Risk Management: An Overview of Risk Management

Slide 1

Principles of Computer Security, Fifth Edition

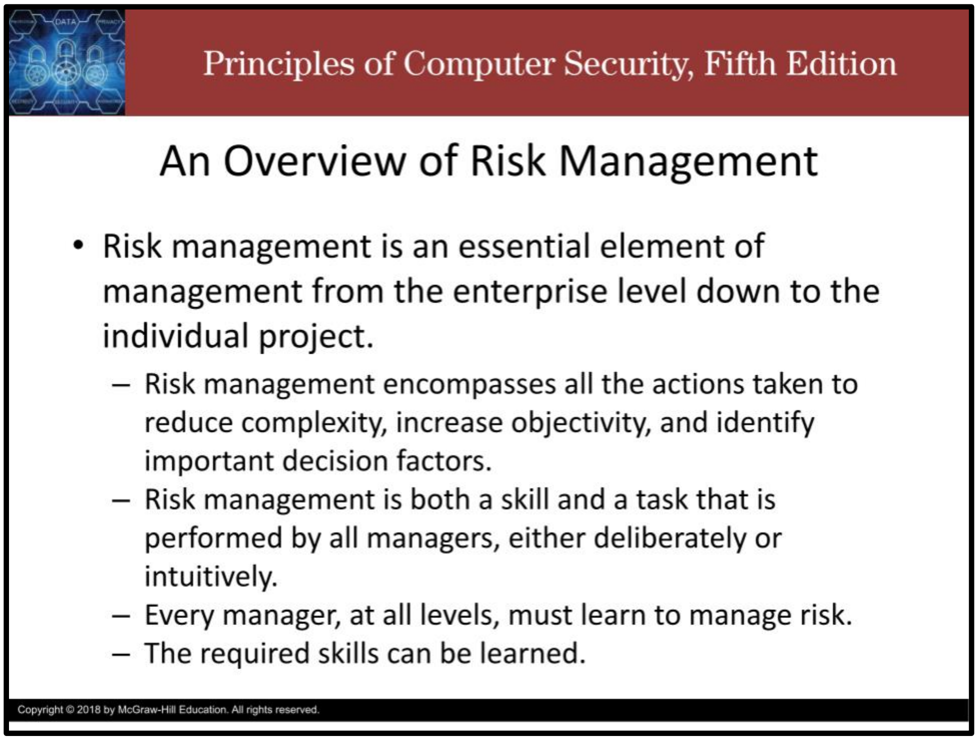
Risk Management

An Overview of Risk Management

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Howdy! In this video, we give an overview of risk management.

Slide 2



Principles of Computer Security, Fifth Edition

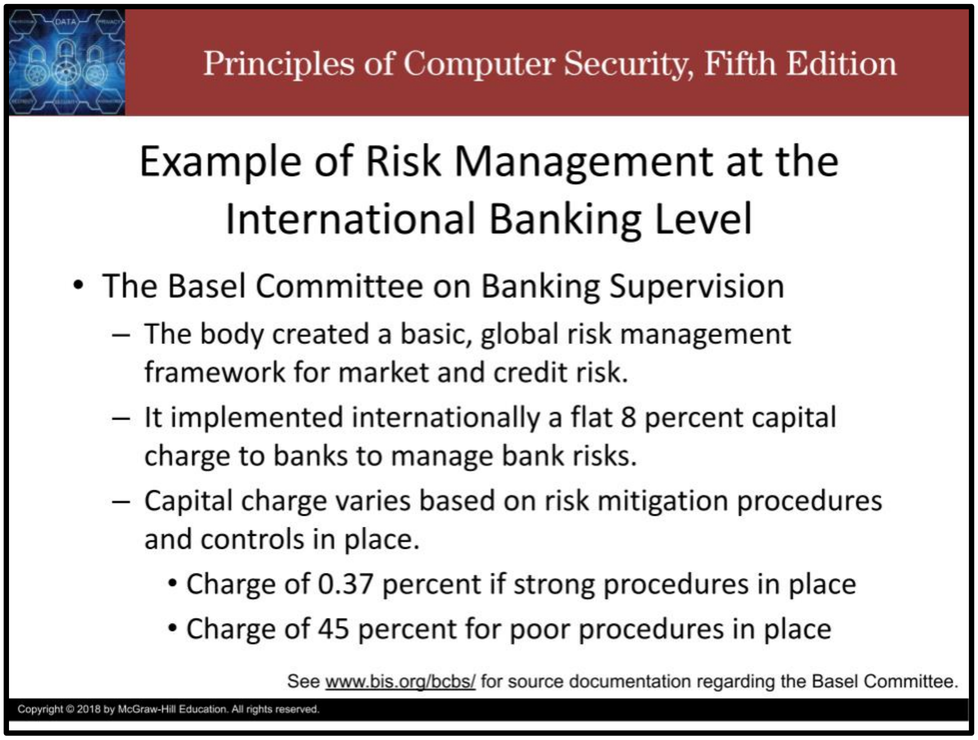
An Overview of Risk Management

- Risk management is an essential element of management from the enterprise level down to the individual project.
  - Risk management encompasses all the actions taken to reduce complexity, increase objectivity, and identify important decision factors.
  - Risk management is both a skill and a task that is performed by all managers, either deliberately or intuitively.
  - Every manager, at all levels, must learn to manage risk.
  - The required skills can be learned.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Risk management is an essential element of management from the enterprise level down to the individual project. It encompasses all the actions taken to reduce complexity, increase objectivity, and identify important decision factors. There has been, and will continue to be, discussion about the complexity of risk management and whether or not it is worth the effort. Businesses must take risks to retain their competitive edge, however, and as a result, risk management must occur as part of managing any business, program, or project. Risk management is both a skill and a task that is performed by all managers, either deliberately or intuitively. It can be simple or complex, depending on the size of the project or business and the amount of risk inherent in an activity. Every manager, at all levels, must learn to manage risk. Like most skills, risk management can be learned.

Slide 3



Principles of Computer Security, Fifth Edition

Example of Risk Management at the International Banking Level

- The Basel Committee on Banking Supervision
  - The body created a basic, global risk management framework for market and credit risk.
  - It implemented internationally a flat 8 percent capital charge to banks to manage bank risks.
  - Capital charge varies based on risk mitigation procedures and controls in place.
    - Charge of 0.37 percent if strong procedures in place
    - Charge of 45 percent for poor procedures in place

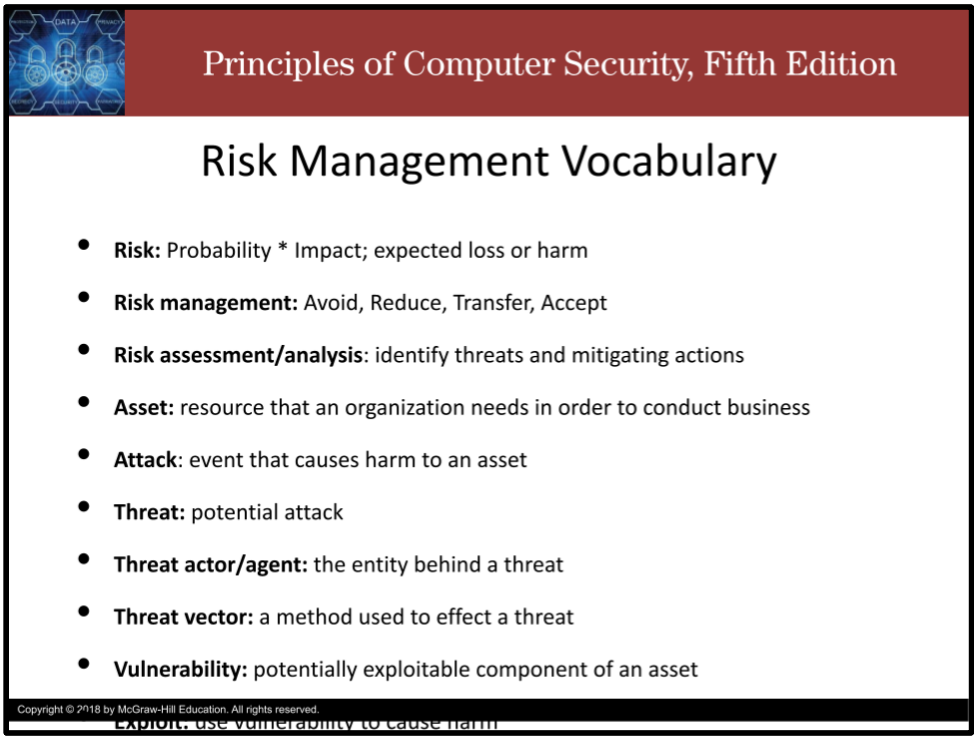
See www.bis.org/bcbs/ for source documentation regarding the Basel Committee.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

The Basel Committee on Banking Supervision comprises government central bank governors from around the world. This body created a basic, global risk management framework for market and credit risk. It implemented internationally a flat 8 percent capital charge to banks to manage bank risks. This means that for every 100 dollars a bank makes in loans, it must possess 8 dollars in reserve to be used in the event of financial difficulties.

However, if banks can show they have very strong risk mitigation procedures and controls in place, that capital charge can be reduced to as low as 0.37 percent (or 37 cents of reserves per 100 dollars of loans). If a bank has poor procedures and controls, that capital charge can be as high as 45 percent, or 45 dollars for every 100 dollars the bank loans out. This example shows how risk management can be used at a very high level. The remainder of this module focuses on smaller implementations and demonstrates how risk management is used in many aspects of business conduct.

Slide 4



Principles of Computer Security, Fifth Edition

Risk Management Vocabulary

- **Risk:** Probability * Impact; expected loss or harm
- **Risk management:** Avoid, Reduce, Transfer, Accept
- **Risk assessment/analysis**: identify threats and mitigating actions
- **Asset:** resource that an organization needs in order to conduct business
- **Attack**: event that causes harm to an asset
- **Threat:** potential attack
- **Threat actor/agent:** the entity behind a threat
- **Threat vector:** a method used to effect a threat
- **Vulnerability:** potentially exploitable component of an asset
- **Exploit:** use vulnerability to cause harm

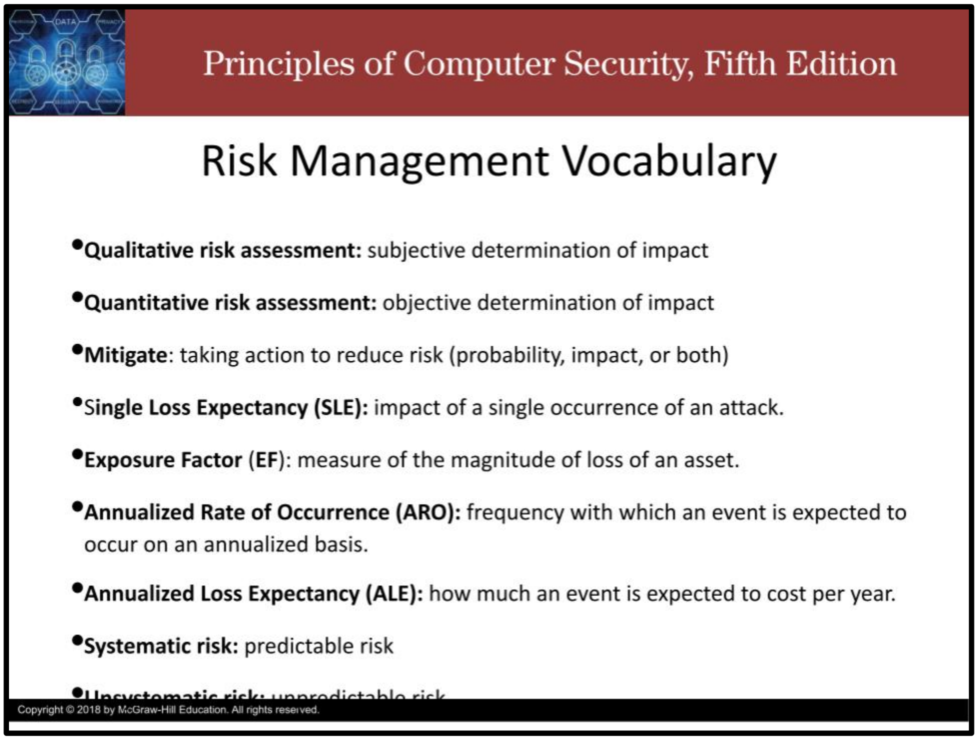
Copyright © 2018 by McGraw-Hill Education. All rights reserved.

You need to understand a number of key terms to manage risk successfully. This vocabulary functions as an overview of risk management topics. Risk is a product of probability and impact (e.g. loss, harm, damage, etc.) Risk is like the expected loss or harm due to a threat..

Risk management is the overall decision-making process of Identifying threats and vulnerabilities and their potential impacts, Determining the costs to mitigate such events, and Deciding what actions are cost effective for controlling these risks.

Risk assessment (or risk analysis) is the process of analyzing an environment to identify the threats and mitigating actions to determine the impact of an event that would affect a project, program, or business. An asset is any resource or information that an organization needs in order to conduct its business. An attack is an event that causes harm to an asset. A threat is any circumstance or event with the potential to cause harm to an asset. A threat actor/agent is the entity behind a threat. A threat vector is a method used to effect a threat. A vulnerability is any characteristic or component of an asset that can be exploited by a threat to cause harm. An exploit takes advantage of a vulnerability. Impact is the loss or harm incurred when a threat exploits a vulnerability. A control is a measure taken to detect, prevent, or mitigate the risk associated with a threat.

Slide 5



Principles of Computer Security, Fifth Edition

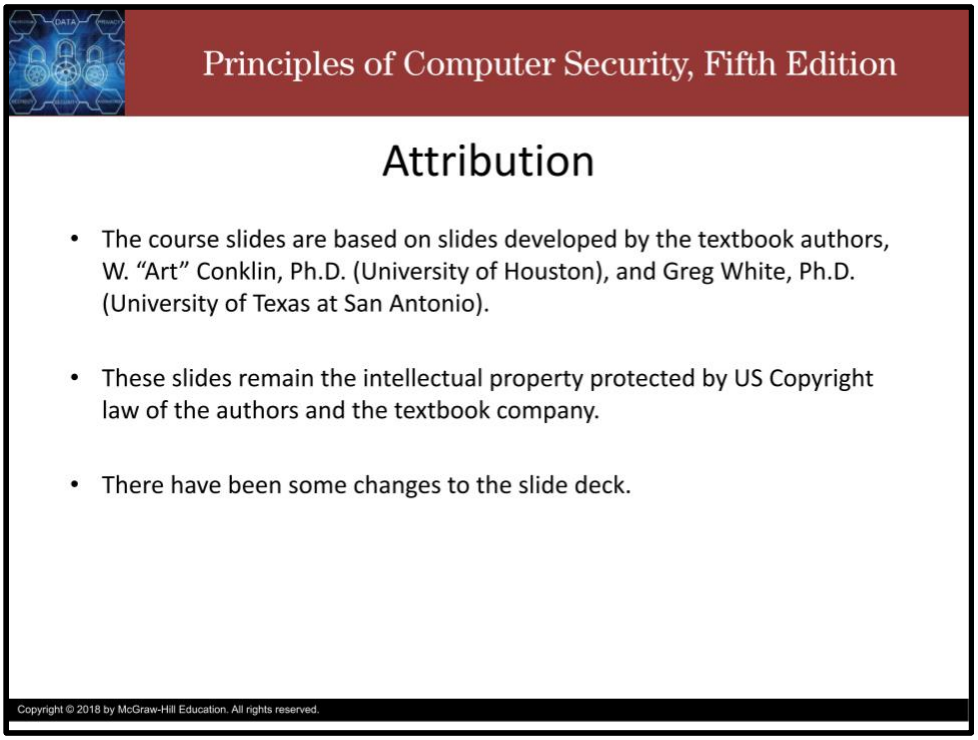
Risk Management Vocabulary

- **Qualitative risk assessment:** subjective determination of impact
- **Quantitative risk assessment:** objective determination of impact
- **Mitigate**: taking action to reduce risk (probability, impact, or both)
- **Single Loss Expectancy (SLE):** impact of a single occurrence of an attack.
- **Exposure Factor** (**EF**): measure of the magnitude of loss of an asset.
- **Annualized Rate of Occurrence (ARO):** frequency with which an event is expected to occur on an annualized basis.
- **Annualized Loss Expectancy (ALE):** how much an event is expected to cost per year.
- **Systematic risk:** predictable risk
- **Unsystematic risk:** unpredictable risk

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Qualitative risk assessment is the process of subjectively determining the impact of an attack. Qualitative means statements like: “It would feel bad.” **Quantitative risk assessment** is the process of objectively determining the impact of an attack. Quantitative means numbers and units like: “It would cost 1 million dollars.” The term **mitigate** refers to taking action to reduce the likelihood of a threat occurring or to reduce the impact if a threat does occur, or both. The **single loss expectancy** is the monetary loss or impact of each occurrence of a threat exploiting a vulnerability. **Exposure factor** is a measure of the magnitude of loss of an asset. It is used in the calculation of single loss expectancy. The **annualized rate of occurrence** is the frequency with which an event (or attack) is expected to occur on an annualized basis. The **annualized loss expectancy** is how much an event (or attack) is expected to cost per year. **Systematic risk** is risk that is predictable under relatively stable circumstances. The probability component of a systematic risk is known with low uncertainty. **Unsystematic risk** is risk that is unpredictable in the aggregate because it results from forces difficult to predict. The probability component of the risk has high uncertainty. A **hazard** is a circumstance that increases the probability or impact of a loss.

