hashing is often used to ensure integrity.
- Availability—Ensuring data and services are available when needed. IT systems are commonly protected using fault tolerance and redundancy techniques. Backups are used to ensure the data is retained even if an entire building is destroyed.

Threats, Vulnerabilities, and Impact Cont.,

- A vulnerability is a weakness. It could be a procedural, technical, or administrative weakness.
- It could be a weakness in physical security, technical security, or operational security.
- It's only when an attacker is able to exploit the vulnerability that a loss to an asset occurs.
- Vulnerabilities may exist because they've never been corrected. They can also exist if security is weakened either intentionally or unintentionally.
- Example: Consider a locked door used to protect a server room. A technician could intentionally unlock it to make it easier to access. If the door doesn't shut tight on its own, it could accidentally be left open. Either way, the server room becomes vulnerable.

Threats, Vulnerabilities, and Impact Cont.,

- The impact is the amount of the loss. The loss can be expressed in monetary terms, such as $5,000.
- The value of hardware and software is often easy to determine. If a laptop is stolen, you can use the purchase value or the replacement value.
- However, some losses aren't easy to determine. If that same laptop held data, the value of the data is hard to estimate.
- Descriptive terms instead of monetary terms can be used to describe the impact.
- You can describe losses in relative terms such as high, medium, or low. As an example, NIST SP 80030 suggests the following impact terms:

Threats, Vulnerabilities, and Impact Cont.,

(1) High impact—If a threat exploits the vulnerability it may:

- Result in the costly loss of major assets or resources.
- Significantly violate, harm, or impede an organization's mission, reputation, or interest.
- Or, result in human death or serious injury.

(2) Medium impact—If a threat exploits the vulnerability it may:

- Result in the costly loss of assets or resources.
- Violate, harm, or impede an organization's mission, reputation, or interest.
- Or, result in human injury.

(3) Low impact—If a threat exploits the vulnerability it may:

- Result in the loss of some assets or resources.
- Or, noticeably affect an organization's mission, reputation, or interest.

End

Security Risk Management and Ehics

Chapter Three: Security Risk Assessment

Textbook : Freund, J., & Jones, J, "Measuring and managing information risk: A FAIR Approach", 1st Edition, Butterworth-Heinemann, 2015. ISBN-13: 9780127999326.

Chapter3: Topics

This chapter covers the following topics and concepts:

- What risk assessment is
- What the critical components of a risk assessment are
- What types of risk assessments are available
- Which risk assessment challenges you should address
- What best practices for risk assessment are

Chapter3: Goals

When you complete this chapter, you will be able to:

- Define risk assessment
- Describe the importance of risk assessment
- Explain when a risk assessment should be performed
- Explain the purpose of a risk assessment and a risk assessment scope
- Explain what's meant by identifying critical areas for a risk assessment
- Identify the main types of risk assessments

Chapter3: Goals

When you complete this chapter, you will be able to:

- Describe the elements of a quantitative risk assessment and a qualitative risk assessment
- Identify the differences between quantitative and qualitative risk assessments
- Identify the benefits and limitations of quantitative risk assessments and qualitative risk assessments
- List the challenges with risks assessments

Risk Assessment

- A risk assessment (RA), also referred to as “risk analysis,” is a process used to identify and evaluate risks. Risks are then quantified based on their importance or impact severity.
- These risks are then prioritized.
- Risk assessments are a major part of an overall risk management program. They help identify which risks are most important.
- A major difference between a risk assessment and a risk management program is that the risk assessment is created at a moment in time, while a risk management program is a continuous process.

Risk Assessment Cont.,

- An RA is used to help identify which safeguards to implement. Safeguards are also known as controls.
- They are used to control or reduce risk. A control may reduce a vulnerability or it may reduce the impact from a threat. Either way, the risk is reduced.
- A RISK ASSESSMENT IS PERFORMED to identify the most serious risks.

- The risk assessment allows you to prioritize the risks. You manage the high-priority risks and accept the low-priority risks.

Importance of Risk Assessments

- Risk assessments are an important part of the risk management process.
- Without an RA, it becomes difficult to determine which systems should be protected. It also remains unclear how to protect them.
- However, an RA will help you identify the most important systems to protect.
- It will also give you insight into what controls will provide the most value.

Importance of Risk Assessments Cont.,

An RA should be completed:

- When evaluating risk—Risk assessments are a part of the overall risk management process. Risk assessments are useful any time risk management is being used. This is especially true if the risks need to be prioritized.

- When evaluating a control—You can use an RA to evaluate the usefulness of a control. Management can't approve all controls. They will approve some controls and not others. An RA helps management decide which controls to adopt.

Importance of Risk Assessments Cont.,

- Periodically after a control has been implemented—An RA is a point-in-time document. However, risks don't stand still. Attackers are constantly upgrading their techniques and tactics. You should schedule RAs on a regular basis after a control has been implemented. The goal is to determine if the control is still useful.

Purpose of a Risk Assessment

- Risk assessments are important tools to assist management. They help management quantify risks.
- They also help management identify controls and evaluate the effectiveness of these controls. Risk assessments tend to:

(1) Support decision making—The RA prioritizes risks. This helps decision makers determine which risks should be reduced. As a reminder, not all risks have to be reduced. Risks can be avoided, transferred, mitigated, or accepted. High-priority risks should be mitigated. Lower priority risks may be accepted.

Purpose of a Risk Assessment Cont.,

(2) Evaluate control effectiveness—You implement controls to reduce a risk. The RA gives insight into how effective specific controls will be for specific risks.

• An RA involves many steps. It isn't a task that you can complete in a single sitting, a single day, or even a single week. When done properly, it involves the input of several key players. Steps involved in the RA include:

Risk Assessment Steps

(1) Identify threats and vulnerabilities—When a threat exploits a vulnerability, a risk occurs. Threats and vulnerabilities are identified as risks.

(2) Identify the likelihood that a risk will occur—This can be based on historical data or opinions. For example, imagine a risk occurred an average of four times in the past three years. If no steps are taken to reduce the risk, it will probably occur four times next year. If historical data isn't available, experts can provide opinions on the likelihood of the risk occurring.

Risk Assessment Steps Cont.,

(3) Identify asset values—The value of assets helps to determine the impact of a risk. The assets can be hardware assets, software assets, or data. Some risks can affect all three.

(4) Determine the impact of a risk—This can also be based on historical data or opinions. Imagine a risk resulted in losses averaging $20,000 a year in the past three years. If no steps are taken to reduce the risk, it will probably result in a loss of about $20,000 next year. If historical data isn't available, experts can provide opinions on the impact of the risk occurring.

Risk Assessment Steps Cont.,

(5) Determine the usefulness of a safeguard or control—Safeguards or controls are used to reduce the risk or reduce the impact. Some controls will be more effective than others. The RA helps determine which ones to implement.

• The RA identifies threats and vulnerabilities against the current system. It assumes current controls are working as expected. Another way of saying this is that an RA is performed at a moment in time based on current conditions. This is unlike risk management as a whole. Risk management is a continuous process. RAs are not continuous.

Critical Components of a Risk Assessment

• There are several components that you should consider when tasking and performing an RA. You should complete three critical steps early. These identify major components of the RA and will directly impact its success.

These steps are:

• Identify scope.

• Identify critical areas.

• Identify team.

Step One: Identify Scope

- The scope identifies the boundary of the RA.
- It's important to identify the scope of a risk management plan to eliminate scope creep. It helps to keep the project on track. Similarly, the scope of the RA helps to keep the RA on track.
- For example, consider Figure 5-1. The figure shows a Web server configured in a network. The server hosts a Web site that is accessible from the Internet. Customers can access the Web site and make purchases. The Web server hosts the Web site application.

Step One: Identify Scope

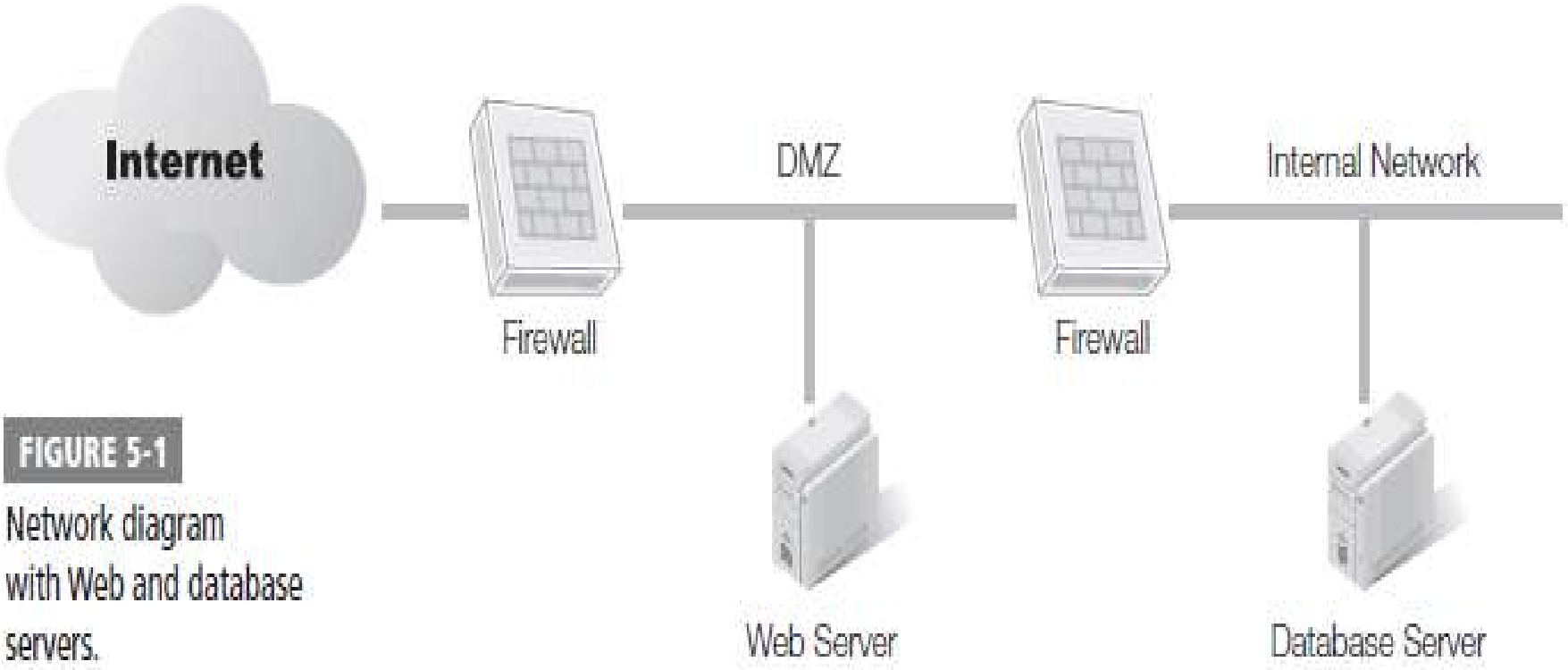


FIGURE 5-1

Network diagram with Web and database servers.