Slide 6



Principles of Computer Security, Fifth Edition

Attribution

- The course slides are based on slides developed by the textbook authors, W. “Art” Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.
- There have been some changes to the slide deck.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Thank you and take care.

Risk Management: What is Risk Management

Slide 1

Principles of Computer Security, Fifth Edition

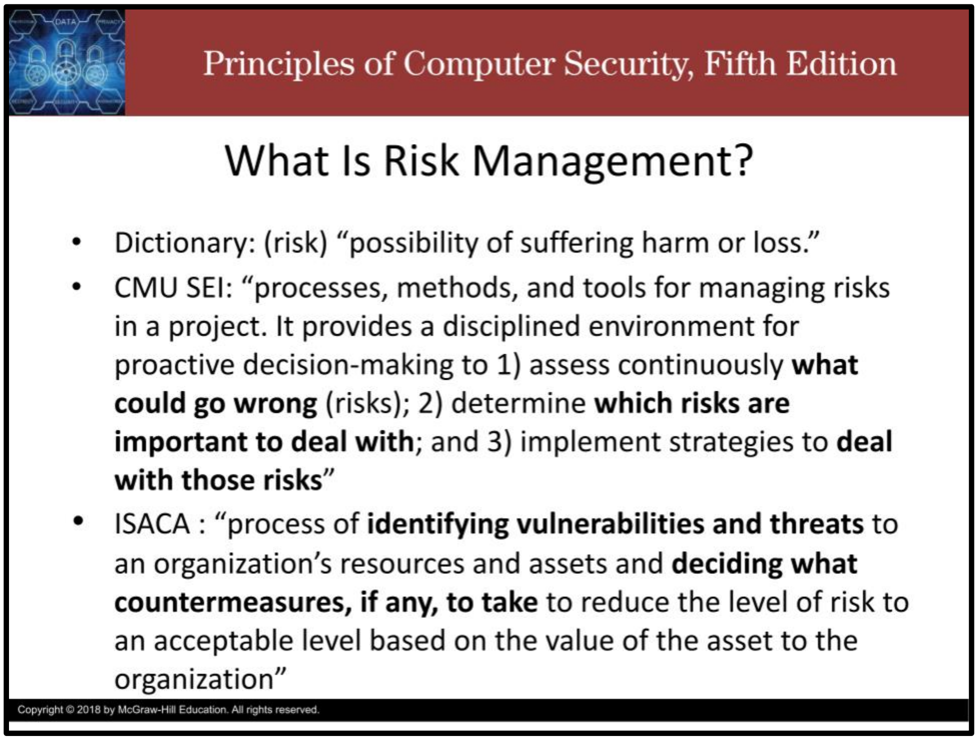
Risk Management

What is Risk Management

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Howdy! In this video we continue our discussion of risk management.

Slide 2



Principles of Computer Security, Fifth Edition

What Is Risk Management?

- Dictionary: (risk) “possibility of suffering harm or loss.”
- CMU SEI: “processes, methods, and tools for managing risks in a project. It provides a disciplined environment for proactive decision-making to 1) assess continuously **what could go wrong** (risks); 2) determine **which risks are important to deal with**; and 3) implement strategies to **deal with those risks**”
- ISACA : “process of **identifying vulnerabilities and threats** to an organization’s resources and assets and **deciding what countermeasures, if any, to take** to reduce the level of risk to an acceptable level based on the value of the asset to the organization”

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

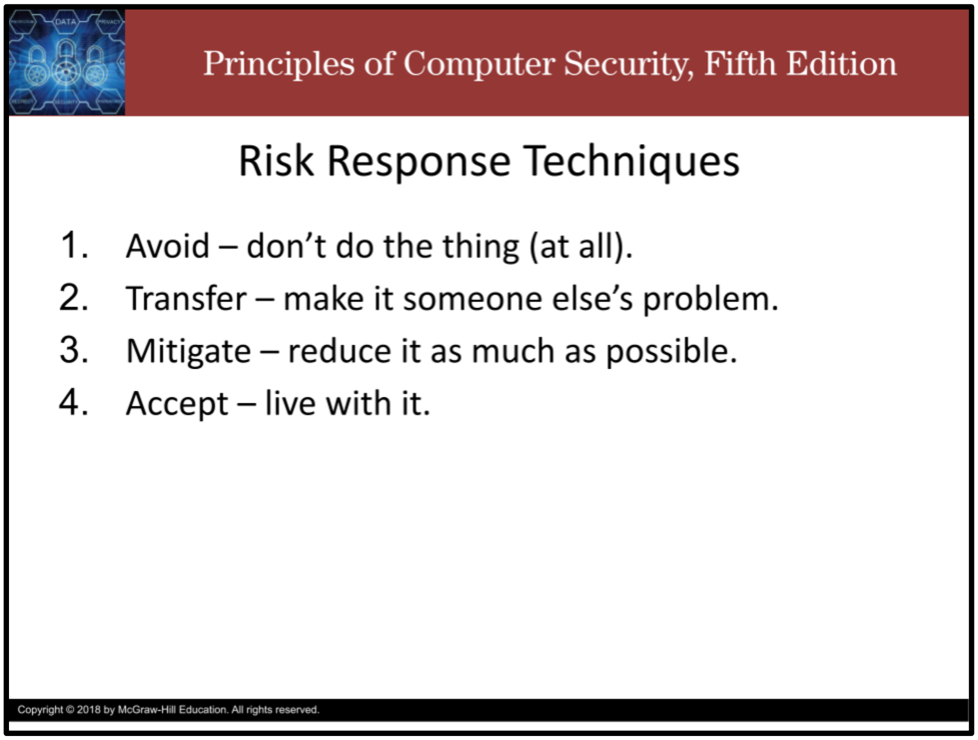
Three definitions relating to risk management reveal why it is sometimes considered difficult to understand:

The dictionary defines risk as the possibility of suffering harm or loss. Carnegie Mellon University’s Software Engineering Institute defines continuous risk management as “processes, methods, and tools for managing risks in a project. It provides a disciplined environment for proactive decision-making to 1) assess continuously what could go wrong (risks); 2) determine which risks are important to deal with; and 3) implement strategies to deal with those risks.”

The Information Systems Audit and Control Association says, “In modern business terms, risk management is the process of identifying vulnerabilities and threats to an organization’s resources and assets and deciding what countermeasures, if any, to take to reduce the level of risk to an acceptable level based on the value of the asset to the organization.”

So, risk management is based on what can go wrong and what action should be taken to deal with it.

Slide 3



Principles of Computer Security, Fifth Edition

Risk Response Techniques

1. Avoid – don't do the thing (at all).
2. Transfer – make it someone else's problem.
3. Mitigate – reduce it as much as possible.
4. Accept – live with it.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Risk is an absolute in that, in general, it cannot be completely eliminated. It can, however, be dealt with. It must be dealt with. There are 3 ways to deal with risk and we go from the top down, doing all 3 things, at least, trying to, until the end. The 4th thing is forced, as you will see.

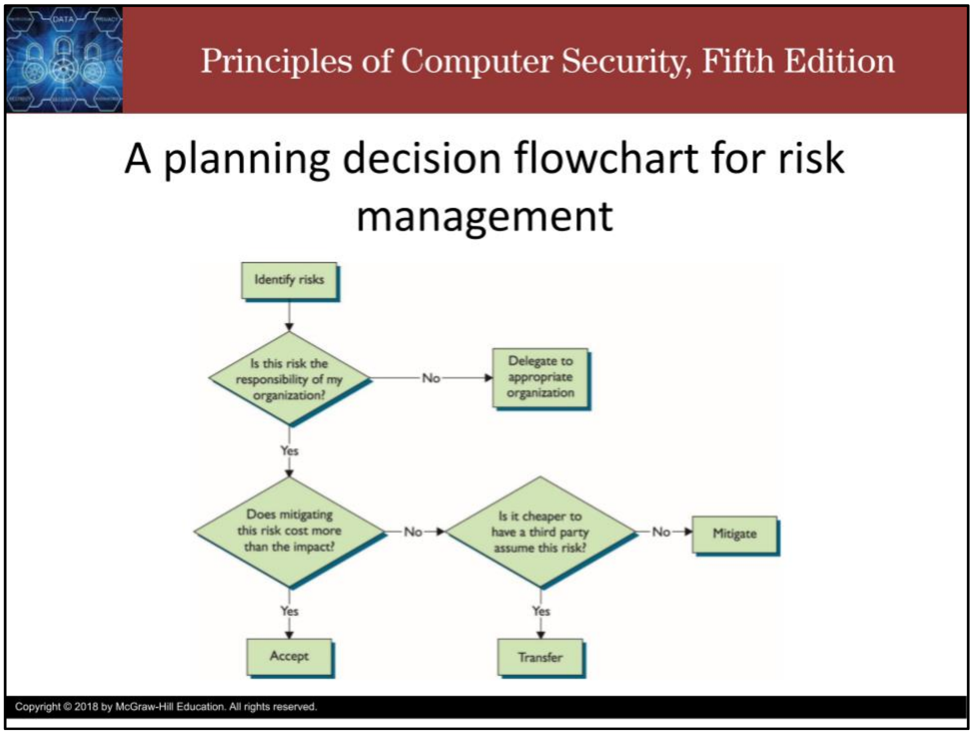
The first thing we try to do is to avoid the risk entirely. This is about as close as we can get to eliminating risk. You can avoid the risk of going sky diving and your parachute not opening by simply not going sky diving. Risk avoided.

The next thing we try to do is to transfer the risk to someone else. Insurance is good example of this. Take health insurance for example. There is a risk that you will get sick or injured and incur medical expenses. In the US, those costs could bankrupt you and your family even unto the 7th generation. So, instead of bearing that risk yourself, you pay someone else to bear it for you. If you get sick or injured and you have medical bills, your health insurance is supposed to cover the costs. Unfortunately, you can't buy health insurance that lets you transfer the physical effects of sickness or injury. Some kinds of risks cannot be avoided or transferred.

After you've avoided all the risk that you can, and then transferred as much as you can, the next step is to mitigate as much of it as you can. Ideally, you would mitigate it into the ground, all the way to 0. But that's usually impossible. There will always be some latent risk. There's also a law of diminishing returns, the more risk you mitigate, the harder and more expensive it is to mitigate more. Getting to 90% mitigation may be the best you can do with your resources. You need to balance the cost of the mitigation with the benefit (the amount of risk reduction).

Finally, after avoiding, transferring, and mitigating all of the risk that you can (or want to), the remaining risk is simply accepted. You have to live with it. This is what is meant when we say the risk is reduced to an acceptable level. Once you are willing to accept the remaining risk, you can stop. Until then, you keep working and iterating to avoid, transfer, and mitigate the risk down to an acceptable level. If you can't get the risk down to an acceptable level, you either avoid it entirely by not doing the thing at all or the risk is force accepted. You are coerced, compelled, required, obligated to bear the risk.

Slide 4



Principles of Computer Security, Fifth Edition

A planning decision flowchart for risk management

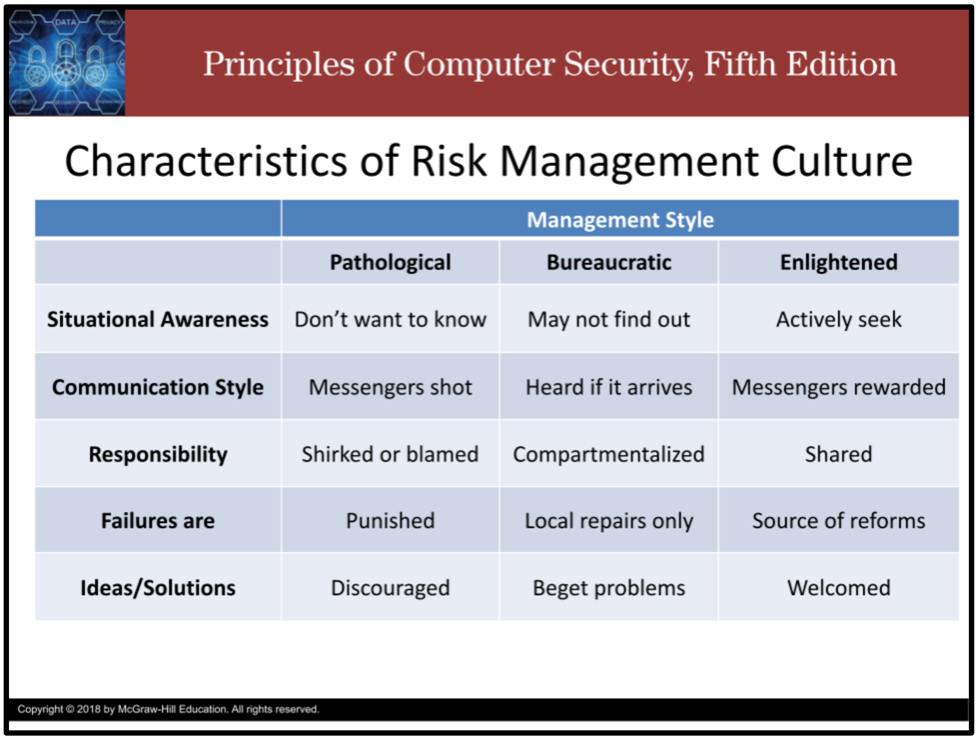
Identify risks
Is this risk the responsibility of my organization?
No
Delegate to appropriate organization
Yes
Does mitigating this risk cost more than the impact?
No
Is it cheaper to have a third party assume this risk?
No
Mitigate
Yes
Accept
Yes
Transfer

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

This flowchart shows an example decision process for risk management. Once risks have been identified, this process has the user trying to take a hard pass on the risk. This is not the same as avoidance. This is more like a complete transfer. An abdication of risk. If the other party agrees to take responsibility for the risk, great. Otherwise, we need to continue working.

Next is a cost/benefit analysis. If the risk is minor enough that it would be more expensive to pay someone to bear it or reduce it, then it can be an easy decision to accept the risk right there. Otherwise, if the magnitude of the risk is too great to bear, then another cost/benefit analysis. We check whether it is cheaper to buy insurance or to make the fixes required to reduce the risk and then act accordingly.

Slide 5



Principles of Computer Security, Fifth Edition

Characteristics of Risk Management Culture

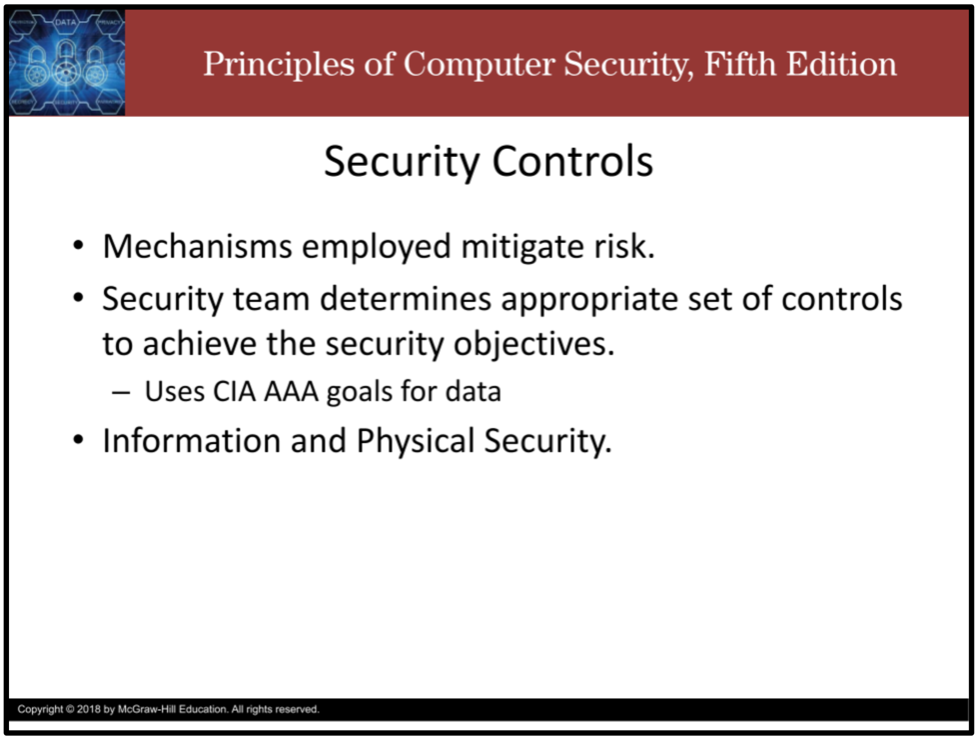
	Management Style		
	Pathological	**Bureaucratic**	**Enlightened**
Situational Awareness	Don’t want to know	May not find out	Actively seek
Communication Style	Messengers shot	Heard if it arrives	Messengers rewarded
Responsibility	Shirked or blamed	Compartmentalized	Shared
Failures are	Punished	Local repairs only	Source of reforms
Ideas/Solutions	Discouraged	Beget problems	Welcomed

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Organizations have a culture associated with their operation. Frequently, this culture is set and driven by the activities of senior management personnel. The risk management culture of an organization can have an effect upon actions being taken by others.

This table captures the symptoms of various management styles with respect to risk management culture. Ideally, management would be enlightened down the board. More likely is some mix of styles, or a borderline style.

Slide 6



Principles of Computer Security, Fifth Edition

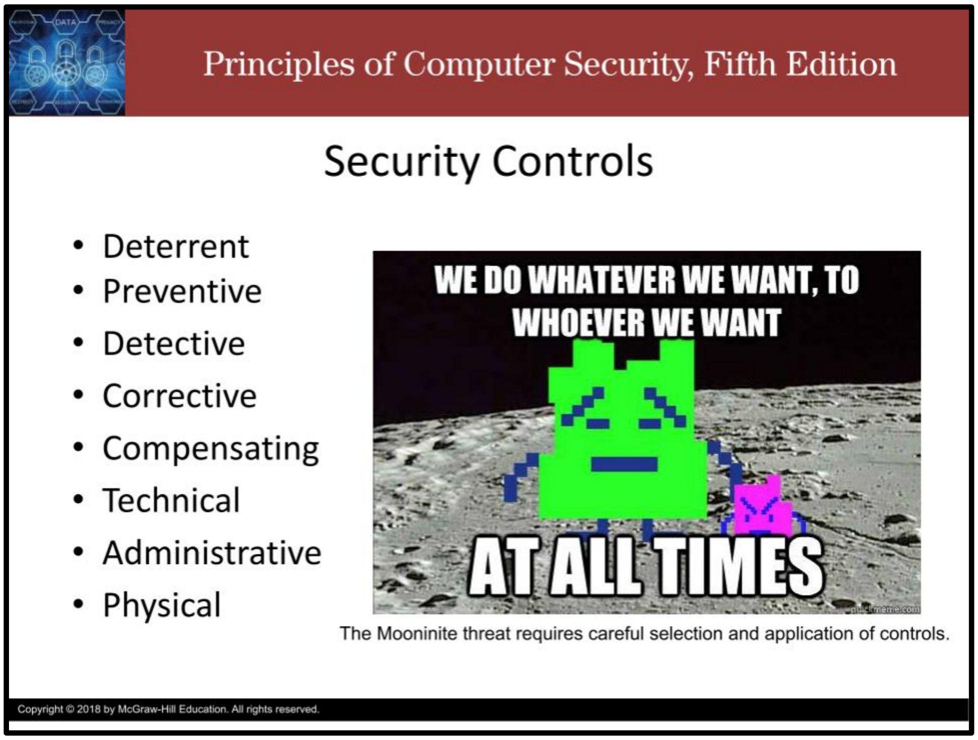
Security Controls

- Mechanisms employed mitigate risk.
- Security team determines appropriate set of controls to achieve the security objectives.
  - Uses CIA AAA goals for data
- Information and Physical Security.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Security controls are the mechanisms employed to minimize exposure to risk and mitigate the effects of loss. The security team must determine the appropriate set of controls to achieve the security objectives by using the security goals associated with the data. Proper application of controls assists in the risk management associated with both information security and physical security.

Slide 7



Principles of Computer Security, Fifth Edition

Security Controls

- Deterrent
- Preventive
- Detective
- Corrective
- Compensating
- Technical
- Administrative
- Physical

WE DO WHATEVER WE WANT, TO WHOEVER WE WANT
AT ALL TIMES
quickmeme.com

The Mooninite threat requires careful selection and application of controls.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Controls come in various types. The different types are not mutually exclusive. A control can belong to more than one type.

A **deterrent** acts to influence the would-be attacker by reducing the likelihood of an attack. In order to be effective, the attacker must believe that the deterrent exists and is effective. For example, putting up security cameras can be a deterrent. But, if the attacker doesn't see them, or if the attacker knows they are fake or not recording, then they are not a deterrent. Also, if the attacker is willing to accept the risk of the deterrent, the deterrent will not be effective.

A **preventative** control is one that prevents specific actions from occurring. A deterrent is a preventative control that acts on the mind. Other preventative controls act on the body (or extensions of it… never mind that the mind may be such an extension; this is not a philosophy class). For example, the a firewall that blocks traffic to port 80 is a preventative control. Preventative controls can still be effective even if the attacker does not know about them.

A **detective** control is one that facilitates the detection of a security breach. Detective controls act during an attack, alerting operators to specific conditions. An alarm is an example of a detective control.

A **corrective** control is one which is used to limit or reverse the damage from an attack. Backups are a good example of a corrective control.

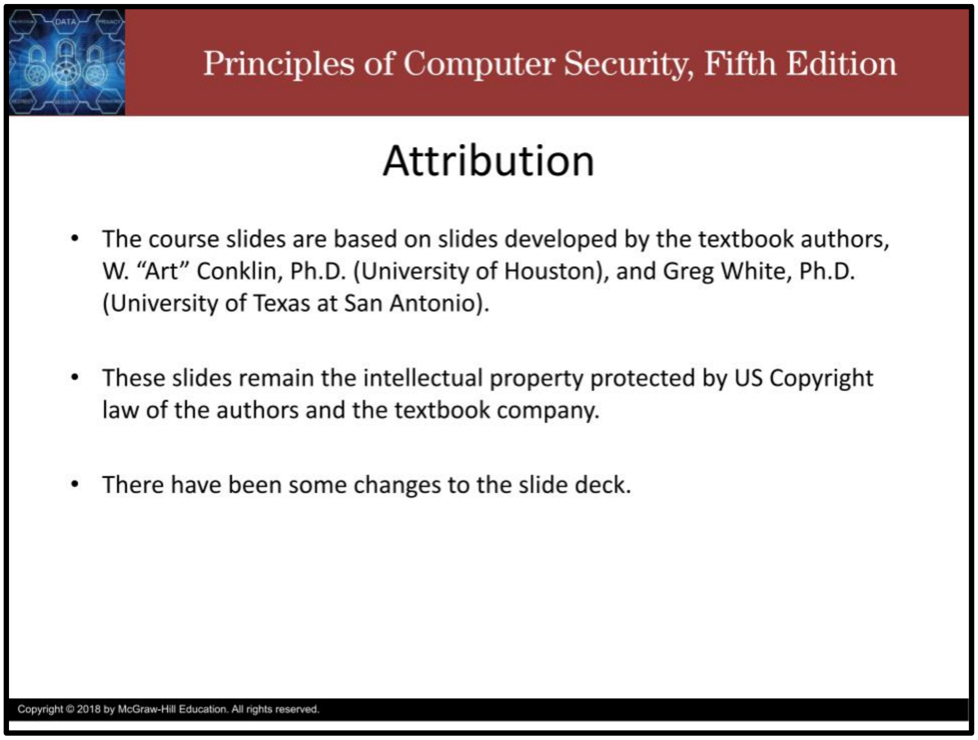
A **compensating** control is one that is used to meet a requirement which cannot be directly satisfied. For example, fire suppressions systems do not prevent fire from happening, but they do limit the amount of damage that a fire can cause.

A **technical** control is one which uses technology that is not purely physical. Biometrics is a good example. Biometrics have a physical component, but their implementation is technical, computational, even.

An **administrative** control is a policy or procedure intended to mitigate risk. A password policy is an administrative control which can be supported with technical controls like a domain controller.

A **physical** control is a preventative control for physical actions. A lock is an example of a physical control, as is a door.

Slide 8



Principles of Computer Security, Fifth Edition

Attribution

- The course slides are based on slides developed by the textbook authors, W. “Art” Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.
- There have been some changes to the slide deck.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Thank you and take care.

Risk Management: Business Risk

Slide 1

Principles of Computer Security, Fifth Edition

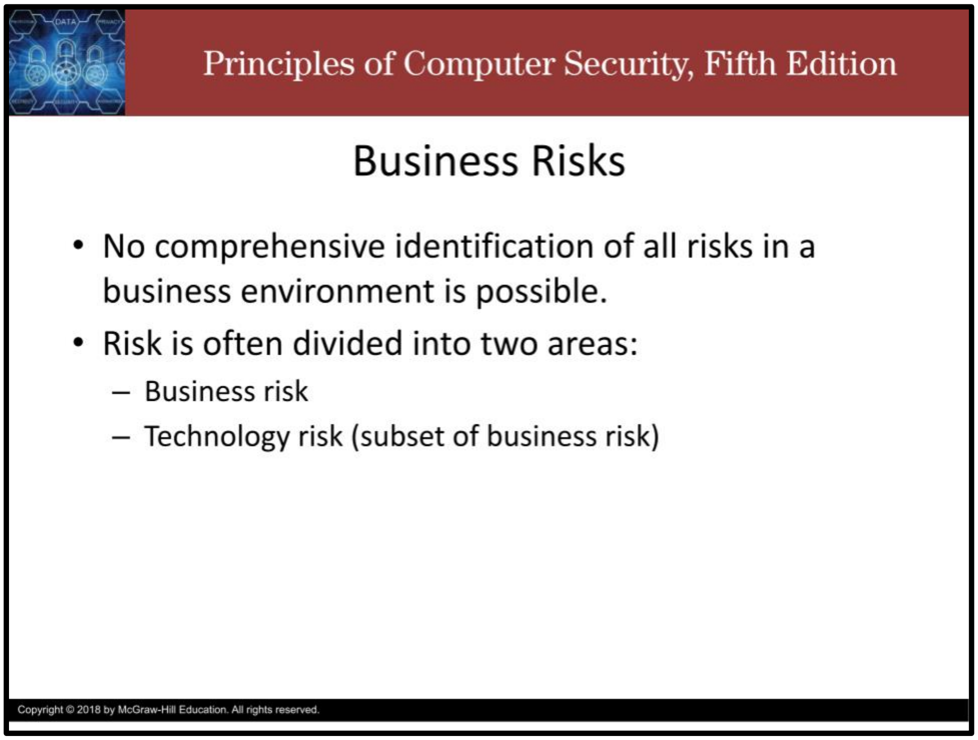
Risk Management

Business Risk

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Howdy! In this video, we discuss business risks.

Slide 2



Principles of Computer Security, Fifth Edition

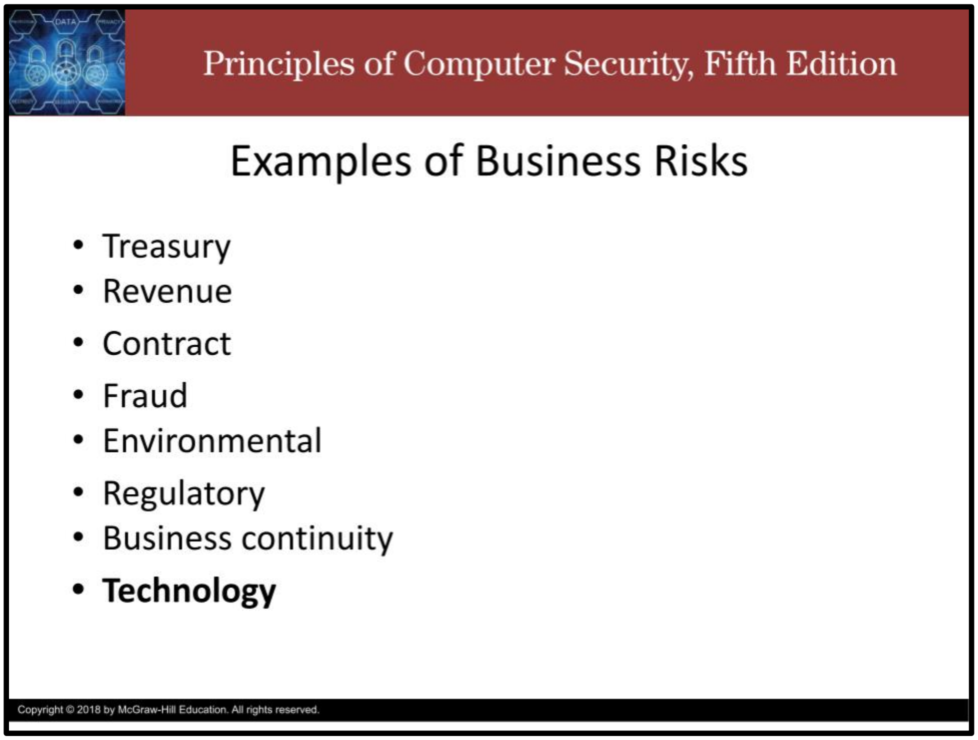
Business Risks

- No comprehensive identification of all risks in a business environment is possible.
- Risk is often divided into two areas:
  - Business risk
  - Technology risk (subset of business risk)

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

A comprehensive identification of all risks in a business environment is impossible. In today's technology-dependent business environment, risk is often simplistically divided into two areas: Business risk and Technology risk (which is a subset of business risk).

Slide 3



Principles of Computer Security, Fifth Edition

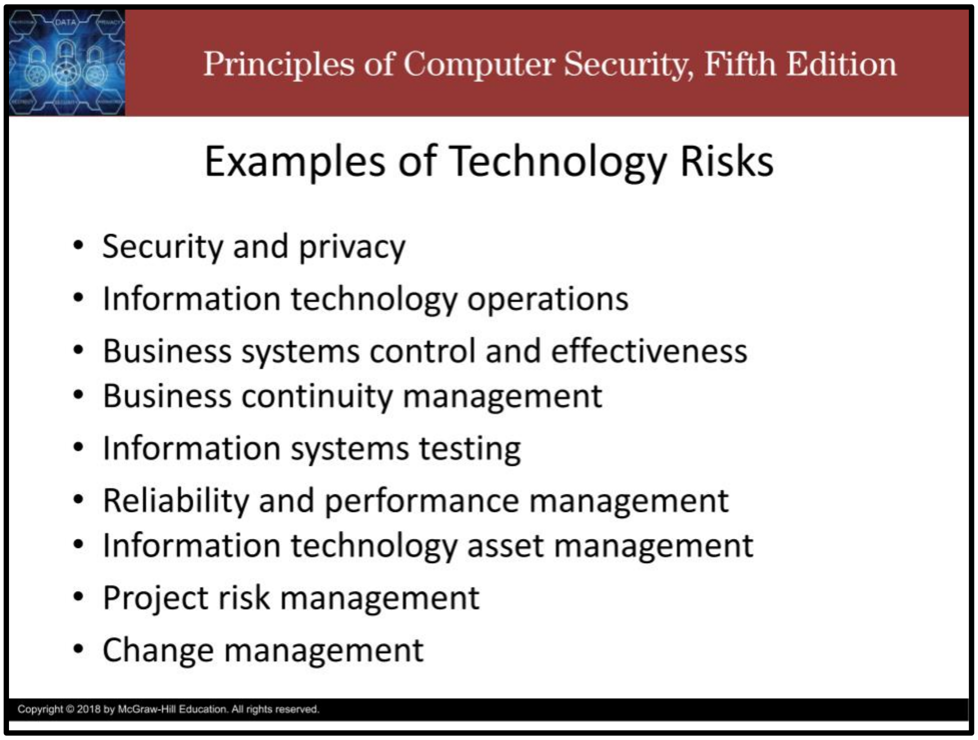
Examples of Business Risks

- Treasury
- Revenue
- Contract
- Fraud
- Environmental
- Regulatory
- Business continuity
- **Technology**

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Some of the most common examples of business risk are listed here. Treasury risk relates to company holdings in bonds, futures, currencies, and so on. Revenue risk relates to consumer behavior and the generation of revenue. Contract risk involves contracts with customers, vendors, partners, and so on. The risk of fraud deals with deliberate deception made for personal gain, to obtain property or services, and so on. Environmental risks are those associated with factors that affect the environment. Regulatory risks are those arising from new or existing regulations. Business continuity risks are associated with recovering and restoring business functions after a disaster or major disruption occurs. Technology risks are associated with technology in its many forms. Technology is so important that these risks should be considered separately.