Step One: Identify Scope Cont..,

- However, all the data is hosted on the back-end database server.
- You could set the scope to focus only on the Web server. Alternatively, the scope could include the Web server and the database server. It's also possible to include both of the firewalls in the demilitarized zone (DMZ).
- Imagine that the Web server was attacked several times in the past year. Some of these attacks resulted in the Web site crashing or the Web server failing. However, existing controls protected the data on the database server. Data was not accessed inappropriately or lost. In this example, you may choose not to include the database server. It's also possible to include the database server just to ensure the existing controls will protect against current risks.

Step One: Identifying Threats Cont..,

• There’s no right or wrong choice for what’s included in the scope. Management can decide to include or exclude anything. The most important point is to make a choice.

Step Two: Identify Critical Areas

- The RA also identifies critical areas that should be included.
- This helps the RA team focus only on what's important. For example, a scope could include a Web server, a database server, and a firewall. The RA could identify the following critical areas:

- Web server—Address all elements of the Web server. This includes hardware, the operating system, and the Web site application. For hardware, focus on any single point of failure.

Step Two: Identify Critical Areas Cont.…,

- A single point of failure (SPOF) is any single piece of hardware whose failure can take down the Web site. You should consider a process that regularly updates the operating system, in addition to applying best practices to prevent attacks on the Web site application. This includes buffer overflow and SQL injection attacks.
- Database server—The database server hosts about 20 databases. You should include in the RA only the databases accessed by the Web server through the firewall. You should definitely consider SQL injection attacks. However, you will implement the primary protection from SQL injection attacks in the Web site application.
-

Step Two: Identify Critical Areas Cont.…,

- Internal firewall—The internal firewall controls all traffic to and from the internal network. You do not need to include all traffic in the RA. Address only the rules affecting communication between the Web server and database server.
- Therefore, when you identify critical areas, you should focus on areas that are most critical to the business. Profitability and survivability were mentioned previously in this chapter.
- It is good to keep these concepts in mind. Some data is critical, such as financial data and customer data. Other data, such as public data, doesn't need the same level of protection. Similarly, some servers or IT services are critical. Other servers and services are less critical.

Step Three: Identify Team

- Risk assessment team personnel should not be the same people who are responsible for correcting deficiencies. This helps avoid a conflict of interest.
- For example, imagine that an administrator is responsible for implementing controls on a Web server. His input may be slanted by his desire to implement the control.
- If disinterested parties provide the input, there is a better chance of getting accurate, objective data.

Step Three: Identify Team Cont.,

- This is not to say that you shouldn't get input from the responsible department.

- Its staff probably has excellent insight into the problems and how to fix them.

- However, when prioritizing risks and determining the usefulness of controls, input from the people who correct deficiencies should not be the deciding factor.

Types of Risk Assessments

• When considering an RA, you first need to identify what method to use. The two primary methods used in the IT field are:

(1) Quantitative—This is an objective method. It uses numbers such as actual dollar values. A quantitative RA requires a significant amount of data. Gathering this data often takes time. If the data is available, this type of RA becomes a simple math problem with the use of formulas.

Types of Risk Assessments Cont..,

(2) Qualitative—This is a subjective method. It uses relative values based on opinions from experts. Experts provide their input on the probability and impact of a risk. A qualitative RA can be completed rather quickly.

• They both have benefits and limitations. However, one method sometimes works better than the other in specific situations. When you're aware of the different options, it becomes easier to choose the right method for the right situation.

Quantitative Risk Assessments

- A quantitative risk assessment uses numbers such as dollar values.
- You gather data and then enter it into standard formulas.

- The results can help you identify the priority of risks.

- You can also use the results to determine the effectiveness of controls.

Quantitative Risk Assessments Cont..,

- Some of the key terms associated with quantitative risk assessments are:
- Single loss expectancy (SLE)—The total loss expected from a single incident. An incident occurs when a threat exploits a vulnerability. The loss is expressed as a dollar value such as $5,000. It includes the value of hardware, software, and data.
- Annual rate of occurrence (ARO)—The number of times an incident is expected to occur in a year. If an incident occurred once a month in the past year, the ARO is 12. Assuming nothing changes, it's likely that it will occur 12 times next year.

Quantitative Risk Assessments Cont..,

• Annual loss expectancy (ALE)—The expected loss for a year. ALE is calculated by multiplying SLE X ARO. Because SLE is a given in a dollar value, ALE is given as a dollar value. For example, if the SLE is $5,000 and the ARO is 12, the ALE is $60,000.

• Safeguard value—This is the cost of a control. Controls are used to mitigate risk. For example, antivirus software could have an average cost of $50 for each computer. If you have 100 computers, the safeguard value is $5,000.

Benefits of Quantitative Risk Assessments

(1) One of the primary benefits of a quantitative RA is that it becomes a simple math problem. This is especially true if you use tools that automate the assessment. For example, applications are available that allow you to plug in values for SLE, ARO, and safeguard value. The application then calculates the results and provides a recommendation. Because the application performs the calculations, the data is often more accurate.

(2) Another big benefit of a quantitative RA is that it provides a cost-benefit analysis (CBA). When you have accurate values for the SLE, ARO, and safeguard value, you can also calculate the CBA. You saw this in the previous section.

Benefits of Quantitative Risk Assessments Cont..,

(3) Management is often familiar with quantitative assessment terminology. For example, a quantitative assessment uses dollar terms to express losses. Because of this, it becomes easy for management to grasp the details of the assessment and its recommendations.

(4) Last, the formulas use verifiable and objective measurements. If a Web site makes $2,000 in revenue an hour, it will lose that revenue if it is down for one hour. This isn't a debatable opinion; it's a verifiable fact.

Qualitative Risk Assessments

• A qualitative risk assessment doesn't assign dollar values. Instead, it determines the level of risk based on the probability and impact of a risk. You determine these values by gathering the opinions of experts. Probability and impact are defined as:

• Probability—The likelihood that a threat will exploit a vulnerability. The risk occurs when a threat exploits a vulnerability. You can use a scale to define the probability that a risk will occur. The scale can be based on word values such as Low, Medium, or High. You can then assign percentage values to these words. For example, you could assign a value of 10 percent to a low probability. You could assign 100 percent to a high probability.

Qualitative Risk Assessments cont..,

- Impact—The negative result if a risk occurs. Impact is used to identify the magnitude of a risk. The risk results in some type of loss. However, instead of quantifying the loss as a dollar amount, an impact assessment could use words such as Low, Medium, or High. You may also use these categories to identify probabilities. However, where a probability is expressed as a percentage, impact is expressed as a relative value. For example, Low could be 10. Medium could be 50. High could be 100.

- You can calculate the risk level with the following formula:

Risk level= Probability * Impact

Qualitative Risk Assessments cont..,

- NOTE: An important point to realize about the qualitative RA is that you must define the scale. However, there is no single standard. One company may use three values of Low, Medium, and High. Another company may use five values of Slight, Slightly Moderate, Moderate, Moderately Severe, and Severe. As long as you define the scale in the RA, any scale can be used.
- Tables 5-1 and 5-2 show one way you could define the scales in an RA. You would assign the values for each of these scales based on current known threats and vulnerabilities, as well as current controls.

Qualitative Risk Assessments cont..,

TABLE 5-1 Probability scale.

PROBABILITY	DESCRIPTION
Low	It is unlikely the risk will occur. Threats are not active. Vulnerabilities are either not known or have been mitigated. Low equates to a value of 10 percent.
Medium	There is a moderate chance the risk will occur. It has occurred in the past, but mitigation controls have reduced recent occurrences. Medium equates to a value of 50 percent.
High	There is a high probability the risk will occur. It has occurred in the past and will occur again if not mitigated. High equates to a value of 100 percent.

Qualitative Risk Assessments cont..,

TABLE 5-2 Impact scale.

IMPACT	DESCRIPTION
Low	If the risk occurs, it will have minimal impact on the company. The attack will not impact any critical data or systems.
Medium	If the risk occurs, it will have a moderate impact on the company. It may affect critical data or systems, but not to a large extent.
High	If the risk occurs, it will have a high impact on the company. It will affect critical data or systems and cause substantial losses.

Qualitative Risk Assessments cont..,

- A qualitative analysis can be divided into two sections:

(1) The first section attempts to prioritize the risk.

(2) The second section evaluates the effectiveness of controls.

- It is possible to perform both sections at the same time.

(1) Prioritizing the Risk

- The goal of this part of the RA is to identify which risks are most important.
- You do this by assigning probability and impact values to known risks.
- For example, your company Web site sells company products.
- Due to some recent outages, you are trying to identify the most important risks to the Web site.
- Based on feedback from several experts, you have come up with a list. You now want to prioritize these risks.

(1) Prioritizing the Risk Cont..,

- The risk categories are:
- DoS attack—Any denial of service (DoS) or distributed DoS (DDoS) attack that results in an outage.
- Web defacing—Modification of the Web site by unauthorized parties.
- Loss of data from unauthorized access—Any loss of confidentiality. This could be from an attacker accessing customer data. It could also be from an attacker accessing any internal private data. It does not include the loss of public data that is freely available.

(1) Prioritizing the Risk Cont..,

• Loss of Web site data due to hardware failure—This indicates the loss of any Web site data. This can include any data used to show the Web pages to customers. It can also include the Web site application used to retrieve and format the data into Web pages.

Example of Prioritizing the Risk

- The Web site is protected in a demilitarized zone (DMZ). It also has antivirus (AV) software installed.
- You could distribute the survey on the next page to key experts to determine risks.
- You can conduct these surveys in several ways: via surveys that are filled out independently, by interviewing experts, or within a meeting but without discussion.
- Consider what can happen if there is discussion: If the boss says “Clearly, loss of data will have a high impact,”.
- After you gather data from the experts, you compile and summarize it. If you assign numerical values to Low, Medium, and High, such as 10, 50, and 100, you can calculate the averages.

Form of Survey for Determining Risks

Survey for Determining Risks

We are attempting to identify the most serious risks to our Web site. Please fill in each block of the following table with a level of Low, Medium, or High. Your decisions should be based on current controls and safeguards. For example, the Web site is currently placed on the Internet and is protected with a host-based firewall. Assume this firewall will remain.

Qualitative analysis survey.		
CATEGORY	**PROBABILITY THE RISK WILL OCCUR (Low, Medium, High)**	**IMPACT IF THE RISK OCCURS (Low, Medium, High)**
DoS attack		
Web defacing		
Loss of data from unauthorized access		
Loss of Web site data due to hardware failure		

Form of Survey for Determining Risks

- Table 5-3 shows how the results could look. The average probabilities and impacts have been summarized and entered into each box.
- For example, for the DoS attack, the average probability was determined to be 100 and the impact was also determined to be 100. This was calculated by averaging each of the inputs by the different experts.
- You determine the risk level by multiplying the Probability * the Impact.