Slide 4



Principles of Computer Security, Fifth Edition

Examples of Technology Risks

- Security and privacy
- Information technology operations
- Business systems control and effectiveness
- Business continuity management
- Information systems testing
- Reliability and performance management
- Information technology asset management
- Project risk management
- Change management

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Some of the most common technology risks are listed here.

Security and privacy risks are associated with protecting personal, private, or confidential information

Information technology operations has risks associated with the day-to-day operation of information technology systems

Business systems control and effectiveness risks are associated with manual and automated controls that safeguard company assets and resources

Business continuity technology risks are associated with the technology and processes to be used in the event of a disaster or major disruption

Information systems testing has risks associated with testing processes and procedures of information systems

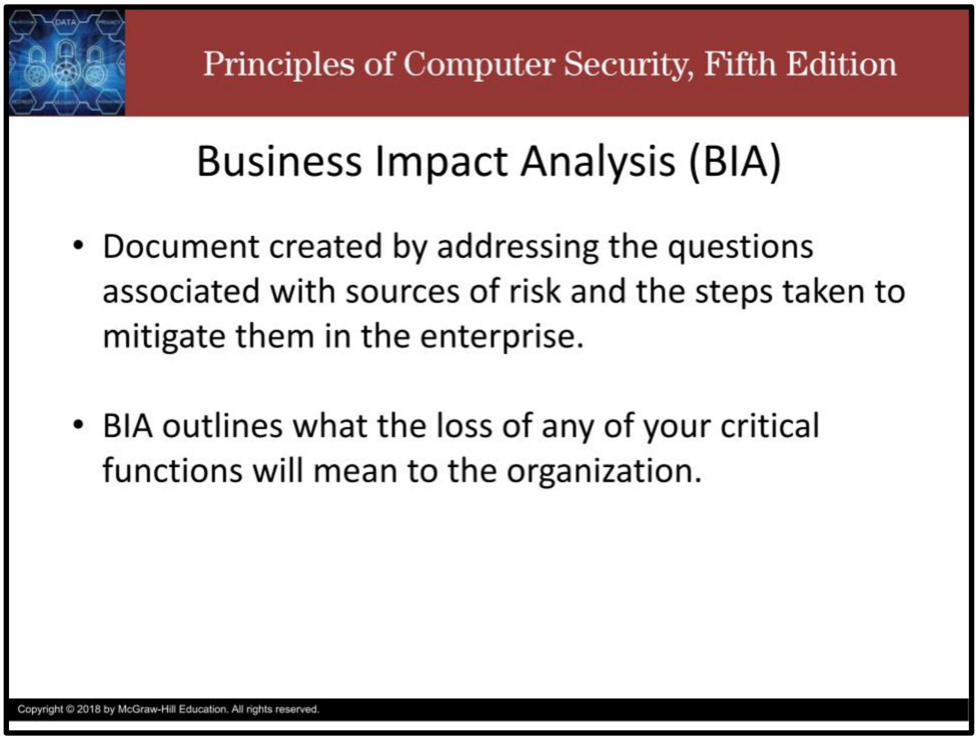
Reliability and performance management deals with risks associated with meeting reliability and performance agreements and measures

Information technology asset management deals with risks associated with safeguarding information technology physical assets

Project risk management deals with the risks associated with managing information technology projects

Change management deals with the risks associated with managing configurations and changes

Slide 5



Principles of Computer Security, Fifth Edition

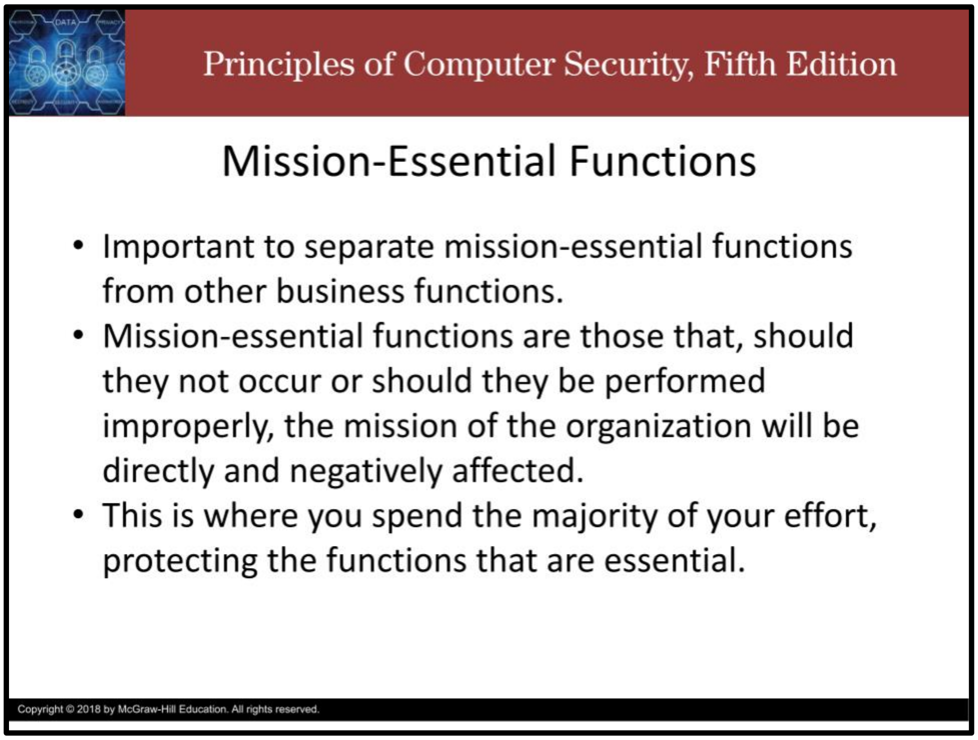
Business Impact Analysis (BIA)

- Document created by addressing the questions associated with sources of risk and the steps taken to mitigate them in the enterprise.
- BIA outlines what the loss of any of your critical functions will mean to the organization.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

A business impact analysis is a document created by addressing questions associated with sources of risk and the steps taken to mitigate them in the enterprise. The BIA outlines what the loss of any of your critical functions will mean to the organization.

Slide 6



Principles of Computer Security, Fifth Edition

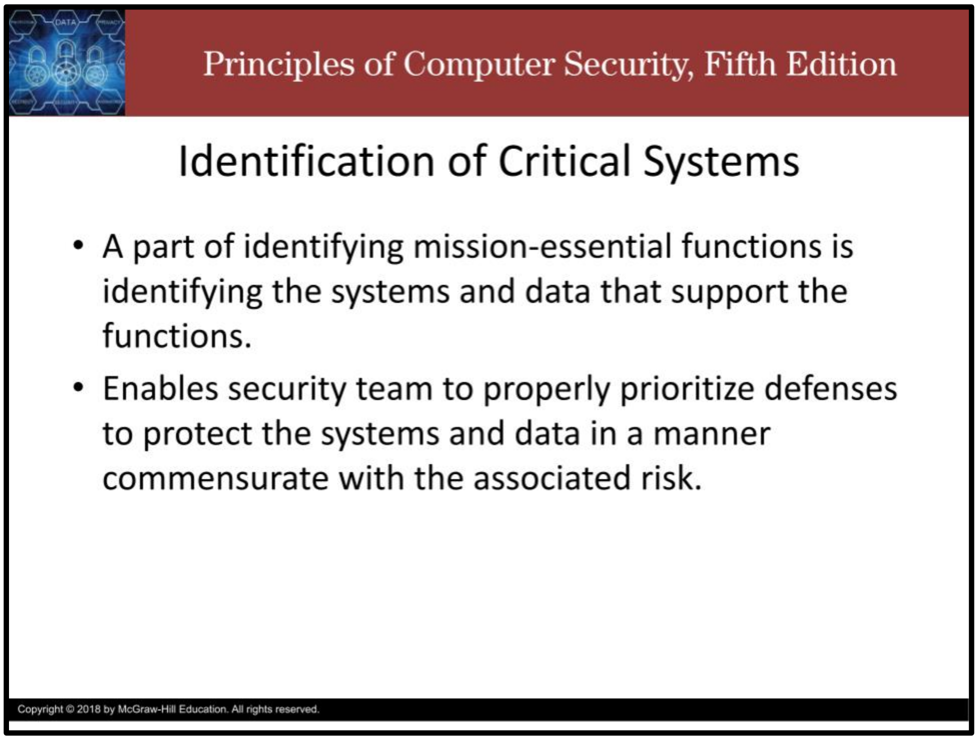
Mission-Essential Functions

- Important to separate mission-essential functions from other business functions.
- Mission-essential functions are those that, should they not occur or should they be performed improperly, the mission of the organization will be directly and negatively affected.
- This is where you spend the majority of your effort, protecting the functions that are essential.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

It is important to separate mission-essential functions from other business functions. Mission-essential functions are those that directly affect the mission of the organization. The reason that identifying these functions is vital for risk management is simple: this is where you spend the majority of your effort, protecting the functions that are essential.

Slide 7



Principles of Computer Security, Fifth Edition

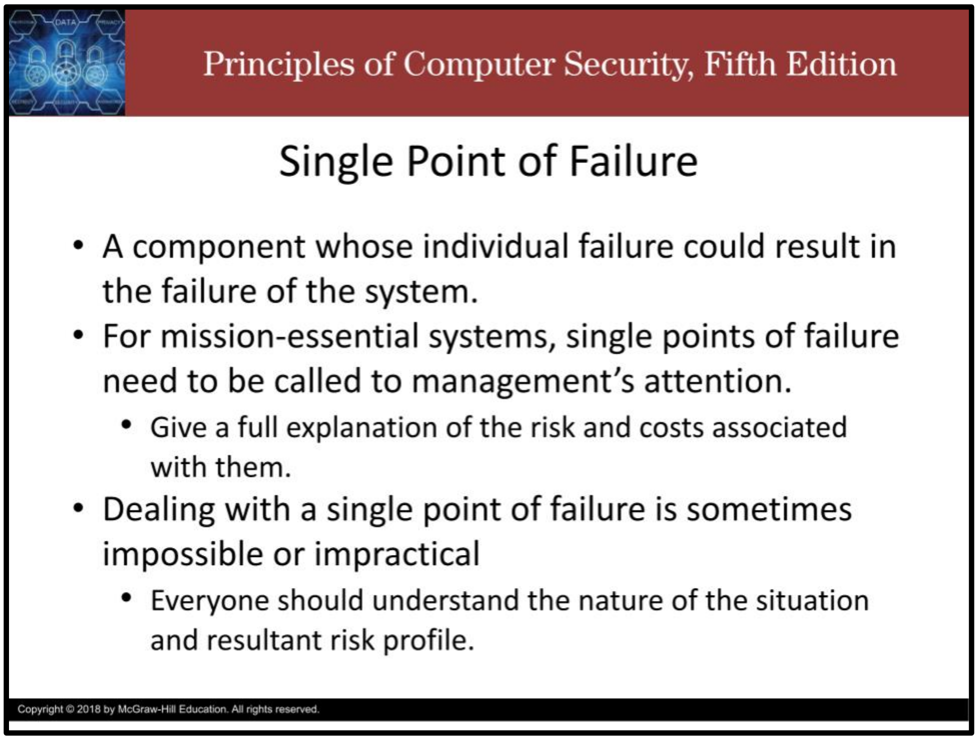
Identification of Critical Systems

- A part of identifying mission-essential functions is identifying the systems and data that support the functions.
- Enables security team to properly prioritize defenses to protect the systems and data in a manner commensurate with the associated risk.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Part of identifying mission-essential functions is to identify the systems and data that support the functions. This enables the security team to properly prioritize defenses to protect the systems and data in a manner commensurate with the associated risk.

Slide 8



Principles of Computer Security, Fifth Edition

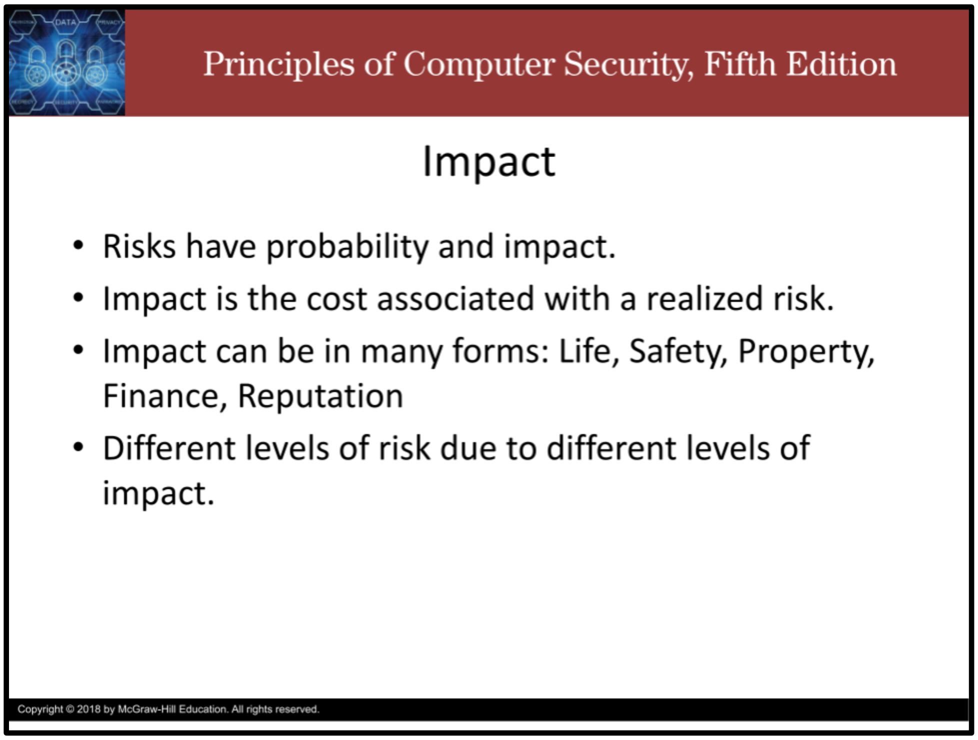
Single Point of Failure

- A component whose individual failure could result in the failure of the system.
- For mission-essential systems, single points of failure need to be called to management’s attention.
    - Give a full explanation of the risk and costs associated with them.
- Dealing with a single point of failure is sometimes impossible or impractical
    - Everyone should understand the nature of the situation and resultant risk profile.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

A single point of failure is any aspect that if triggered could, on its own, result in the failure of the system. For mission-essential systems, single points of failure are items that need to be called to management’s attention, with a full explanation of the risk and costs associated with them.
There may be times that dealing with the single point of failure is not possible or practical, but everyone should understand the nature of the situation and resultant risk profile.