Form of Survey for Determining Risks

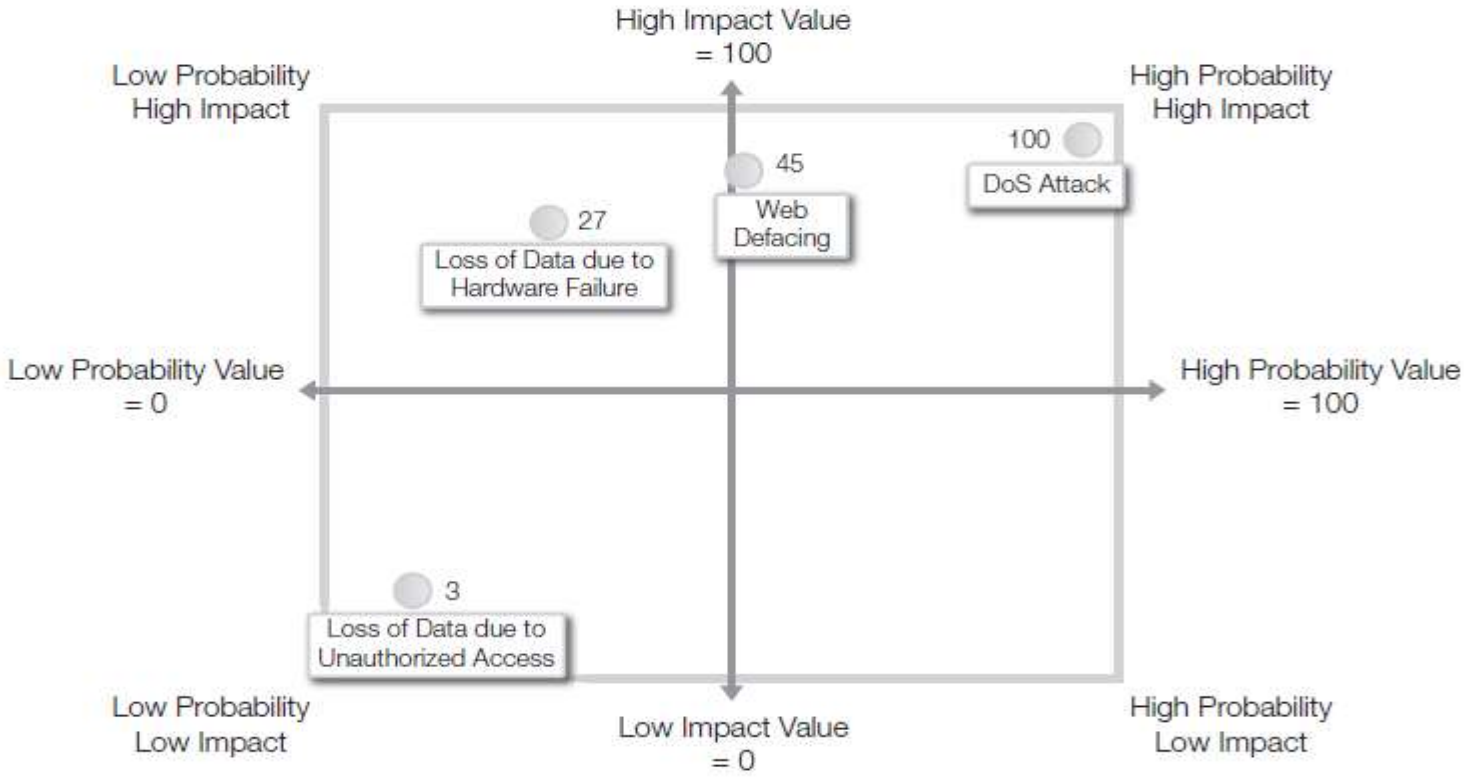
TABLE 5-3 Qualitative analysis survey results.

CATEGORY	PROBABILITY	IMPACT	RISK LEVEL (1 to 100)
DoS attack	100	100	100 (1.0 × 100)
Web defacing	50	90	45 (0.5 × 90)
Loss of data from unauthorized access	30	10	3 (0.3 × 10)
Loss of Web site data due to hardware failure	30	27	27 (0.3 × 90)

Form of Survey for Determining Risks

- You can present this data graphically in many ways. The risk matrix in Figure 5-2 shows one method.

FIGURE 5-2
Risk matrix.



Form of Survey for Determining Risks

- At this point, it's clear that the highest risk is from a DoS attack. It has a risk level of 100. The lowest risk level is 3 for the loss of data from unauthorized access.
- Loss of data sounds as if it would be very important. However, if existing controls and practices have removed most of the risk, the impact is reduced.
- For example, all non-public data could already have been removed from the Web site. While someone may try to hack into the Web site to get the data, the impact is Low since the site holds only public data.

Form of Survey for Determining Risks

- On the other hand, the risk of a DoS attack clearly rises to the top as the biggest risk.
- Based on the current controls, the experts agree that the system will be attacked. When it is attacked, they also agree that the impact will be high.
- The list of risks from most important to least important is:
- Priority 1—DoS attack, with a value of 100
- Priority 2—Web defacing, with a value of 45
- Priority 3—Loss of Web site data due to hardware failure, with a value of 27
- Priority 4—Loss of data from unauthorized access, with a value of 3.

(2) Evaluating the Effectiveness of Controls

- A this point, you could determine which safeguards or controls to apply for high-impact risks.
- A survey could help here also. For example, you could use the following survey.
- Notice that “Loss of data from unauthorized access” is not included in the survey table. Because the experts have agreed that it doesn’t present a risk, there is no need to mitigate it.
- Said another way, management in this case has decided to accept the risk.

(2) Evaluating the Effectiveness of Controls

Survey for Determining Safeguards or Controls

The following table lists controls in the left column. Across the top it lists risks. Please enter a value of Low, Medium, or High in each box. The value you enter should indicate the value of the control to mitigate the risk. For example, if you think placing the Web server in a DMZ will have a high success rate in preventing DoS attacks, enter High in this box. If you think it will have a low success rate, enter Low.

Mitigation choices survey.			
CONTROL	**DOS ATTACK** (Low, Medium, High)	**WEB DEFACING** (Low, Medium, High)	**LOSS OF WEB SITE DATA DUE TO HARDWARE FAILURE** (Low, Medium, High)
Place Web server in DMZ			
Add IDS			
Add RAID for data			
Create backup plan			

(2) Evaluating the Effectiveness of Controls

• Just as you can summarize the risks, you can also summarize the effectiveness of the controls. Table 5-4 shows the presumed results of the survey. As in other surveys, high has a value of 100. Medium has a value of 50. Low has a value of 10.

• RAID is an acronym for redundant array of independent disks. It is also called “redundant array of inexpensive disks.” Different RAID configurations allow a system to continue to run even if a disk drive fails. Sophisticated RAIDs allow a system to operate even if more than one disk drive fails. RAID provides fault tolerance. A fault can occur and the disk subsystem can tolerate it. It will continue to operate. “IDS” stands for intrusion detection system.

(2) Evaluating the Effectiveness of Controls Cont..

TABLE 5-4 Mitigation choices survey results.

CONTROL	DOS ATTACK	WEB DEFACING	LOSS OF WEB SITE DATA DUE TO HARDWARE FAILURE
Place Web server in DMZ	100	75	10
Add IDS	75	25	10
Add RAID for data	10	10	100
Create backup plan	10	50	100

(2) Evaluating the Effectiveness of Controls Cont..

- From Table 5-4 you can see that placing the server in the DMZ will provide the best protection from a DoS attack.
- Additionally, an IDS will also provide a high level of protection.
- The table helps to match up the best controls for the individual risks as follows:
- DoS attack—Protect with DMZ and/or IDS.
- Web defacing—Protect with DMZ.
- Loss of Web site data due to hardware failure— Protect with RAID and backup plan.

Benefits of Qualitative Assessment

A qualitative assessment has several primary benefits:

- Uses the opinions of the experts
- Is easy to complete
- Uses words that are easy to express and understand
- Data is gathered from the experts. These people know the systems the best. Their combined system knowledge and experience allows them to identify the source of problems quickly. As long as you have access to the experts, the RA is easy to complete. You don't even need to have them meet together. You can interview them separately. You can provide the experts with surveys and have them complete the surveys at their own pace.

Benefits of Qualitative Assessment Cont..

- The qualitative risk assessment uses scales. These scales can easily be adapted to the culture of the organization. They allow individuals to understand what the values are, and they can be expressed in words they use every day. This also makes it easier to involve people who may be expert in their field, but not an expert on security or computers.

Performing an Assessment with the Delphi Method

- One way that is commonly used to perform a qualitative assessment is the Delphi Method.
- This can be used to gather data and help create or identify a consensus.
- A primary benefit of the Delphi Method is that it allows individuals to freely share their opinions without pressure. Instead of all the participants talking through an issue in a meeting, responses are gathered independently.

The Delphi Method can be accomplished in several ways. One way is to work through the following steps:

Performing an Assessment with the Delphi Method Cont…

1. Identify a problem. This can be a single IT system or a group of servers. The problem should be within the knowledge of experts you'll add to the team. For example, the problem could be related to the Web site failures. It could be stated as: Web Server1 has suffered four failures in the past year resulting in losses.
2. Gather input from experts. Send the problem to the group of experts and ask them to respond. For the Web server failure, you could ask them to identify primary risks. If you have an idea of the causes, you can then ask them to identify the probability and risk. If you know the highest risks, you can repeat the process to identify the best solutions.

Performing an Assessment with the Delphi Method Cont…

3. Collate the responses. The responses will be in different forms for different phases. For example, the responses could just be a list of risks. They could be a prioritized list of risks. Or they could be a list of controls to mitigate the risk.
4. Share the results. This will also look different depending on the phase you're in. If you've just collated a list of risks, you can now ask the team to identify the probability and impact of each risk. When you start working on the controls, you can repeat the process. Ask for a list of controls to mitigate the risk. You can then ask the team to identify the effectiveness of the different controls for specific risks.
5. Repeat as necessary. Repeat the process until all the data is gathered.

Sample Risk Assessment Report

- A risk assessment ends with a report. This report can then be used by management to decide what controls to implement. The following is a list of topics that are commonly included in a risk assessment report:
- Introduction—The introduction provides the purpose and scope of the risk assessment. It includes descriptions about the components, users, and locations for the system considered in the RA.
- Risk assessment approach—This section identifies the approach used to complete the RA. It includes details on how the data was collected and who was involved. If a qualitative approach is used it will describe the risk scale.

Sample Risk Assessment Report Cont..

- System characterization— This section provides more details on the system. It could include details on the hardware, software, or network connections. It may include diagrams to graphically show the assessed system.

- Threat statement—This section lists potential threats, threat sources, and threat actions. For example, one threat may be an attacker launching a denial of service (DoS) attack on an Internet facing server.

Sample Risk Assessment Report Cont..

- Risk assessment results—Results can be listed as vulnerability/threat pairs representing a risk. The risk is described with existing security controls. The likelihood of the risk occurring with current controls is listed. How the risks are described depends on which analysis is used. A quantitative method uses terms such as SLE, ARO, and ALE. A qualitative method identifies probability and impact based on a defined scale. All of this data is supported with discussions identifying how the result was obtained.
- Control recommendations—A list of recommended safeguards or controls is provided. This list can include comments on the effectiveness of the controls. A quantitative method will often be accompanied by a CBA for each control. qualitative method will often rank the effectiveness of the control.

Sample Risk Assessment Report Cont..

- Summary—The summary can be in one or more tables that summarize the results. This format makes it easy for management to see the highest risks based on the risk rating. It also makes it easy to approve any of the recommendations.

Best Practices for Risk Assessment

- The following list identifies several best practices for risk assessment approaches:
- Start with clear goals and a defined scope—Ensure that you know what you want to achieve with the assessment. A risk assessment should include a scope statement. The scope statement helps keep the assessment on track and prevents scope creep.
- Ensure senior management support—Senior management needs to be committed to the RA. Without support, the RA loses value. When RA teams realize the RA isn't valued, they put less time and effort into it. An assessment without senior management support is almost doomed from the outset.

Best Practices for Risk Assessment Cont..

- Build a strong RA team—The value of the RA is based on the competence and expertise of the RA team. Team members should have expertise in the system. For example, imagine that you are using a qualitative analysis. If you are gathering data from personnel who aren't experts, their opinions aren't as valuable. Team members should also understand the methodology used for the RA.

Best Practices for Risk Assessment Cont..

- Repeat the RA regularly—Threats, risks, and vulnerabilities are constantly evolving. An RA should be repeated on a regular basis. Some federal agencies require RAs to be repeated at least every three years. Many organizations create a risk assessment policy. The policy identifies what the organization is expected to do on a recurring basis. It can also be used to define generic goals for any risk assessments.

Best Practices for Risk Assessment Cont..

- Define a methodology to use—If you consistently use the same methodology, people become better at it. For example, your company could decide to use qualitative risk assessments on a regular basis. If this is the case, you should also define scales that should be used. When assessments are done the same way, they are easier to accomplish and tend to provide higher quality results.

Best Practices for Risk Assessment Cont..

- Provide a report of clear risks and clear recommendations—Every risk assessment should end with a report that identifies the findings. These findings should be clearly stated. It's important to ensure that the risks are clearly defined. It's even more important to ensure that recommendations are clear. The whole purpose of the RA is ultimately to mitigate risks with recommended controls. If the recommendations aren't clear, the report loses a significant amount of value.

End

Security Risk Management and Ehics

Chapter Four: Identifying and Analyzing Threats, Vulnerabilities, and Exploits

Textbook : Freund, J., & Jones, J, "Measuring and managing information risk: A FAIR Approach", 1st Edition, Butterworth-Heinemann, 2015. ISBN-13: 9780127999326.

Chapter4: Topics

This chapter covers the following topics and concepts:

- What threat assessments are
- What vulnerability assessments are
- What exploit assessments are

Chapter4: Goals

When you complete this chapter, you will be able to:

- Describe techniques used to identify threats
- List best practices for threat assessments within the seven domains

of a typical IT infrastructure

- Describe the value of reviewing documentation for a vulnerability

assessment

- Describe the value of reviewing system logs, audit trails, and intrusion detection system outputs for a vulnerability assessment

Chapter4: Goals

- Identify tools used to perform vulnerability scans
- List best practices for vulnerabilities assessments within the seven domains of a typical IT infrastructure
- Identify exploits throughout the seven domains of a typical IT infrastructure

Threat Assessments

- A threat assessment identifies and evaluates potential threats.
- The goal is to identify as many potential threats as possible. You then evaluate the threats.
- One important element is an estimate of a threat's frequency.
- In previous Chapter, we covered risk assessments. As a reminder, a risk assessment is performed for a specific time.
- Risks that exist today may not exist in a year. Similarly, a threat assessment is performed at a specific time.
- The threat assessment evaluates current threats in the existing environment.

Threat Assessments Cont.,

• Threats were presented in Chapter 1. A threat is any activity that represents a possible danger. This includes any circumstances or events with the potential to adversely cause an:

(1) Impact on confidentiality—Any unauthorized disclosure of data. You can apply access controls to ensure only specific users have access to data. Encryption techniques also help to protect confidentiality.

Threat Assessments Cont.,

(2) Impact on integrity—The modification or destruction of data. Access controls protect data from malicious attackers who want to modify or destroy data. Hashing techniques verify integrity by detecting if the data has been modified.

(3) Impact on availability—The availability of any service or system. Different fault tolerance strategies ensure that systems and services continue to operate even if an outage occurs. Data is backed up to ensure it can be restored even if data is lost or becomes corrupt.

Threat Assessments Cont.,

- Figure 8-1 shows the different threats to an organization. They are generically categorized as either human or natural.
- Human threats can be internal or external. They can also be

intentional or unintentional.

- Internal threats are by far the biggest threats to a company.
- Natural threats occur from weather or other non-manmade events.
- External attackers can be hackers launching denial of service (DoS) attacks on your network. They can be malware writers trying to access, modify, or corrupt your organization's data. They can even be terrorists launching attacks on buildings or entire cities.

Threat Assessments Cont.,

- Internal users can also cause damage. A disgruntled employee may be able to access, modify, or corrupt the organization's data. If proper access controls aren't used, other employees may also access, modify, or corrupt data. Although the disgruntled employee's actions will be purposeful, regular employees' actions are accidental.

- Natural threats include weather events such as floods, earthquakes, tornados, and electrical storms. Fires can also be a natural threat.

The Top Threats Are Internal

• It's not always apparent, but the top threats are internal. Some are accidental, and some are malicious. However, if you can train employees and control their actions, you'll reduce a significant number of threats.

• Some of the common threats from internal sources are:

(1) unintentional access—Access controls take a lot of effort to implement and maintain. This includes ensuring authentication processes are secure. It also includes enforcement of least-privilege and need-to-know policies. When users have access to data they don't need, the data is at risk. Users can accidentally delete the data. They can also share the data with someone else who shouldn't have access to it.

The Top Threats Are Internal

(2) Disgruntled ex-employees—When an employee is terminated, the user account should be either deleted or disabled. If not, the ex-employee may be able to access the same data or systems. The ex-employee could also pass on his or her credentials to someone else in-house to act as a proxy. The unauthorized access could result in data corruption or system sabotage.

(3) Responding to phishing attempts—Many users don't understand the risks with computers. More sophisticated phishing attempts target specific companies and fool the users. Spear-phishing is a targeted phishing attempt that looks as if it's coming from someone in the company.

The Top Threats Are Internal

(4) Forwarding viruses—Users can open infected e-mails and forward them to coworkers without realizing the danger. Users can bring viruses from home on universal serial bus (USB) flash drives.

(5) Lack of laptop control—Laptops are easily stolen. When users don't exercise physical control over laptops, the computers often disappear. The organization loses the hardware and software. What's more, data on the laptop is compromised.

Threat Assessments Cont.,

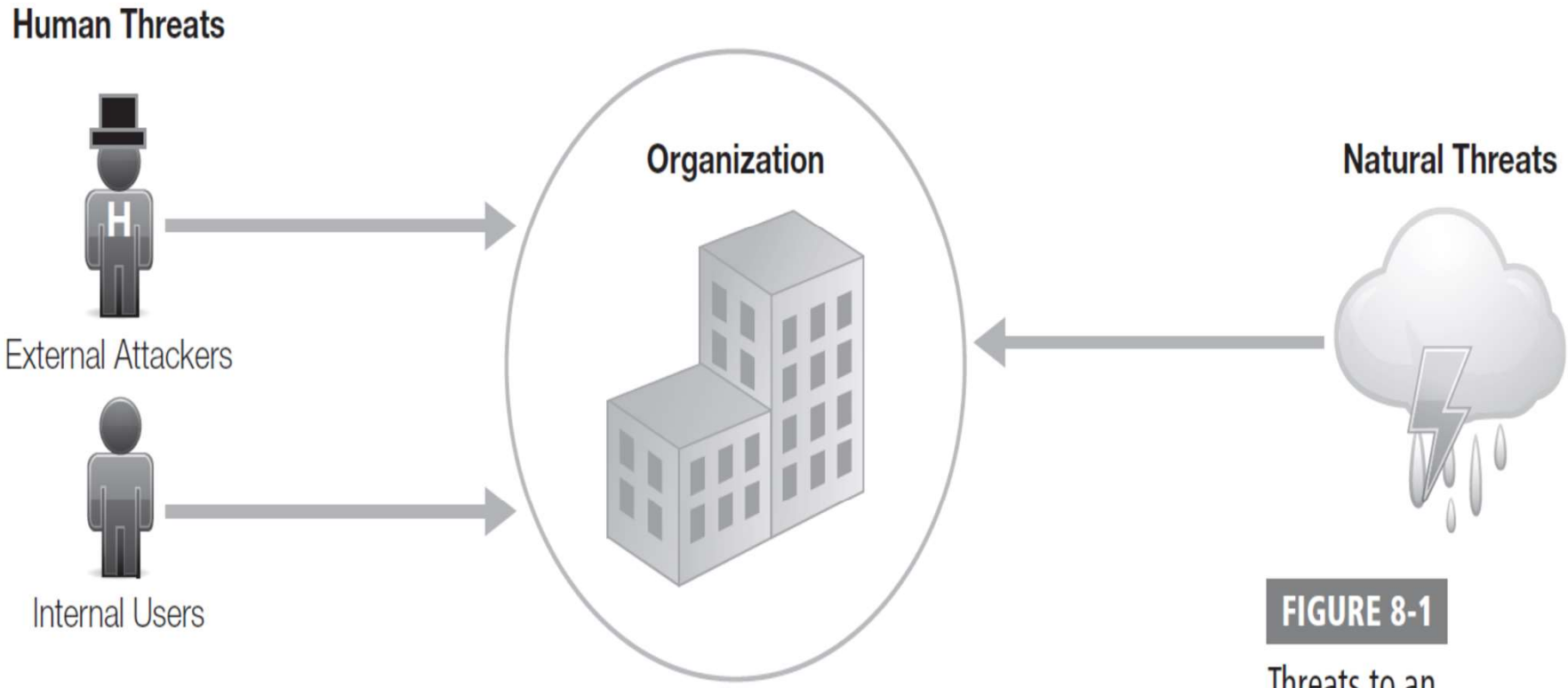


FIGURE 8-1

Threats to an organization.

Threat Assessments Cont.,

- The goal of a threat assessment is to identify threats. You can identify threats by reviewing historical data. You can also identify threats using threat modeling.
- After you've identified threats, you'll try to determine the likelihood of the threat. Some threats are more likely to occur, while others are less likely. Next, you prioritize the threats. There are times when you'll be able to match threats with vulnerabilities to determine costs.
- However, other times you won't be able to identify costs without also completing a vulnerability assessment.