Slide 9



Principles of Computer Security, Fifth Edition

Impact

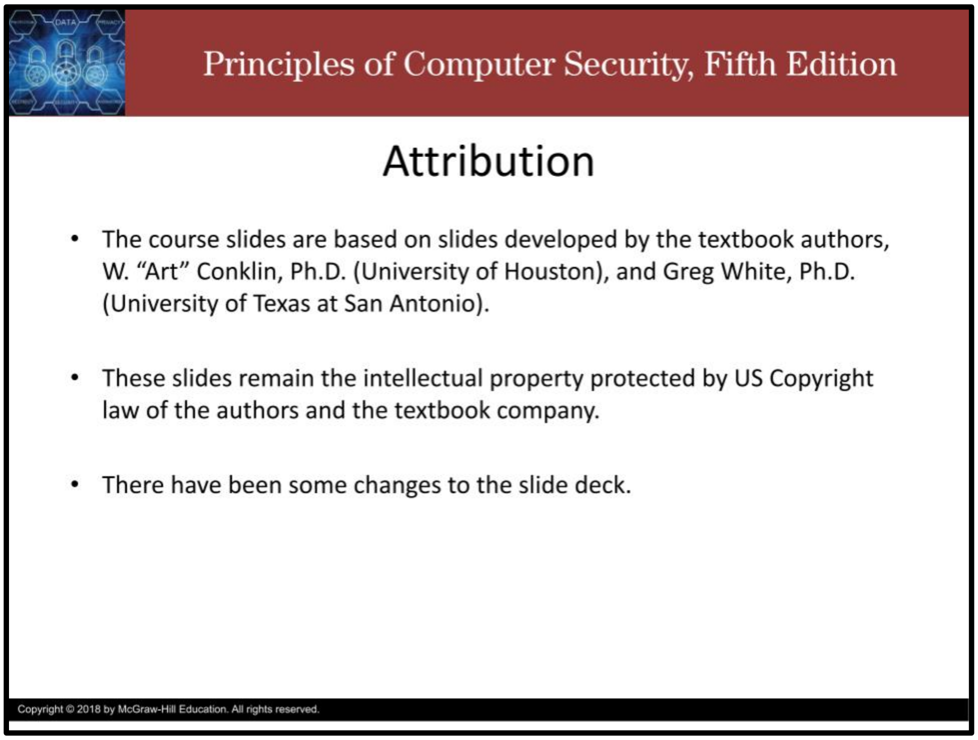
- Risks have probability and impact.
- Impact is the cost associated with a realized risk.
- Impact can be in many forms: Life, Safety, Property, Finance, Reputation
- Different levels of risk due to different levels of impact.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Risk is often stated as a probability and an impact. The probability is the chance that the risk actually happens. The impact is the cost associated with the risk actually happening. Impacts can take many forms, none of which are mutually exclusive:
Life as in injury or death to animals and plants but especially humans, safety as in non-lethal harm to humans, or damage to the environment, property damage such as destruction of assets, or environmental damage, financial loss, or loss of reputation. For many businesses, all types of risks get mapped to a dollar amount. Some risks, like broken equipment have relatively clear dollar-costs. Other risks, especially the existential risks like loss of life or environmental damage are not so easy to map to money.

Different risks can have different levels of impacts. But, a single risk can also have different levels of impact based on how the risk is realized. An oil pipeline leaking has many impacts. The amount of impact and the probability, and therefore the amount of risk, depends on the size of the leak (how fast and how long it leaks). A little leak will cause a little damage. A big leak will cause a lot of damage. The risk of a little leak and the risk of a big leak may be sufficiently different that they deserve separate mitigations.

Slide 10



Principles of Computer Security, Fifth Edition

Attribution

- The course slides are based on slides developed by the textbook authors, W. “Art” Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.
- There have been some changes to the slide deck.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Thank you and take care.

Risk Management: Risk Mitigation Strategies

Slide 1

Principles of Computer Security, Fifth Edition

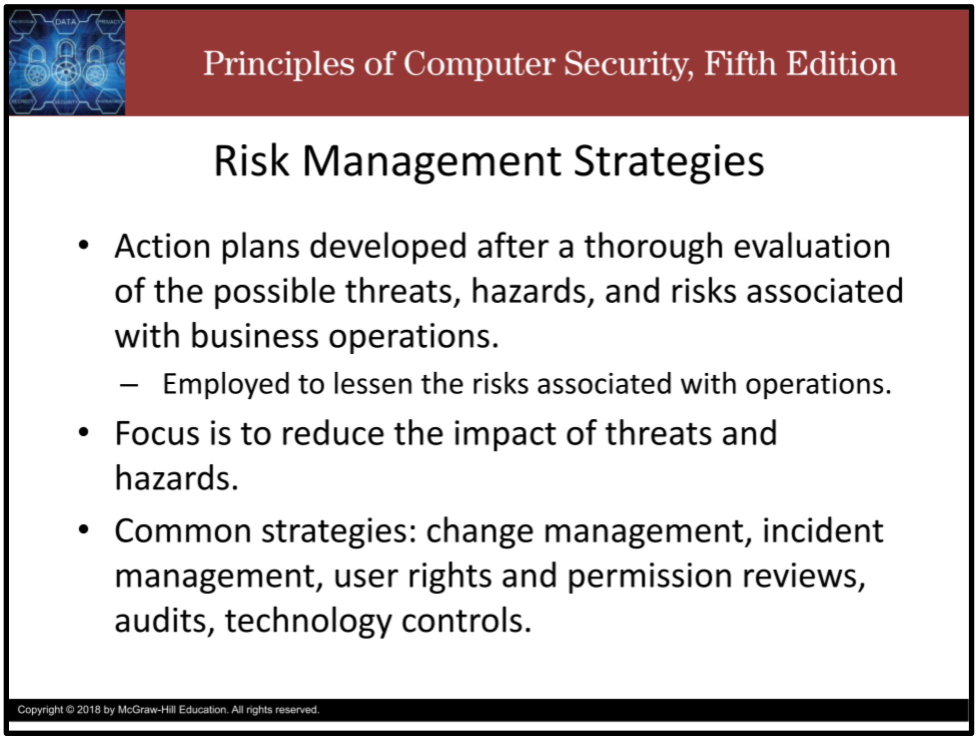
Risk Management

Risk Mitigation Strategies

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Howdy! In this video, we discuss risk management strategies.

Slide 2



Principles of Computer Security, Fifth Edition

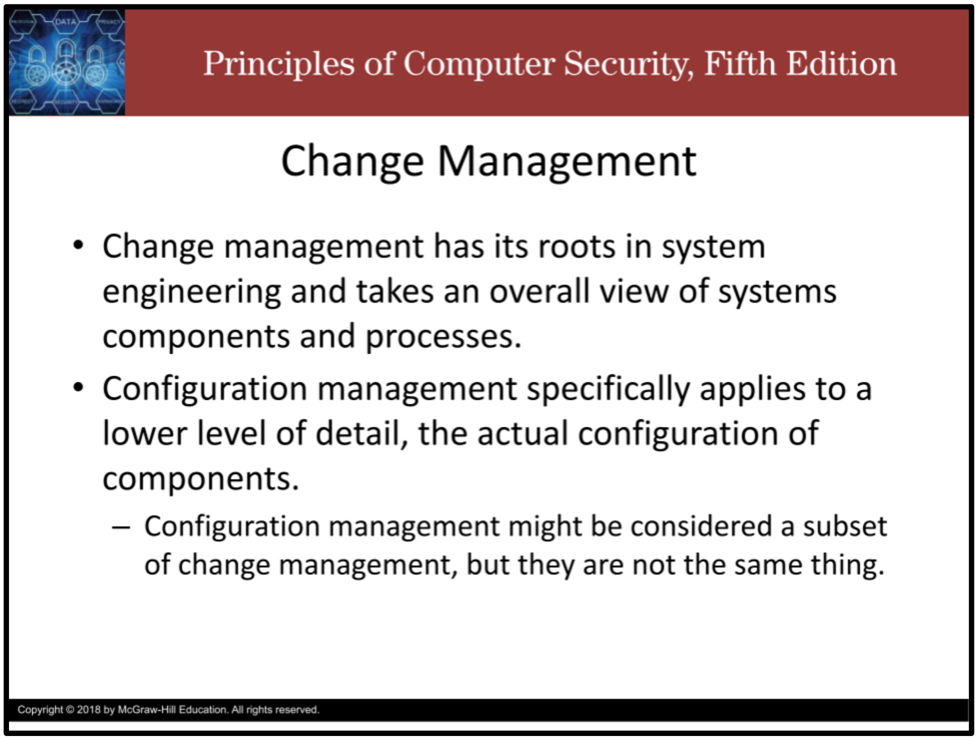
Risk Management Strategies

- Action plans developed after a thorough evaluation of the possible threats, hazards, and risks associated with business operations.
  - Employed to lessen the risks associated with operations.
- Focus is to reduce the impact of threats and hazards.
- Common strategies: change management, incident management, user rights and permission reviews, audits, technology controls.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Risk management strategies are action plans developed after a thorough evaluation of the possible threats, hazards, and risks associated with business operations. These strategies are employed to lessen the risks associated with operations. The focus of risk mitigation strategies is to reduce the impact of threats and hazards. Common risk mitigation strategies include change management, incident management, user rights and permission reviews, audits, technology controls.

Slide 3



Principles of Computer Security, Fifth Edition

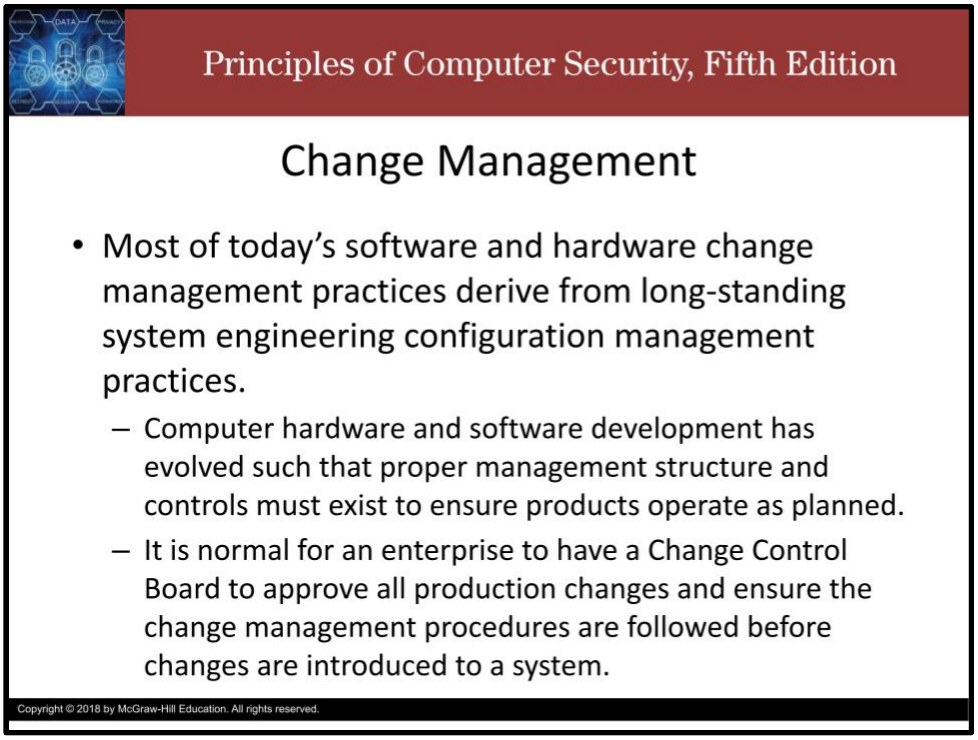
Change Management

- Change management has its roots in system engineering and takes an overall view of systems components and processes.
- Configuration management specifically applies to a lower level of detail, the actual configuration of components.
  - Configuration management might be considered a subset of change management, but they are not the same thing.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Change management has its roots in system engineering and takes an overall view of systems components and processes. Configuration management specifically applies to a lower level of detail, the actual configuration of components. Configuration management might be considered a subset of change management, but they are not the same thing.

Slide 4



Principles of Computer Security, Fifth Edition

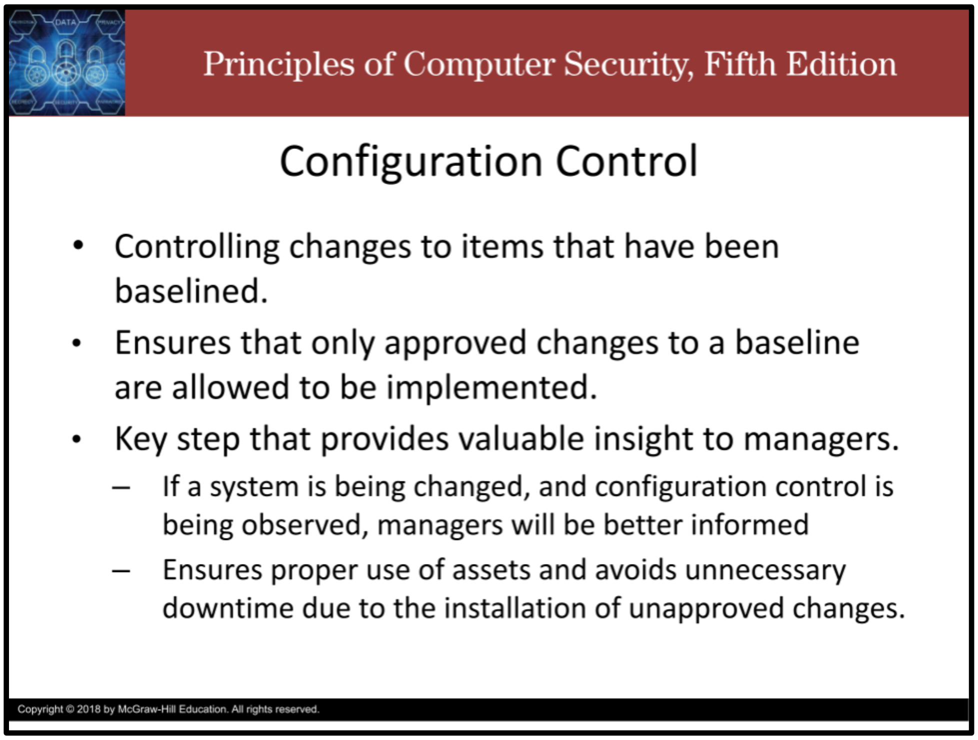
Change Management

- Most of today's software and hardware change management practices derive from long-standing system engineering configuration management practices.
  - Computer hardware and software development has evolved such that proper management structure and controls must exist to ensure products operate as planned.
  - It is normal for an enterprise to have a Change Control Board to approve all production changes and ensure the change management procedures are followed before changes are introduced to a system.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Most of today's software and hardware change management practices derive from long-standing system engineering configuration management practices. Computer hardware and software development has evolved such that proper management structure and controls must exist to ensure products operate as planned. It is normal for an enterprise to have a Change Control Board to approve all production changes and ensure that change management procedures are followed before changes are introduced to a system.

Slide 5



Principles of Computer Security, Fifth Edition

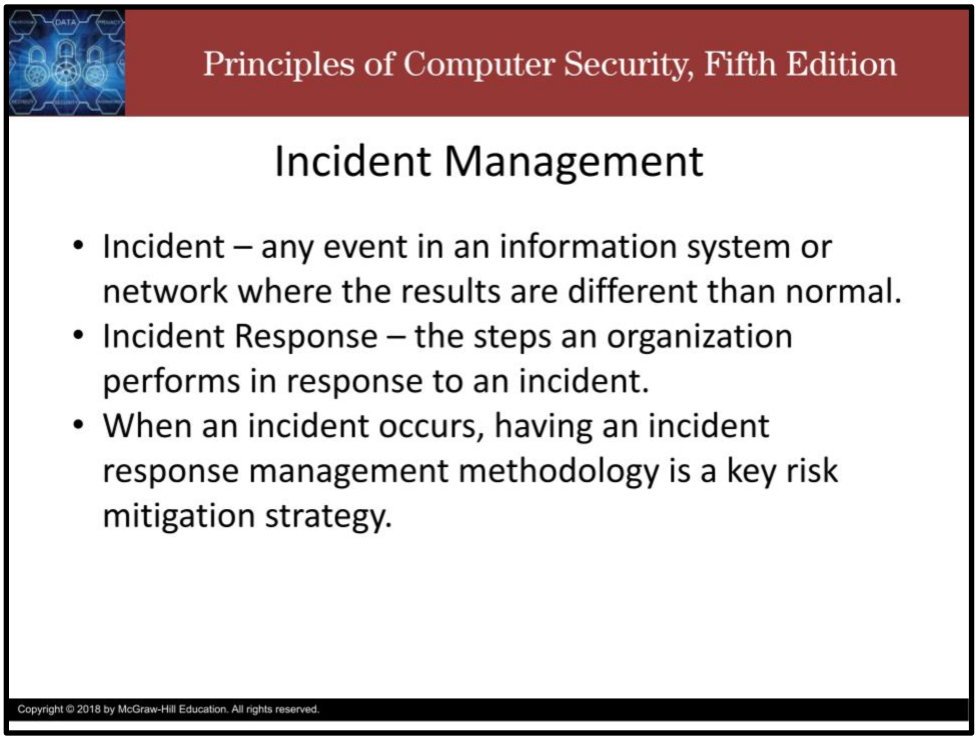
Configuration Control

- Controlling changes to items that have been baselined.
- Ensures that only approved changes to a baseline are allowed to be implemented.
- Key step that provides valuable insight to managers.
  - If a system is being changed, and configuration control is being observed, managers will be better informed
  - Ensures proper use of assets and avoids unnecessary downtime due to the installation of unapproved changes.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Configuration control is the process of controlling changes to items that have been baselined. Configuration control ensures that only approved changes to a baseline are allowed to be implemented. It is easy to understand why a software system, such as a web-based order-entry system, should not be changed without proper testing and control—otherwise, the system might stop functioning at a critical time. Configuration control is a key step that provides valuable insight to managers. If a system is being changed, and configuration control is being observed, managers and others involved will be better informed. This ensures proper use of assets and avoids unnecessary downtime due to the installation of unapproved changes.