Threat Assessments Cont.,

• The last step in a threat assessment is to provide a report. This report lists the findings. It includes the threats, the likelihood, and any identified costs.

• This section on threat assessments includes:

- Techniques for identifying threats

- Best practices for threat assessments within the seven domains of a typical IT infrastructure

Techniques for Identifying Threats

- There are two primary techniques you can use to identify threats.

(1) You can review historical data.

(2) You can also perform threat modeling.

- The techniques you choose depend largely on your environment and available materials. It's possible to use both techniques.

- If you have historical data available, this is often the easier approach. Historical data provide specific information on past threats.

Techniques for Identifying Threats Cont..,

- However, there is no guarantee that past threats will repeat.
- Additionally, there is no guarantee that a new threat won't appear.

- Threat modeling is more complex. It requires you to examine systems and services from a broader perspective. The process can be very time consuming.

(1) Review Historical Data

• One of the best ways to determine what threats exist is to analyze past incidents. This includes past incidents at the organization, at similar organizations, and in the local area:

• Organization—A review of past incidents will reveal threats that have resulted in losses.

• Similar organizations—Incidents with organizations in the same business will reveal possible threats in your organization.

• Local area—Natural and weather events are likely to repeat in the same area.

(1) Review Historical Data Cont..,

• You can gather this data by compiling records and conducting interviews. Data can be compiled from any existing records. These can be security records. They can be insurance claims. You can also review troubleshooting records to determine outages and their causes. You can conduct interviews with management and other employees. Employees often know exactly what the problems are and where the threats exist. Management knows the particular threats that have resulted in significant losses.

(1) Review Historical Data Cont..,

• Organization Historical Data. You can review an organization's historical data to identify past incidents from threats. Past incidents can take many forms. They can result from users accidentally or maliciously causing problems. They can come from external attackers. They can come from natural events. Here are a few possible examples:

(1) Internal users—Users were granted access to data they didn't need. They stumbled upon it and shared it with coworkers. This resulted in unauthorized disclosure of confidential data.

(1) Review Historical Data Cont..,

(2) Disgruntled employee—An employee was terminated for cause on a Monday. His account was not disabled or deleted. The employee accessed his account on Wednesday and deleted a significant amount of data. Some of the data was not backed up and was lost permanently.

(3) Equipment failure—A server crashed after a power spike. The server remained down for several hours until a power supply was replaced.

(1) Review Historical Data Cont..,

(4) Software failure—An ordering database application crashed on a database server. The server had to be rebuilt from scratch. Administrators reinstalled the operating system. They reinstalled the database application. They then restored the data from backups. This process took over 10 hours and customers could not place online orders during this time.

(5) Data loss—All users are required to store their data on a central file server. The data is backed up once a week on Sunday. The file server crashed on a Wednesday and many users lost over two days of work.

(6) Attacks—An e-mail server became infected with a virus. This virus spread to all the e-mail users' mailboxes. It took approximately two days to clean the system and return e-mail services to users.

(1) Review Historical Data Cont..,

- Similar Organization's Historical Data. Many threats are common to similar organizations. By identifying the threats against similar organizations, you can identify possible threats against your organization.
- For example, attackers get a kick out of defacing any law enforcement Web site. Years ago, there were many instances of such Web sites being defaced. However, most law enforcement agencies recognize the threat today. They take additional steps to protect their Web sites. This is not to say they are immune to the threat. They have simply taken extra steps to protect themselves.
- Any organization with public-facing servers faces similar threats. Apache is a popular Web server product that can run on UNIX, Linux, and Microsoft platforms. It serves Web pages over the Internet. Any company that hosts Apache faces the same threats.

(1) Review Historical Data Cont..,

Local Area Data. Primary considerations for the local area are weather conditions and natural disasters. If a location is on the coast, and the coast has had hurricanes in the past, it will likely have hurricanes in the future. If a location is in a flood zone, it will likely flood in the future.

(2) Threat Modeling

- Threat modeling is more complex than just researching historical data for threats.
- It is a process used to assess and document an application or system's security risks.
- Ideally, you perform threat modeling before writing an application or deploying a system. This is done when security is considered throughout the full life cycle of a product or service. In other words, if security is only considered at the end of the project, it frequently falls short.

(2) Threat Modeling Cont..,

- When threat modeling is used, you first need to identify the assets you want to evaluate. In previous chapters covered the importance of asset management. Asset management helps you to identify the assets that are important to an organization, including their value. You can then take steps to identify the threats against the valuable assets.

- An excellent starting point when performing threat modeling is to use the seven domains of a typical IT infrastructure. As a reminder, the seven domains were covered in Chapter 1. They are presented later in this section with some best practices.

(2) Threat Modeling Cont..,

- When threat modeling is used, you first need to identify the assets you want to evaluate. In previous chapters covered the importance of asset management. Asset management helps you to identify the assets that are important to an organization, including their value. You can then take steps to identify the threats against the valuable assets.

- An excellent starting point when performing threat modeling is to use the seven domains of a typical IT infrastructure. As a reminder, the seven domains were covered in Chapter 1. They are presented later in this section with some best practices.

(2) Threat Modeling Cont..,

- Some of the key questions you can ask yourself when performing threat modeling are:
- What system are you trying to protect?
- Is the system susceptible to attacks?
- Who are the potential adversaries?
- How might a potential adversary attack?
- Is the system susceptible to hardware or software failure?
- Who are the users?
- How might an internal user misuse the system?

(2) Threat Modeling Cont..,

- Threat modeling for complex systems can become quite extensive. Depending on the system you're evaluating, you may need to define specific objectives to limit the scope of the evaluation.
- When performing threat assessments, it's important to ensure you understand the system or application you're evaluating. This includes what systems are involved. It also includes an understanding of how data flows in and out of systems. Without a full understanding of a system, it's difficult to shift your perspective to an attacker. Understanding a system often requires you to interview the experts and review the documentation on the system.

Best Practices for Threat Assessments Within the Seven Domains of a Typical IT Infrastructure

- One method of ensuring that you have addressed all threats is to use the seven domains of a typical IT infrastructure.

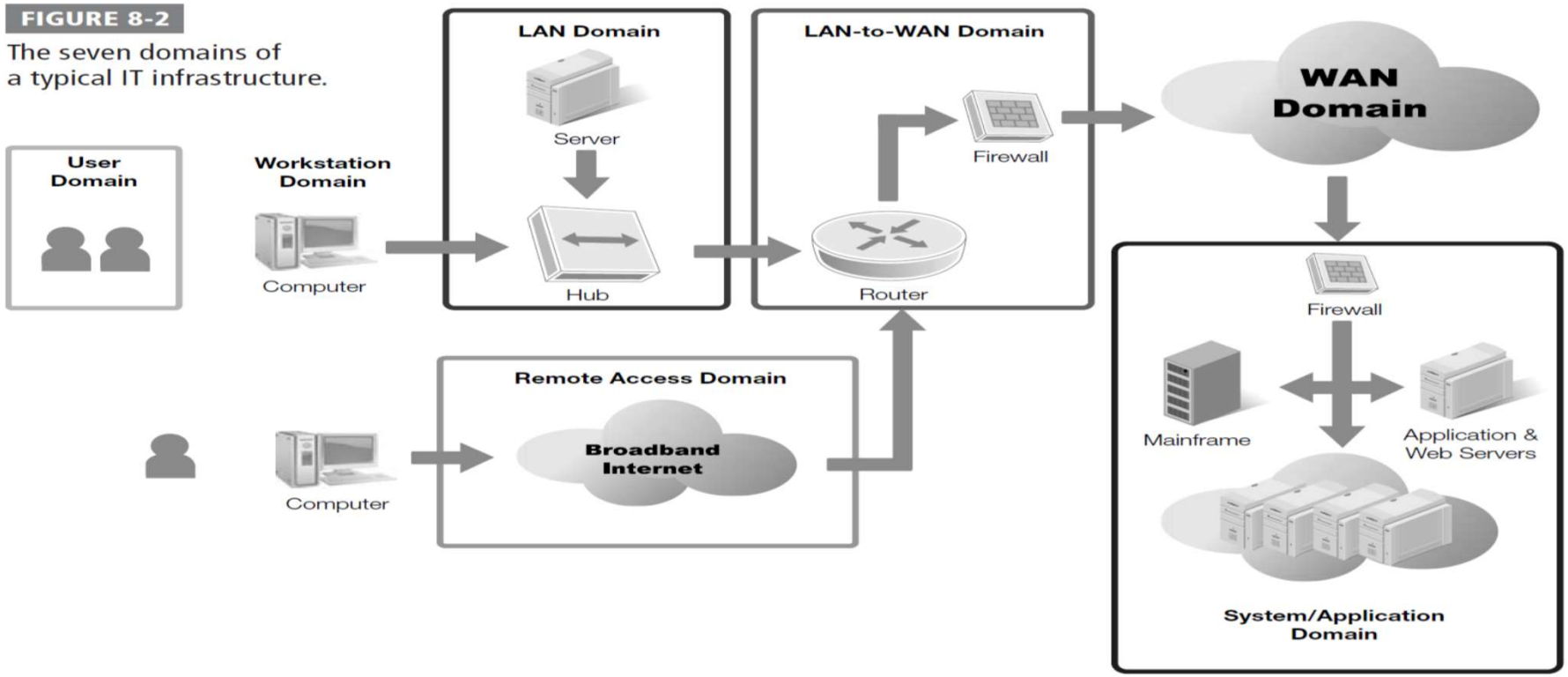
- As a reminder, the seven domains are the User Domain, Workstation Domain, LAN Domain, LAN-to-WAN Domain, WAN Domain, Remote Access Domain, and System/Application Domain. Figure 8-2 shows the seven domains.

- You can methodically go through each of these domains and evaluate the threats.

Best Practices for Threat Assessments Within the Seven Domains of a Typical IT Infrastructure Cont..,

- Some best practices you can use when evaluating these threats include:
- Verify that systems operate and are controlled as expected.
- Limit the scope of the assessment to a single domain at a time.
- Use documentation and flow diagrams to understand the system you're evaluating.
- Identify all possible entry points for the domain you're evaluating.
- Consider threats to confidentiality, integrity, and availability.
- Consider internal and external human threats.
- Consider natural threats.

Best Practices for Threat Assessments Within the Seven Domains of a Typical IT Infrastructure Cont..,



Vulnerability Assessments

- A vulnerability assessment (VA) is performed to identify vulnerabilities within an organization.
- Vulnerabilities are any weaknesses in your IT infrastructure. They can exist for a specific server. They can exist for entire networks. They can also exist with personnel.
- For example, a single Web server could be vulnerable to a buffer overflow attack. Imagine that a buffer overflow bug has been discovered in May. If it's not patched until July, it remains vulnerable between May and July.

Vulnerability Assessments Cont..,

- Entire networks can be vulnerable if access controls aren't implemented. For example, if all users are granted the same rights and permissions for a network, there is no access control. All data on the network could be vulnerable to unauthorized disclosure. However, administrative models can be used to implement access controls. The principles of least privilege and need to know ensure that users have the access they need, but no more.
- Vulnerabilities exist with personnel if they don't understand the value of security. Social engineering tactics trick people into revealing sensitive information or taking unsafe actions. If users don't understand the value of security practices, they are less likely to take specific actions. For example, an employee may receive a phone call that goes like this:

Vulnerability Assessments Cont..,

"Hi. This is Joe in IT. We're doing a system upgrade and discovered a problem with your user account. In order to fi x it and ensure you don't lose any data, we'll need to log onto your account from the server. Can you give me your user name and password?"

Of course, Joe doesn't work in the IT shop, but instead is trying to get a user to reveal a user name and password. If users frequently give out their password to administrators, this will easily succeed. If users are told to never give out their passwords, it may not succeed.

Vulnerability Assessments Cont..,

- You perform vulnerability assessments to check for any of these types of vulnerabilities. You will perform some assessments more often than others.

- Automated vulnerability scans of systems are usually performed more frequently. You can do them with assessment tools on a weekly basis. You can perform audits on an annual basis to see if security controls are being used as expected. For example, an annual audit can detect if access controls are still being used as expected. Additionally, you can do tests to see if personnel respond to social engineering tactics on annual basis.

Vulnerability Assessments Cont..,

You can perform vulnerability assessment testing internally or externally:

- Internal assessments—Security professionals try to exploit the internal system to see what they can learn about vulnerabilities. Some large companies have dedicated staff that regularly perform assessments. A smaller company could assign this as an extra task

for an IT administrator.

- External assessments—Personnel outside the company try to exploit the system to see what they can learn. These are consultants hired to assess the security. Outside consultants provide a fresh look at your system. They are usually very good at quickly identifying weaknesses.

Vulnerability Assessments Cont..,

This section on vulnerability assessments includes the following topics:

- Documentation review
- Review of system logs, audit trails, and intrusion detection system outputs
- Vulnerability scans and other assessment tools
- Audits and personnel interviews
- Process analysis and output analysis
- System testing
- Best practices for performing vulnerability assessments within the seven domains of a typical IT infrastructure

Documentation Review

- One of the steps you can take when performing a VA is to review the available documentation. The documentation can be from multiple sources, including:

(1) Incidents—If any security incidents have occurred, you should review the documentation from the incident. Often, the cause of an incident is directly related to a vulnerability. For example, a successful buffer overflow attack on an Internet facing server may have resulted in a malware infection. This may indicate that the system is not being updated often enough.

(2) Outage reports—You can investigate any outage that has affected the mission of the business. If the outage affected the bottom line, you can probably identify a vulnerability.

Documentation Review Cont..,

(3) Assessment reports—Past assessment reports should be reviewed. This helps identify common problems. It also helps identify problems that have not been corrected.

Review of System Logs, Audit Trails, and Intrusion Detection System Outputs

- In addition to reviewing past assessment reports, there is a lot of additional information you can review to determine vulnerabilities. The three common sources of information are system logs, audit trails, and intrusion detection systems.

(1) System Logs

- Any computer system has some type of system logs. These logs have different names for different operating systems, but overall have the same purpose. They log data based on what the system is doing.

Review of System Logs, Audit Trails, and Intrusion Detection System Outputs

- For example, Microsoft Windows systems have a log called System. You view this log using the Windows Event Viewer. The System log records system events such as when systems and services start or stop. The log records errors, warning, and information events.

- You can determine what is happening to a system by reviewing the system logs. Some events such as warnings and errors will jump right out, indicating obvious problems. Others need a little more analysis to identify trends.

Review of System Logs, Audit Trails, and Intrusion Detection System Outputs

(2) Audit Trails

- An audit trail is a series of events recorded in one or more logs. These logs are referred to as audit logs, but an audit trail can be recorded in many types of logs.
- For example, Microsoft Windows includes a Security log that records auditable events. Additionally, security applications like firewalls record auditable events.
- Any type of audit log attempts to log at least who, what, when, and where. If a user is logged on, the credentials are used to identify who accessed the data. For some logs such as firewall logs, the “who” may be the source’s Internet Protocol (IP) address instead of a user name.

Review of System Logs, Audit Trails, and Intrusion Detection System Outputs

- Auditable events are any events that you want to track. For example, you may want to know if anyone accessed a folder. You could enable auditing on the folder, and each time someone accessed any files within the folder, the access would be recorded. The event would include the user name, what file was accessed, when it was accessed, and the server or computer where it was accessed.
- Many organizations have automated systems that can review audit trails. An automated system has the capability of examining logs from multiple sources. These are sometimes combined with intrusion detection systems that can review the events to detect intrusions.

Review of System Logs, Audit Trails, and Intrusion Detection System Outputs

- Auditable events are any events that you want to track. For example, you may want to know if anyone accessed a folder. You could enable auditing on the folder, and each time someone accessed any files within the folder, the access would be recorded. The event would include the user name, what file was accessed, when it was accessed, and the server or computer where it was accessed.
- Many organizations have automated systems that can review audit trails. An automated system has the capability of examining logs from multiple sources. These are sometimes combined with intrusion detection systems that can review the events to detect intrusions.

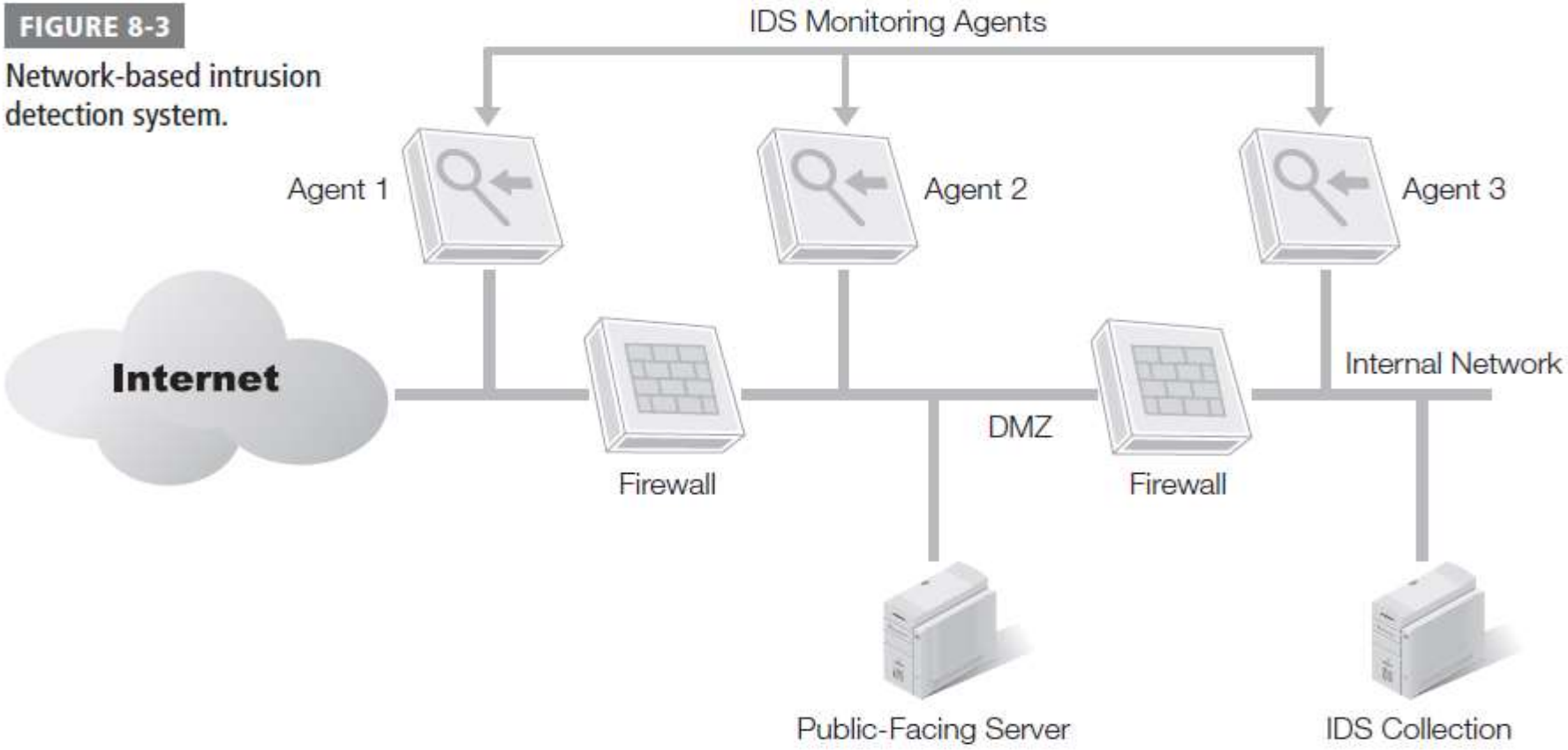
Review of System Logs, Audit Trails, and Intrusion Detection System Outputs

(3) Intrusion Detection System Outputs

- Intrusion detection system (IDS) is able to monitor a network or system and send an alert when an intrusion is detected.
- A host-based IDS is installed on a single system.
- A network-based IDS has several monitoring agents installed throughout the network that report to a central server.
- Figure 8-3 shows an example of a network-based IDS with three monitoring agents installed on the network. Notice the location of the three monitoring agents.

Review of System Logs, Audit Trails, and Intrusion Detection System Outputs

FIGURE 8-3
Network-based intrusion detection system.



Review of System Logs, Audit Trails, and Intrusion Detection System Outputs

- One is on the Internet side. One is in the demilitarized zone (DMZ). One is on the internal network.
- If you examine the output of the IDS, it will reveal several key points.
- These three agents work together to identify what type of attacks are launched against the network. They also give you insight into the success of different mitigation techniques.
- Events from agent 1 show how many attacks are launched against your network from the Internet.

Review of System Logs, Audit Trails, and Intrusion Detection System Outputs

- Events from agent 2 identify the attacks that are able to get through the external firewall. This shows you the effectiveness of the firewall against specific types of attacks. It also helps reveal the vulnerabilities for any public-facing servers in the DMZ.
- Agent 3 shows the attacks that are able to get through the second firewall of the DMZ.
- These attacks on your internal network can be very damaging if not addressed.

Review of System Logs, Audit Trails, and Intrusion Detection System Outputs

- Although the focus of Figure 8-3 is on attacks from the Internet, it's also possible to have internal attacks. The network agent on the internal network monitors for internal attacks. It's common for a network to have several internal agents installed to monitor an internal network.

- Internal attacks aren't necessarily from malicious users. Instead, internal attacks are often from malware that has infected one or more systems on the network. However, the benefit of a network-based IDS is early detection of an infection.