Slide 6



Principles of Computer Security, Fifth Edition

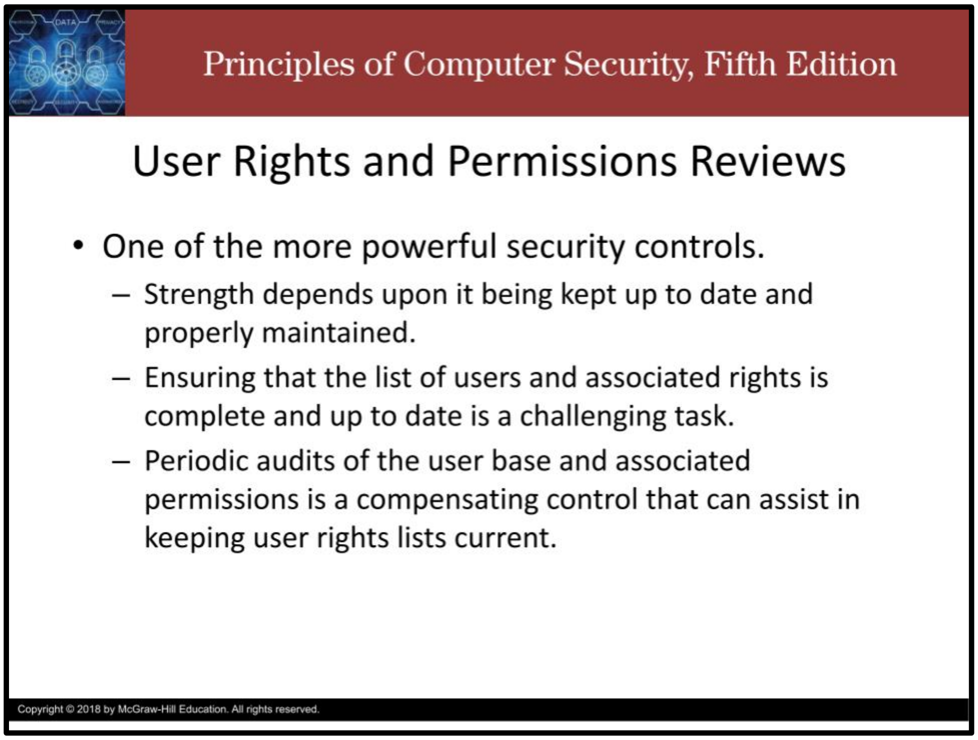
Incident Management

- Incident – any event in an information system or network where the results are different than normal.
- Incident Response – the steps an organization performs in response to an incident.
- When an incident occurs, having an incident response management methodology is a key risk mitigation strategy.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

When an incident occurs, having an incident response management methodology is a key risk mitigation strategy. Incident response and incident management are essential security functions and are covered in more detail in another module.

Slide 7



Principles of Computer Security, Fifth Edition

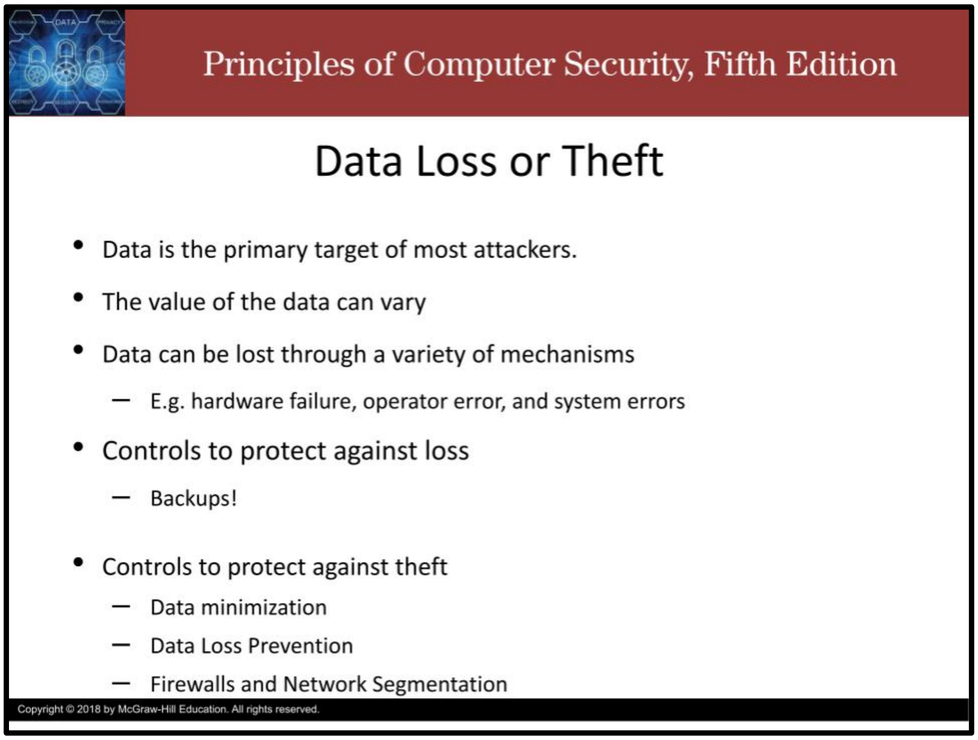
User Rights and Permissions Reviews

- One of the more powerful security controls.
  - Strength depends upon it being kept up to date and properly maintained.
  - Ensuring that the list of users and associated rights is complete and up to date is a challenging task.
  - Periodic audits of the user base and associated permissions is a compensating control that can assist in keeping user rights lists current.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

User rights and permissions reviews are one of the more powerful security controls. However, the strength of this control depends upon it being kept up to date and properly maintained. Ensuring that the list of users and associated rights is complete and up to date is a challenging task in anything bigger than the smallest enterprises. A compensating control that can assist in keeping user rights lists current is a set of periodic audits of the user base and associated permissions.

Slide 8



Principles of Computer Security, Fifth Edition

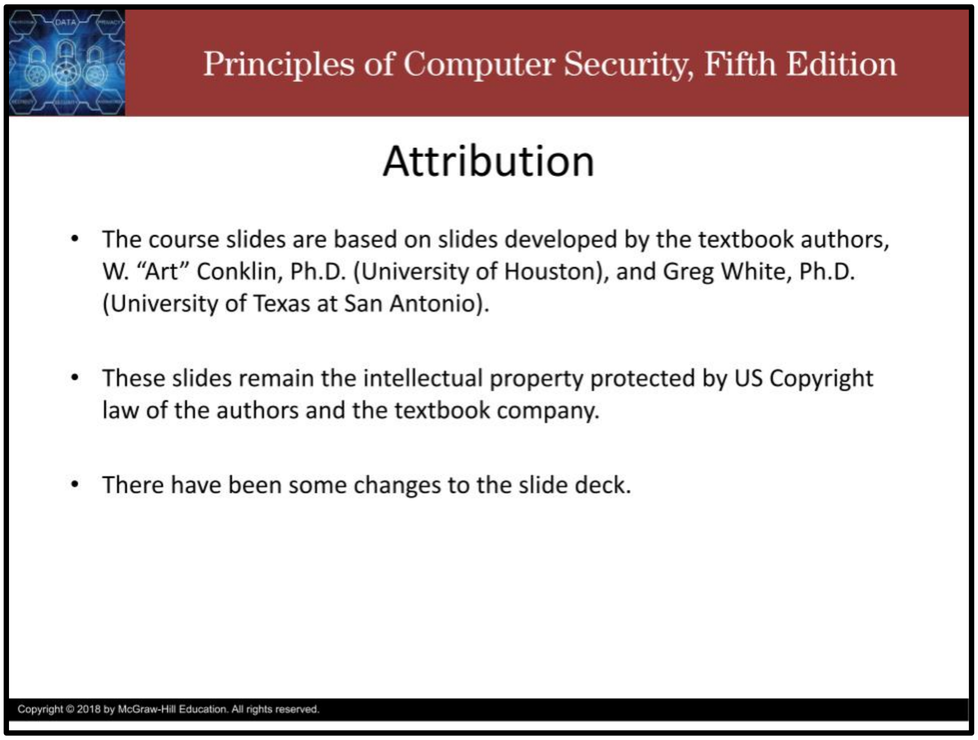
Data Loss or Theft

- Data is the primary target of most attackers.
- The value of the data can vary
- Data can be lost through a variety of mechanisms
  - E.g. hardware failure, operator error, and system errors
- Controls to protect against loss
  - Backups!
- Controls to protect against theft
  - Data minimization
  - Data Loss Prevention
  - Firewalls and Network Segmentation

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Data is the primary target of most attackers. The value of the data can vary, making some data more valuable and hence more at risk of theft. Data can be lost through a variety of mechanisms, with hardware failure, operator error, and system errors being common causes. Regardless of the cause of loss, an organization can take various actions to mitigate the effects of the loss. Backups are at the top of the list of actions, because they can provide the very good protection against loss. To prevent theft, a variety of controls can be employed. Some are risk mitigation steps, such as data minimization, which is the act of not storing what isn't needed. If it must be stored and has value, then technologies such as data loss prevention (which includes encryption) can be used to provide a means of protection. Simple security controls such as firewalls and network segmentation can also act to make data theft more difficult.

Slide 9



Principles of Computer Security, Fifth Edition

Attribution

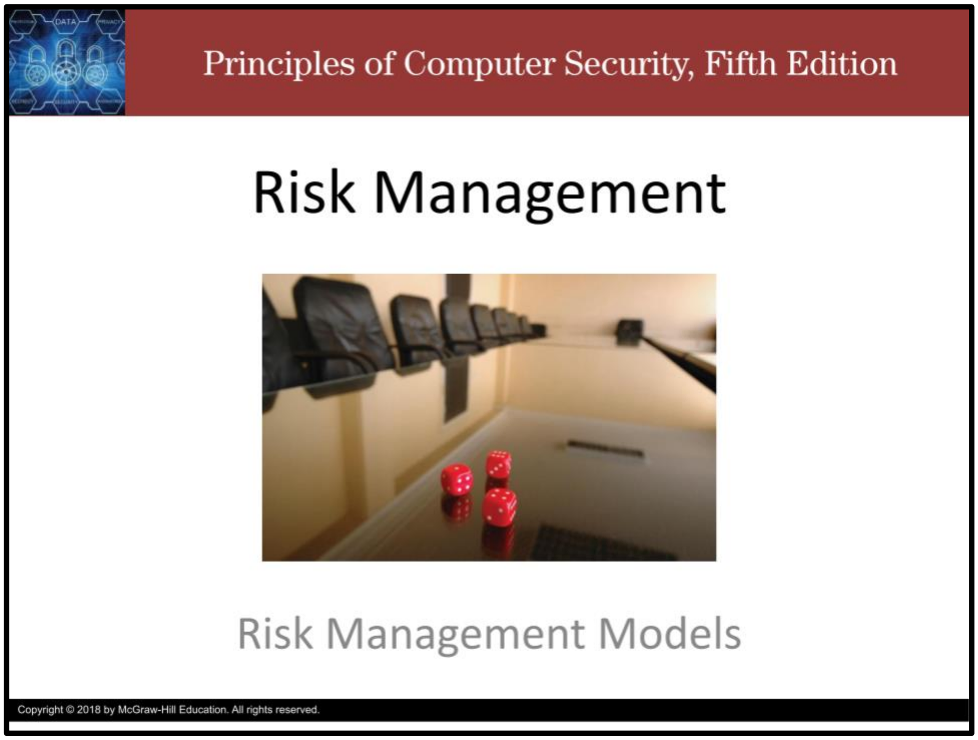
- The course slides are based on slides developed by the textbook authors, W. “Art” Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.
- There have been some changes to the slide deck.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Thank you and take care.

Risk Management: Risk Management Models

Slide 1



Principles of Computer Security, Fifth Edition

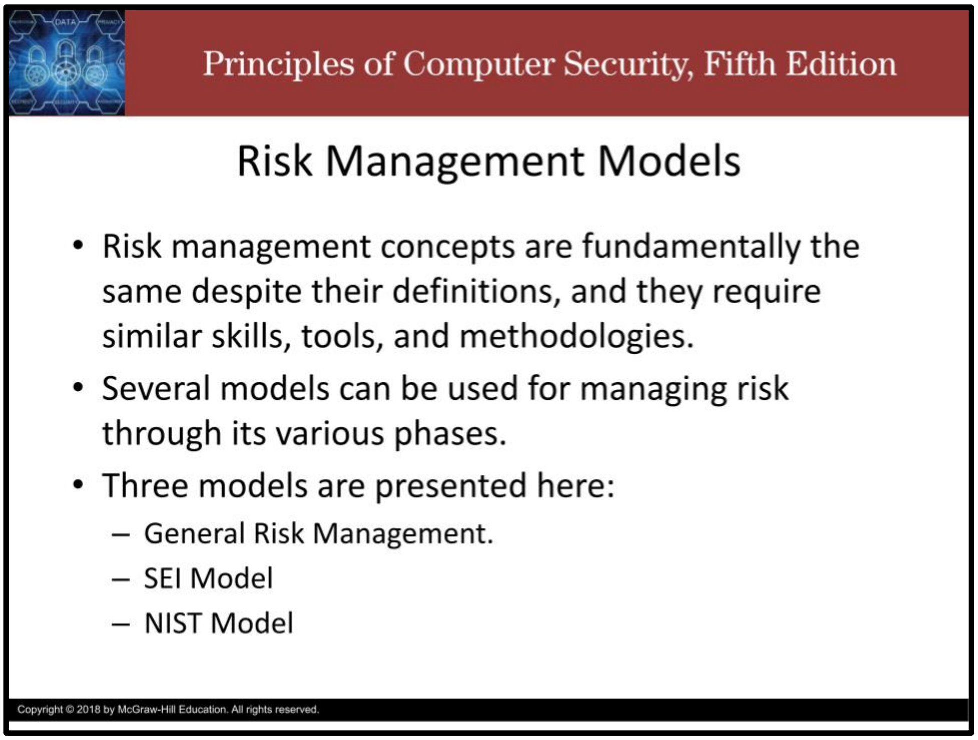
Risk Management

Risk Management Models

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Howdy! In this video, we discuss risk management models.

Slide 2



Principles of Computer Security, Fifth Edition

Risk Management Models

- Risk management concepts are fundamentally the same despite their definitions, and they require similar skills, tools, and methodologies.
- Several models can be used for managing risk through its various phases.
- Three models are presented here:
  - General Risk Management.
  - SEI Model
  - NIST Model

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

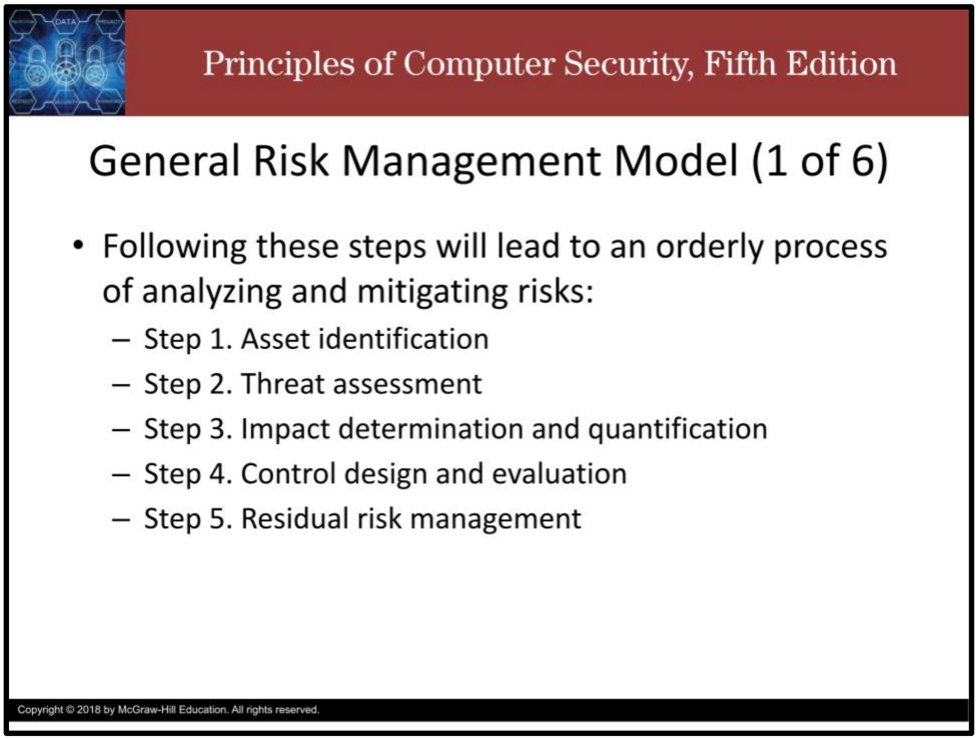
Risk management concepts are fundamentally the same despite their definitions, and they require similar skills, tools, and methodologies. Several models can be used for managing risk through its various phases. Three models are presented here:

The first can be applied to managing risks in general.

The second is tailored for managing risk in software projects.

The third can be applied to an enterprise.

Slide 3



Principles of Computer Security, Fifth Edition

General Risk Management Model (1 of 6)

- Following these steps will lead to an orderly process of analyzing and mitigating risks:
  - Step 1. Asset identification
  - Step 2. Threat assessment
  - Step 3. Impact determination and quantification
  - Step 4. Control design and evaluation
  - Step 5. Residual risk management

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Five steps can be used in virtually any risk management process. Following these steps will lead to an orderly process of analyzing and mitigating risks:

Step 1. Asset identification

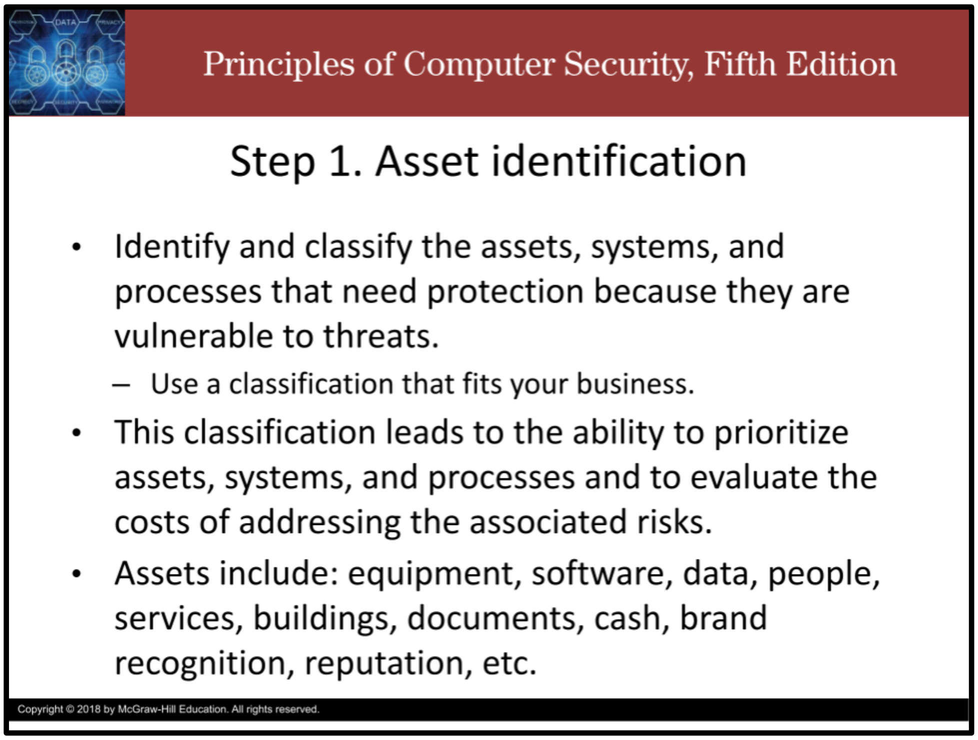
Step 2. Threat assessment

Step 3. Impact determination and quantification

Step 4. Control design and evaluation

Step 5. Residual risk management

Slide 4



Principles of Computer Security, Fifth Edition

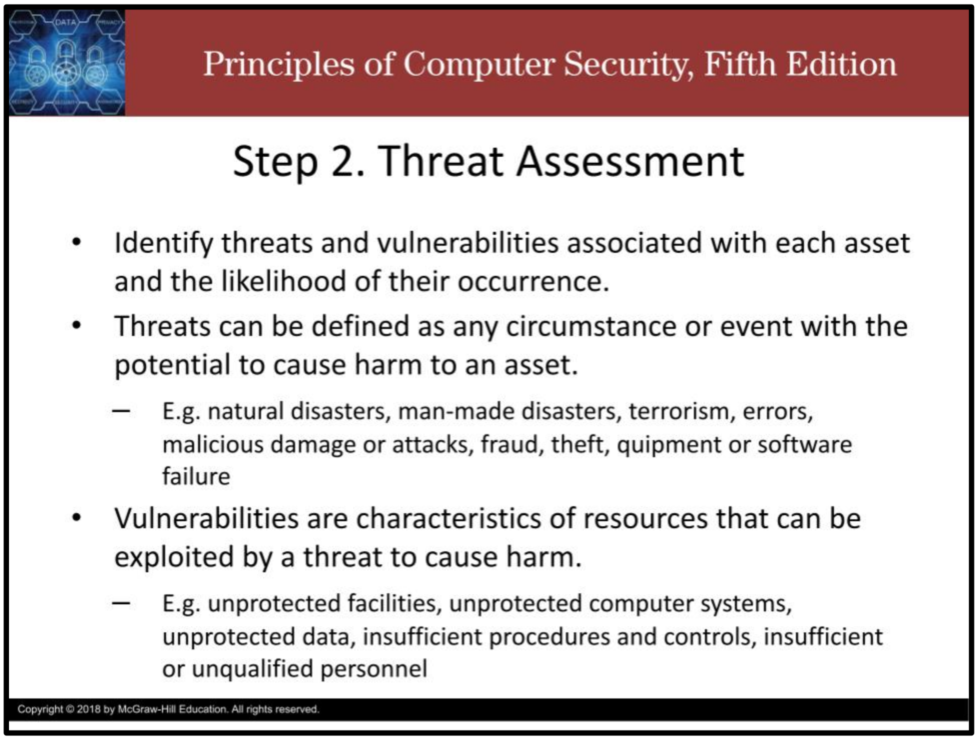
Step 1. Asset identification

- Identify and classify the assets, systems, and processes that need protection because they are vulnerable to threats.
  - Use a classification that fits your business.
- This classification leads to the ability to prioritize assets, systems, and processes and to evaluate the costs of addressing the associated risks.
- Assets include: equipment, software, data, people, services, buildings, documents, cash, brand recognition, reputation, etc.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Identify and classify the assets, systems, and processes that need protection because they are vulnerable to threats. This classification leads to the ability to prioritize assets, systems, and processes and to evaluate the costs of addressing the associated risks. Assets can include the following: equipment, software, data, people, services, buildings, documents, cash, brand recognition, reputation, and more.

Slide 5



Principles of Computer Security, Fifth Edition

Step 2. Threat Assessment

- Identify threats and vulnerabilities associated with each asset and the likelihood of their occurrence.
- Threats can be defined as any circumstance or event with the potential to cause harm to an asset.
  - E.g. natural disasters, man-made disasters, terrorism, errors, malicious damage or attacks, fraud, theft, quipment or software failure
- Vulnerabilities are characteristics of resources that can be exploited by a threat to cause harm.
  - E.g. unprotected facilities, unprotected computer systems, unprotected data, insufficient procedures and controls, insufficient or unqualified personnel

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

After identifying the assets, you identify both the possible threats and the possible vulnerabilities associated with each asset and the likelihood of their occurrence.

Threats are circumstances or event with the potential to cause harm to an asset.

Vulnerabilities are characteristics of resources that can be exploited by a threat to cause harm.

Common classes of threats include:

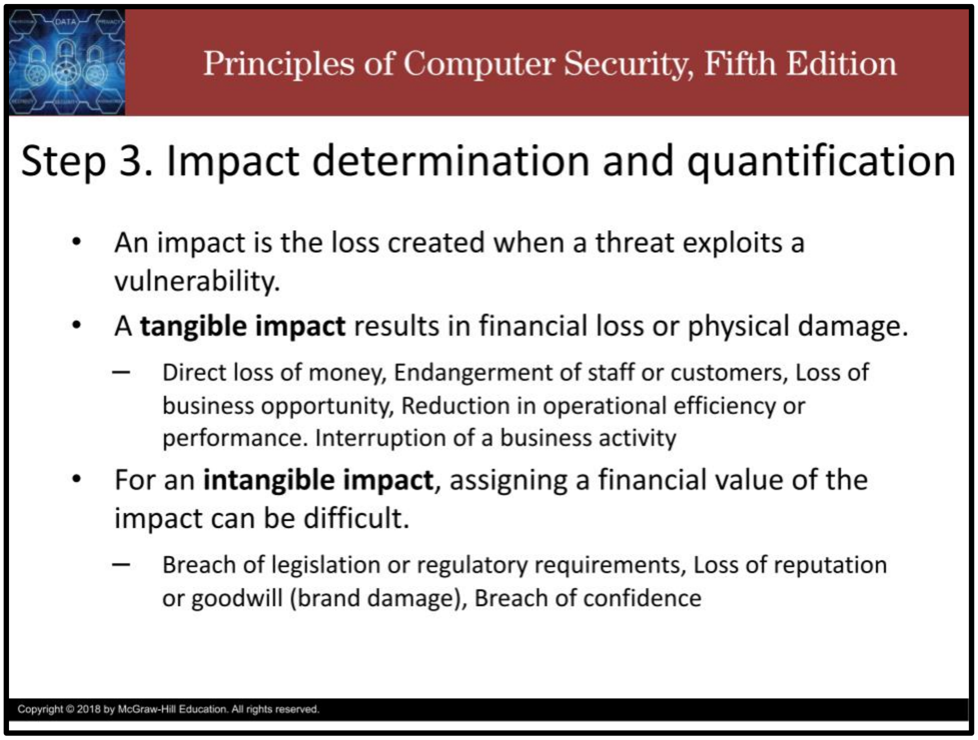
- **Natural disasters** like hurricanes, earthquakes, lightning, and so on.
- **Man-made disasters** like oil spills and climate change.
- **Terrorism** like the January 6th insurrection, mass shootings, and white nationalism
- **Errors** such as employees not following safety or configuration management procedures.
- **Malicious damage or attacks** such as a disgruntled employee purposely corrupting data files.
- **Fraud** such as an executive falsifying travel expenses or vendor invoices and payments.
- **Theft** such as someone stealing a computer
- **Equipment or software failure** such as an error in the calculation of a company-wide bonus underpaying employees.

Common classes of vulnerabilities include:

- **Unprotected facilities** such as company offices with no security officer present or no card-entry system.
- **Unprotected computer systems** such as a server temporarily connected to the network before being properly configured/secured.
- **Unprotected data** such as not installing critical security patches to eliminate application security vulnerabilities.
- **Insufficient procedures and controls** such as a single person having authority create vendors in the accounting system, enter invoices, and authorize check payments.

Insufficient or unqualified personnel such as an employee not sufficiently securing a server due to a lack of training.

Slide 6



Principles of Computer Security, Fifth Edition

Step 3. Impact determination and quantification

- An impact is the loss created when a threat exploits a vulnerability.
- A **tangible impact** results in financial loss or physical damage.
  - Direct loss of money, Endangerment of staff or customers, Loss of business opportunity, Reduction in operational efficiency or performance. Interruption of a business activity
- For an **intangible impact**, assigning a financial value of the impact can be difficult.
  - Breach of legislation or regulatory requirements, Loss of reputation or goodwill (brand damage), Breach of confidence

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

An impact is the loss created when a threat exploits a vulnerability. For example, in a manufacturing facility, storing and using flammable chemicals creates a risk of fire to the facility.

The vulnerability is that flammable chemicals are stored there. The threat would be that a person could cause a fire by mishandling the chemicals (either intentionally or unintentionally).

A **tangible impact** would be the loss incurred if a person ignites the chemicals and fire then destroys part of the facility. An example of an **intangible impact** would be the loss of goodwill or brand damage caused by the impression that the company doesn't safely protect its employees or the surrounding geographic area.

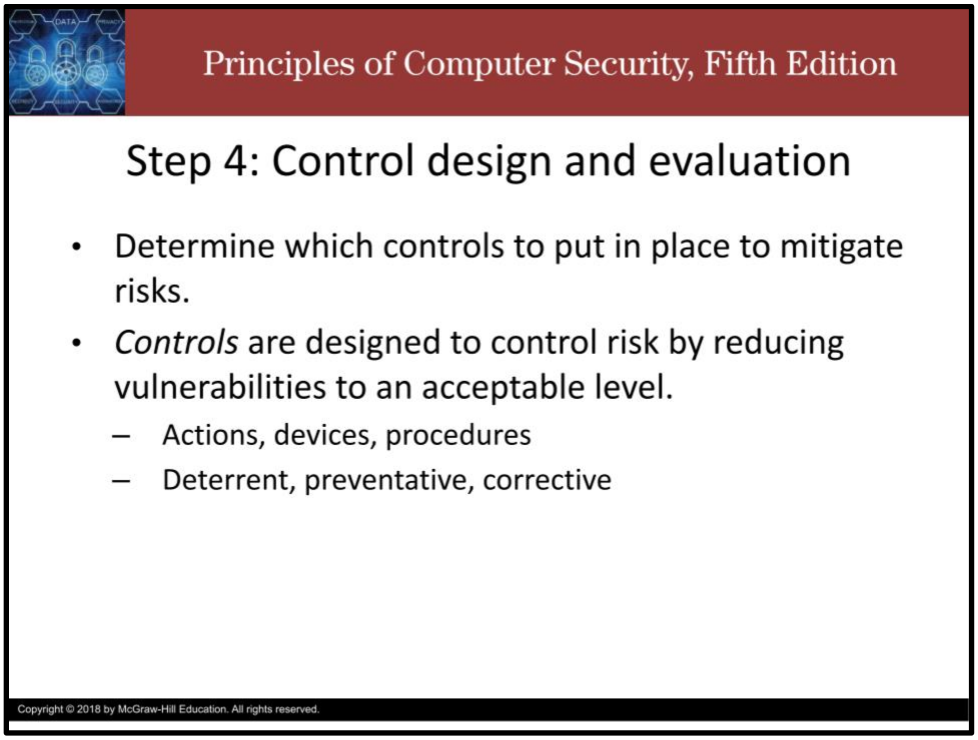
Tangible impacts include:

- Direct loss of money
- Endangerment of staff or customers
- Loss of business opportunity
- Reduction in operational efficiency or performance
- Interruption of a business activity

Intangible impacts include:

- Breach of legislation or regulatory requirements
- Loss of reputation or goodwill and
- Breach of confidence

Slide 7



Principles of Computer Security, Fifth Edition

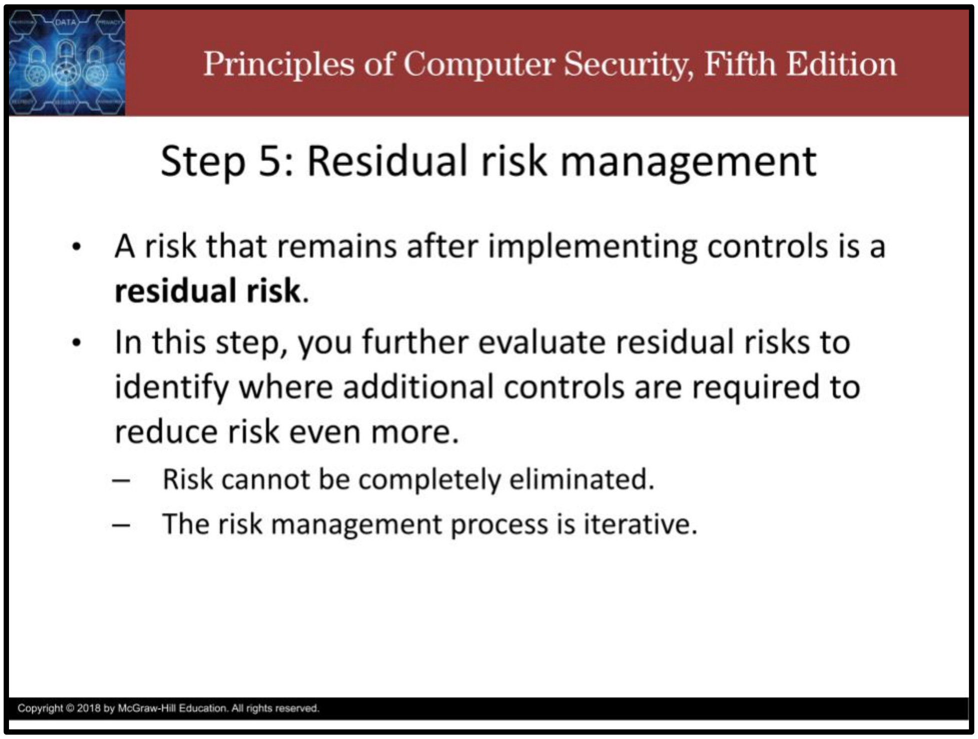
Step 4: Control design and evaluation

- Determine which controls to put in place to mitigate risks.
- *Controls* are designed to control risk by reducing vulnerabilities to an acceptable level.
  - Actions, devices, procedures
  - Deterrent, preventative, corrective

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

In this step, you determine which controls to put in place to mitigate risks.
Controls are designed to control risk by reducing vulnerabilities to an acceptable level.
Controls can be actions, devices, or procedures and they can be deterrent, preventative, or corrective.