Vulnerability Scans and Other Assessment Tools

(4) Vulnerability Scans and Other Assessment Tools

- Many tools are available to perform vulnerability scans within a network.
- There are several commonly used tools, such as Nmap, Nessus, SATAN, and SAINT.
- These tools provide several benefits. Some of the benefits include:
- Identify vulnerabilities—They provide a fast and easy method to identify vulnerabilities. You simply run the scan and then analyze the report.

Vulnerability Scans and Other Assessment Tools

- Scan systems and network—Vulnerability scanners can inspect and detect problems on the network and on individual hosts. They can detect vulnerabilities based on the operating system, applications, and services installed on the host. They can detect open ports and access points on the network.
- Provide metrics—A key part of management is measurement. If you can measure something, you can identify progress. This is also true with vulnerabilities. If you are just starting to run regular vulnerability scans, the scans will likely discover many vulnerabilities.

Vulnerability Scans and Other Assessment Tools

- Six months later, if you analyze the metrics, you'll notice that the issues are significantly reduced. If not, you may have other problems. For example, if you have all of the same vulnerabilities six months after the first scan, the vulnerabilities are not getting fixed.
- Document results—The resulting documentation provides input for internal reports. It also provides documentation for compliance. You can use scanner reports to prove compliance with different laws and regulations.

Vulnerability Scans and Other Assessment Tools

(5) Audits and Personnel Interviews

- An audit is performed to check compliance with rules and guidelines. A VA audit checks compliance with internal policies. In other words, an audit will check to see if an organization is following the policies that are in place.

- For example, an organization may have a policy in place related to employees who leave the company. The policy may state that user accounts should be disabled if an employee leaves. Six months later, the account should be deleted.

Vulnerability Scans and Other Assessment Tools

• An audit determines if the policy is being followed. The audit can be quick and automated if the auditor has some scripting skills. An auditor could write a script to check for enabled accounts that haven't been used in the past 15 days. The output is then checked with the human resources department to determine if any of these users are still employed. A similar script could be used to determine if any accounts exist that haven't been used in the past six months.

Vulnerability Scans and Other Assessment Tools

- In addition, you can conduct personnel interviews to identify the security knowledge of personnel. For example, employees could be asked when it is acceptable to give out their password. A secure organization will have a policy in place stating that users should never give out their password to anyone.

Vulnerability Scans and Other Assessment Tools

(6) Process Analysis and Output Analysis

• Process analysis is performed in some systems to determine if vulnerabilities exist in the process. In other words, instead of just looking at the output, you evaluate the processes used to determine the output.

• Output analysis, on the other hand, is performed by examining the output to determine if a vulnerability exists. Neither analysis is superior to the other. However, there are times when one will be preferable over the other.

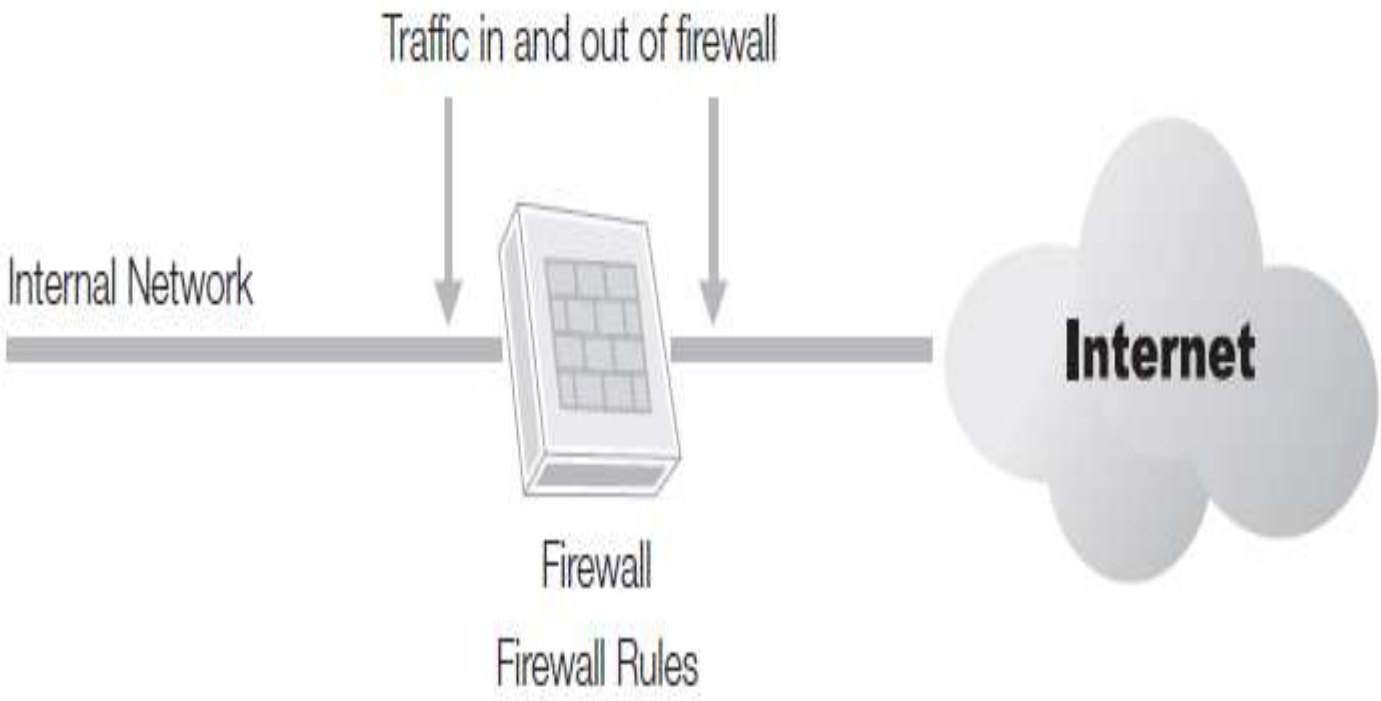
Vulnerability Scans and Other Assessment Tools

- For example, you may be concerned about the effectiveness of a firewall. Firewalls use rules to determine if traffic is allowed. You can use either process analysis or output analysis to determine the effectiveness of the firewall.
- Consider Figure 8-4. The firewall is blocking and allowing traffic into and out of the network. Process analysis requires you to review all the rules to determine if the rules provide the desired security. Output analysis will examine the input and output of the firewall to determine if only desired traffic is allowed through the firewall. If the firewall has only five rules, process analysis would be completed rather easily.

Vulnerability Scans and Other Assessment Tools

FIGURE 8-4

Network-based intrusion detection system.



Vulnerability Scans and Other Assessment Tools

- For example, you may be concerned about the effectiveness of a firewall. Firewalls use rules to determine if traffic is allowed. You can use either process analysis or output analysis to determine the effectiveness of the firewall.
- Consider Figure 8-4. The firewall is blocking and allowing traffic into and out of the network. Process analysis requires you to review all the rules to determine if the rules provide the desired security. Output analysis will examine the input and output of the firewall to determine if only desired traffic is allowed through the firewall. If the firewall has only five rules, process analysis would be completed rather easily.

Vulnerability Scans and Other Assessment Tools

(7) System Testing

- System testing is used to test individual systems for vulnerabilities. This includes individual servers and individual end-user systems. The primary testing performed on systems is related to patches and updates. This is because the majority of vulnerabilities occur because of bugs that are resolved by patching.
- For example, you could have a bank of servers that are running Microsoft Windows Server 2008. Several patches and updates have been released for the servers since they've been installed. System testing queries the servers to determine if they are up-to-date.

Vulnerability Scans and Other Assessment Tools

• For example, Microsoft includes traditional tools such as Windows Server Update Services (WSUS) and System Center Configuration Manager (SCCM). Each of these server products can query systems in the network and ensure they have all the appropriate updates. If a system doesn't have an update, WSUS or SCCM can push the update to the system and double check to ensure it has been installed..

Vulnerability Scans and Other Assessment Tools

For example, Microsoft Security Bulletin MS08-067 identified a critical vulnerability in the Server service for almost any Windows systems from Windows 2000 to Windows 2008. This vulnerability allows attackers to send specially crafted requests to the systems that can then run arbitrary code. The arbitrary code can install malware. You can read about this vulnerability at http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx.

Vulnerability Scans and Other Assessment Tools

(8) Functionality Testing

- Functionality testing is primarily used with software development. It helps ensure that a product meets the functional requirements or specifications defined for the product.
- One of the problems that can occur with software development is scope creep.
- This occurs when additional capabilities are added that weren't originally planned. In other words, the add-ons are outside the scope of the original product specifications. While this looks good on the surface, it adds additional security issues.

Vulnerability Scans and Other Assessment Tools

(8) Functionality Testing

- Functionality testing is primarily used with software development. It helps ensure that a product meets the functional requirements or specifications defined for the product.
- One of the problems that can occur with software development is scope creep.
- This occurs when additional capabilities are added that weren't originally planned. In other words, the add-ons are outside the scope of the original product specifications. While this looks good on the surface, it adds additional security issues.

Vulnerability Scans and Other Assessment Tools

(9) Access Controls Testing

- Access controls testing verifies user rights and permissions. A “right” grants the authority to perform an action on a system, such as to restart it. A “permission” grants access to a resource, such as a file or printer.
- Most organizations have administrative models in place that specify what rights and permissions regular users are granted.
- These models ensure that users have what they need to perform their job, but no more. They help support security principles of least privilege and need to know.

Vulnerability Scans and Other Assessment Tools

- Consider Figure 8-5. A company has some resources that only sales personnel should access. It has other resources that only IT department personnel should access.

- Access restrictions are enforced by putting employees into the appropriate groups and assigning permissions to the group.

Vulnerability Scans and Other Assessment Tools

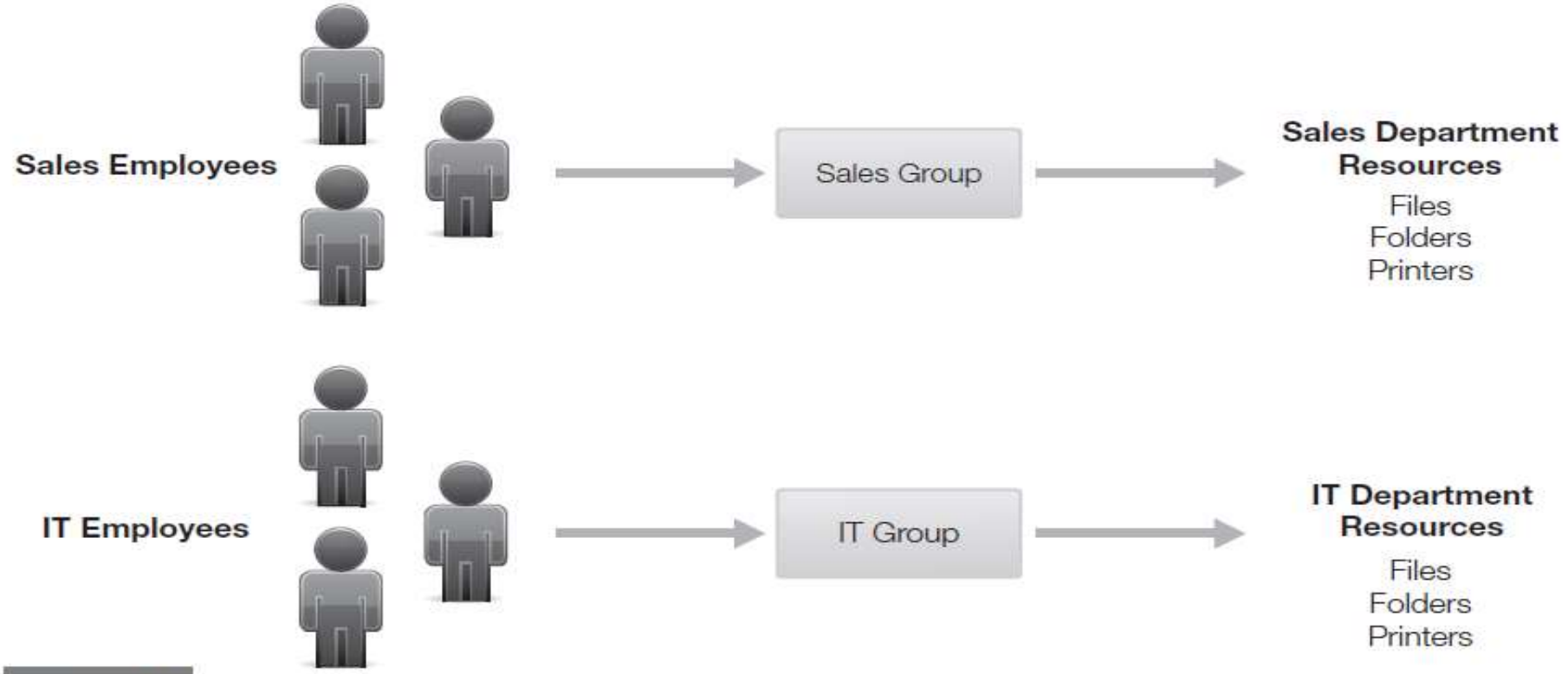


FIGURE 8-5
Access controls applied to users.

Vulnerability Scans and Other Assessment Tools

• Any member of the IT group automatically has access to the IT resources. Members of the Sales group do not have access to IT department resources. Members of the IT group do not have access to Sales department resources.

• Access controls testing verifies that the users are granted the rights and permissions needed to perform their jobs, and no more. It ensures that an administrative model is used as it was designed.

Vulnerability Scans and Other Assessment Tools

(10) Penetration Testing

- Penetration testing attempts to exploit vulnerabilities. In other words, you'll often complete a VA to discover vulnerabilities. You'll then perform a penetration test to see if a vulnerability can be exploited.
- A penetration test can be much more invasive than VA tests. Specifically, if a penetration test is successful, it may actually take a system down. With this in mind, you need to be cautious when performing penetration tests.

Vulnerability Scans and Other Assessment Tools

- Penetration testing verifies the effectiveness of countermeasures or controls. In other words, you've discovered a vulnerability and implemented a control to protect against the vulnerability. You can now perform a penetration test to see if the control works. If the penetration test is successful, you know the controls aren't adequate. You'll need to take additional steps to protect against an attack.

Best Practices for Performing Vulnerability Assessments Within the Seven Domains of a Typical IT Infrastructure

- Identify assets first—Asset management helps you identify what resources to protect. There is no need to perform VAs on all assets. You only want to take these steps on the valuable assets.
- Ensure scanners are kept up to date—Vulnerability scanners need to be updated regularly. This is similar to how antivirus (AV) software needs to be updated with malware definitions. An AV program that isn't kept up to date is only marginally better than no AV program at all. This is the same for a vulnerability scanner. A scanner that isn't kept up date is only marginally better than no scanner at all.

Best Practices for Performing Vulnerability Assessments Within the Seven Domains of a Typical IT Infrastructure

- Perform internal and external checks—Attacks can come from internal and external sources. You should perform VAs from internal and external locations. Check within the firewall. Check from outside the firewall. If you have a DMZ, check for vulnerabilities from outside the network.
- Document the results—Document the results of every VA. You can use this documentation in several ways. Older results can be compared against current results to track progress. Some VAs can be used to document compliance with laws and regulations.
- Provide reports—Provide reports to management. These reports will summarize the important findings and provide recommendations.

End

Security Risk Analysis and Management

Chapter Five: Developing Risk Management Plan

Dr. Mohammed Amin Almaiah
University of Jordan

Chapter5: Topics

This chapter covers the following topics and concepts:

- What the objectives of a risk management plan are
- What the scope of a risk management plan is
- How to assign responsibilities in a risk management plan
- How procedures and schedules are described in the risk management plan
- What the reporting requirements are
- What a plan of action and milestones is
- How to chart the progress of a risk management plan

THE UNIVERSITY OF JORDAN

Chapter5: Goals

When you complete this chapter, you will be able to:

- Describe the objectives of a risk management plan
- Describe the purpose of a plan's scope
- Identify the importance of assigning responsibilities
- Describe the purpose of the procedures list in a risk management plan
- List reporting requirements of a risk management plan
- Document findings of a risk management plan
- Create a plan of action and milestones
- Identify a milestone plan chart
- Identify a Gantt chart and define a critical path chart

THE UNIVERSITY OF JORDAN

Objectives of a Risk Management Plan

• The objectives identify the goals of the project. These objectives outline what you

should include in the plan. Some common objectives for a risk management plan are:

- A list of threats
- A list of vulnerabilities
- Costs associated with risks
- A list of recommendations to reduce the risks
- Costs associated with recommendations
- A cost-benefit analysis
- One or more reports

THE UNIVERSITY OF JORDAN

Two case study for performing risk management plan

Throughout this chapter, two examples are used. These examples show how you can create a risk management plan for actual projects. The two examples are:

(1) Web site—Your company, Acme Widgets, hosts a Web site used to sell widgets on the Internet. The Web site is hosted on a Web server owned and controlled by your company. The Web site was recently attacked and went down for two days. The company lost a large amount of money. Additionally, the company lost the goodwill of many customers. This was the second major outage for this Web site in the past two months. There have been many outages in the past three years.

Two case study for performing risk management plan

(2) Health Insurance Portability and Accountability Act (HIPAA) compliance—Your company recently purchased Mini Acme. Mini Acme has not complied with HIPAA. Management wants to identify the risks associated with this noncompliance. Managers also want to ensure that issues are corrected as soon as possible.

THE UNIVERSITY OF JORDAN

Case study 1: Web site

Determine the objectives of the Example: Web Site

The Acme Widgets Web site has suffered outages. These outages have resulted in unacceptable losses. These losses could have been prevented by managing risks with the Web site. You can use the risk management plan to identify these risks.

The objectives of the plan are to:

(1) Identify threats—This means any threats that

directly affect the Web site. These may include:

- Attacks from the Internet
- Hardware or software failures
- Loss of Internet connectivity

Case study 1: Web site

(2) Identify vulnerabilities—These are weaknesses and may include:

- Lack of protection from a firewall
- Lack of protection from an intrusion

detection system

- Lack of antivirus software
- Lack of updates for the server
- Lack of updates for the antivirus software

THE UNIVERSITY OF JORDAN

Case study 1: Web site

(3) Assign responsibilities—Assign responsibility to specific departments for collecting data. This data will be used to create recommendations. Later in the plan, you will assign responsibilities to departments to implement and track the plan.

(4) Identify the costs of an outage—Include both direct and indirect costs. The direct costs are the lost sales during the outage. The amount of revenue lost if the server is down for 15 minutes or longer will come from sales data. Indirect costs include the loss of customer goodwill and the cost to recover the goodwill.

THE UNIVERSITY OF JORDAN

Case study 1: Web site

(3) Assign responsibilities—Assign responsibility to specific departments for collecting data. This data will be used to create recommendations. Later in the plan, you will assign responsibilities to departments to implement and track the plan.

(4) Identify the costs of an outage—Include both direct and indirect costs. The direct costs are the lost sales during the outage. The amount of revenue lost if the server is down for 15 minutes or longer will come from sales data. Indirect costs include the loss of customer goodwill and the cost to recover the goodwill.

THE UNIVERSITY OF JORDAN

Case study 1: Web site

(5) Provide recommendations—Include a list of recommendations to mitigate the risks. The recommendations may reduce the weaknesses. They may also reduce the impact of the threats. For example, you could address a hardware failure threat by recommending hardware redundancy. You could address a lack of updates by implementing an update plan.

(6) Identify the costs of recommendations—Identify and list the cost of each recommendation.

Case study 1: Web site

(7) Provide a cost-benefit analysis (CBA)—Include a CBA for each recommendation. The CBA compares the cost of the recommendation against the benefit to the company of implementing the recommendation. You can express the benefit in terms of income gained or the cost of the outage reduced.

(8) Document accepted recommendations—Management will choose which recommendations to implement. They can accept, defer, or modify recommendations. You can then document these choices in the plan.

THE UNIVERSITY OF JORDAN

Case study 1: Web site

(7) Provide a cost-benefit analysis (CBA)—Include a CBA for each recommendation. The CBA compares the cost of the recommendation against the benefit to the company of implementing the recommendation. You can express the benefit in terms of income gained or the cost of the outage reduced.

(8) Document accepted recommendations—Management will choose which recommendations to implement. They can accept, defer, or modify recommendations. You can then document these choices in the plan.

THE UNIVERSITY OF JORDAN

Scope of the case study: Web Site

• The purpose of the risk management plan is to secure the Acme Widgets Web site. The scope of the plan includes:

• Security of the server hosting the Web site

• Security of the Web site itself

• Availability of the Web site

• Integrity of the Web site's data

- Stakeholders for this project include:

• Vice president of sales

• IT support department head

THE UNIVERSITY OF JORDAN

Describing Procedures and Schedules for Accomplishment

In this project, should create this part of the risk management plan after the project has started. You include a recommended solution for any threat or vulnerability, with a goal of mitigating the associated risk. For example, an existing firewall may expose a server to multiple vulnerabilities. The solution could be to upgrade the firewall. This upgrade can be broken down into several steps, such as:

- Determine what traffic should be allowed.
- Create a firewall policy.
- Purchase a firewall.
- Install the firewall.
- Configure the firewall.
- Test the firewall.
- Implement the firewall.

Describing Procedures and Schedules for Accomplishment

Threats

Attackers
Buffer Overflow Attacks
DoS, DDoS
Syn Flood Attack
Malware

Vulnerabilities

Network

Open Ports on Firewall
No IDS
Loss of Connectivity

Server

No Antivirus Software
Operating System Updates
Unneeded Services Running
Unneeded Protocols Running
Hardware Failure
No Backups

Recommendations

Upgrade Firewall Manage Firewall
Add Network Firewall Add Host Firewall
Add Intrusion Detection System (IDS)
Add Administrator

End

THE UNIVERSITY OF JORDAN