Slide 8



Principles of Computer Security, Fifth Edition

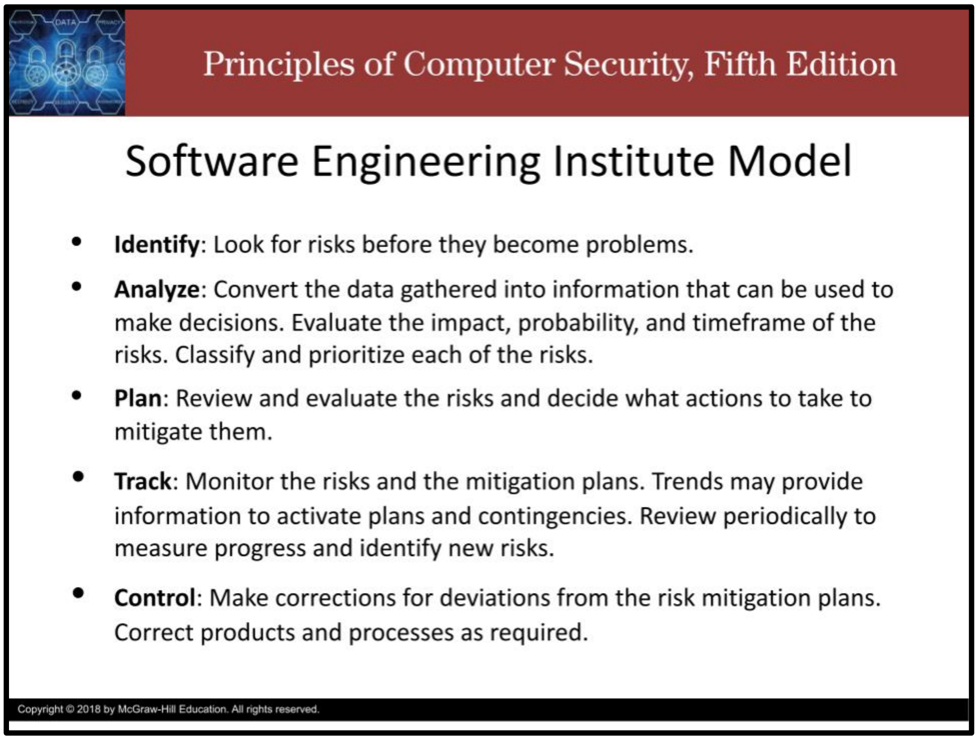
Step 5: Residual risk management

- A risk that remains after implementing controls is a **residual risk**.
- In this step, you further evaluate residual risks to identify where additional controls are required to reduce risk even more.
  - Risk cannot be completely eliminated.
  - The risk management process is iterative.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Risk that remains after implementing controls is called **residual risk**. In this step, you evaluate residual risks to identify where additional controls are required to reduce risk even more. Recall that Risk cannot be completely eliminated, and the risk management process is iterative.

Slide 9



Principles of Computer Security, Fifth Edition

Software Engineering Institute Model

- **Identify**: Look for risks before they become problems.
- **Analyze**: Convert the data gathered into information that can be used to make decisions. Evaluate the impact, probability, and timeframe of the risks. Classify and prioritize each of the risks.
- **Plan**: Review and evaluate the risks and decide what actions to take to mitigate them.
- **Track**: Monitor the risks and the mitigation plans. Trends may provide information to activate plans and contingencies. Review periodically to measure progress and identify new risks.
- **Control**: Make corrections for deviations from the risk mitigation plans. Correct products and processes as required.

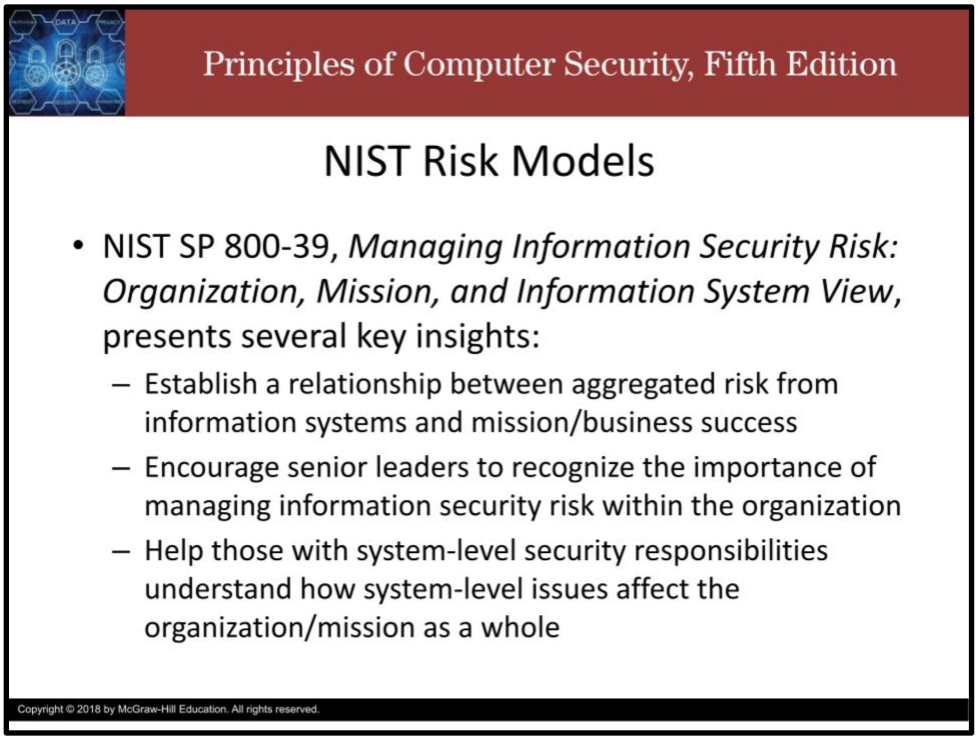
Copyright © 2018 by McGraw-Hill Education. All rights reserved.

In an approach tailored for managing risk in software projects, SEI uses the paradigm of Identify, Analyze, Plan, Track, and Control.

In the Identify activity, we look for risks before they become problems.
In the Analyze activity, we convert the data gathered into information that can be used to make decisions. We evaluate the impact, probability, and timeframe of the risks. And we classify and prioritize each of the risks.
In the Plan activity, we review and evaluate the risks and decide what actions to take to mitigate them.
In the Track activity, we monitor the risks and the mitigation plans. We look for trends that may provide information to activate plans and contingencies. And we conduct periodic reviews to measure progress and identify new risks.
In the Control activity, we make corrections for deviations from the risk mitigation plans. We correct products and processes as required.

Although the terminology varies slightly from the General Risk Management model, the relationships are apparent, and either model can be applied wherever risk management is used.

Slide 10



Principles of Computer Security, Fifth Edition

NIST Risk Models

- NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, presents several key insights:
  - Establish a relationship between aggregated risk from information systems and mission/business success
  - Encourage senior leaders to recognize the importance of managing information security risk within the organization
  - Help those with system-level security responsibilities understand how system-level issues affect the organization/mission as a whole

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

NIST has several informative risk models that can be applied to an enterprise. NIST has published several Special Publications associated with risk management.

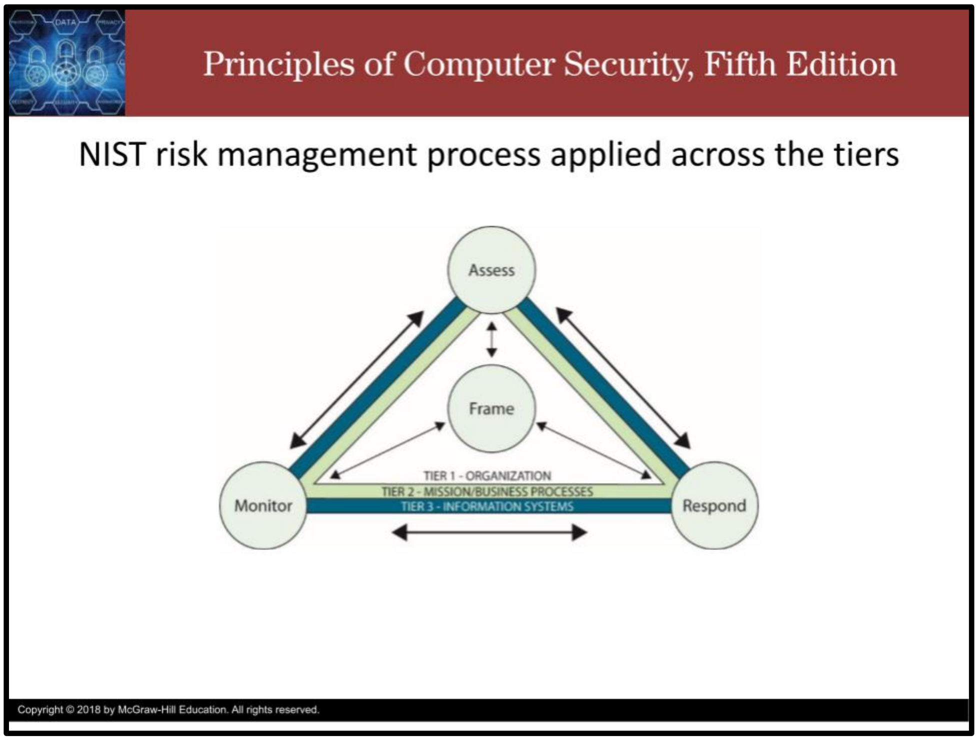
NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, presents several keys to effective and successful risk management:

There needs to established a relationship between aggregated risk from information systems and mission/business success

Senior leaders must recognize the importance of managing information security risk within the organization

Those with system-level security responsibilities must understand how system-level issues affect the organization/mission as a whole

Slide 11



Principles of Computer Security, Fifth Edition

NIST risk management process applied across the tiers

Assess
Frame
Monitor
Respond
TIER 1 - ORGANIZATION
TIER 2 - MISSION/BUSINESS PROCESSES
TIER 3 - INFORMATION SYSTEMS

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

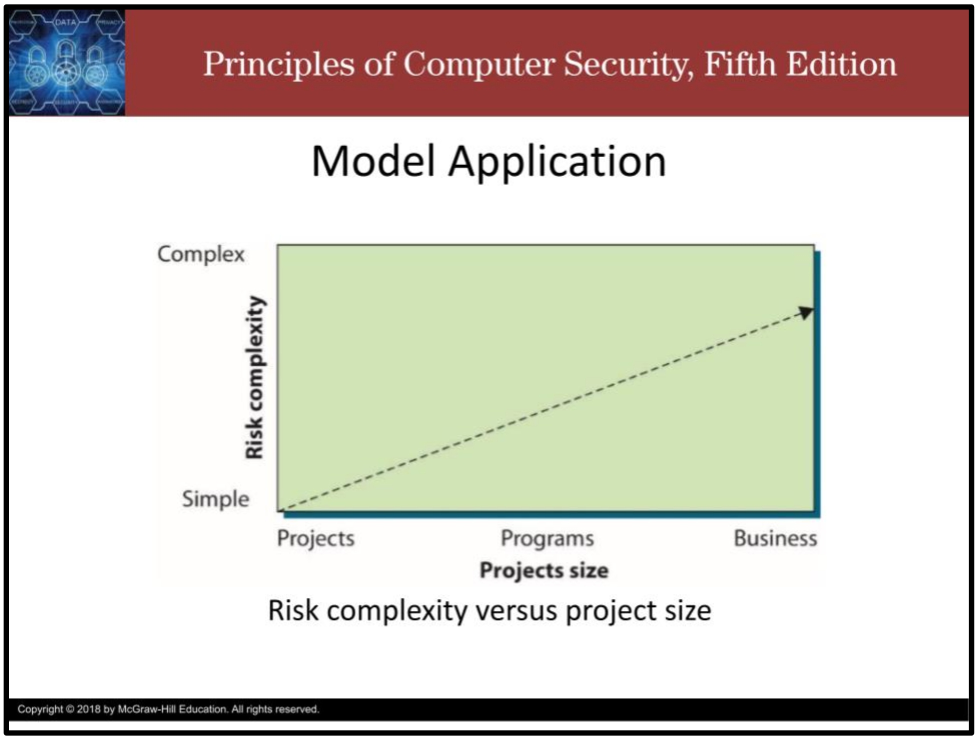
The SP 800-39 model has two distinct levels of analysis, which work together as one in describing risk management actions.

The first level of analysis is represented by four elements: Frame, Assess, Respond, and Monitor.
The second level is related to the tiers represented in the hierarchical triangles: Organization, Mission/Business Processes, and Information Systems.

The Frame element represents the organization’s risk framing that establishes the context and provides a common perspective on how the organization manages risk.
Risk framing is central to the model.
Its principal output is a risk management strategy that addresses how the organization assesses risk, responds to risk, and monitors risk.
The three tiers represent the different distinct layers in an organization that are associated with risk.
Tier 1, representing the executive function, is where the risk framing occurs.
At Tier 2, the mission and business process layer, the risk management functions of assess, respond, and monitor occur.
Tier 3 is the information system layer where activities of risk management are manifested in the systems of the organization.

But, actually, all steps of the risk management and assessment process can occur at all three layers.

Slide 12



Principles of Computer Security, Fifth Edition

Model Application

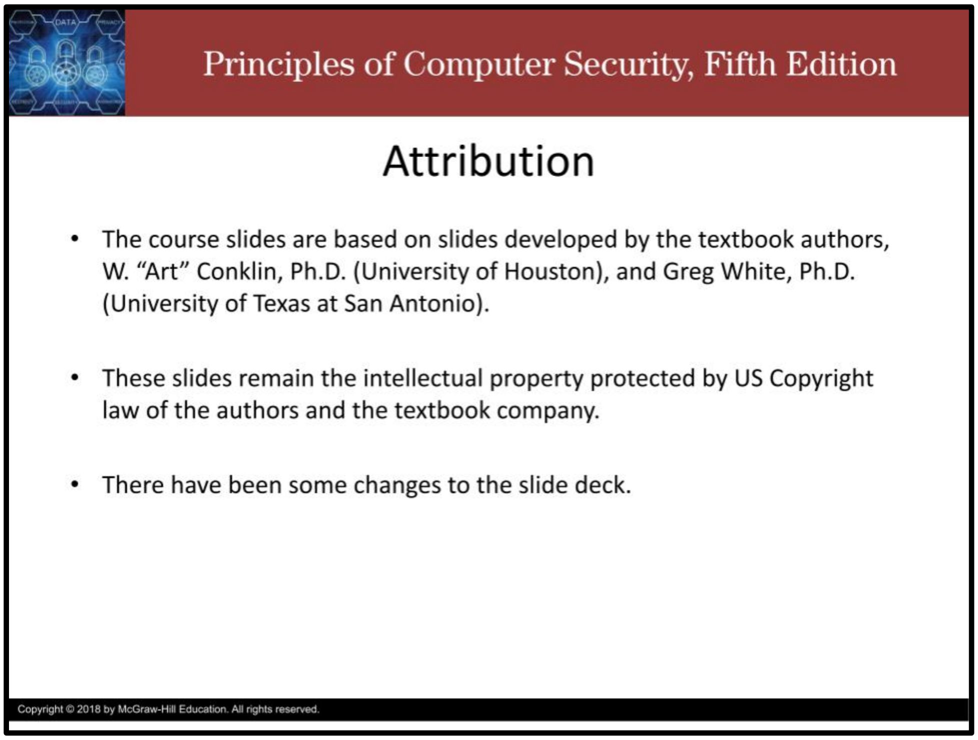
Risk complexity versus project size

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

The three model examples define steps to use in any general or software risk management process.

These risk management principles can be applied to any project, program, or business activity, no matter how simple or complex.
The Figure shows how risk management can be applied across the continuum and that the complexity of risk management generally increases with the size of the project, program, or business to be managed.
I should note that, despite what the figure seems to imply, the complexity of risk at the simple level is not 0. The risk complexity is never 0 unless there is no activity whatsoever.

Slide 13



Principles of Computer Security, Fifth Edition

Attribution

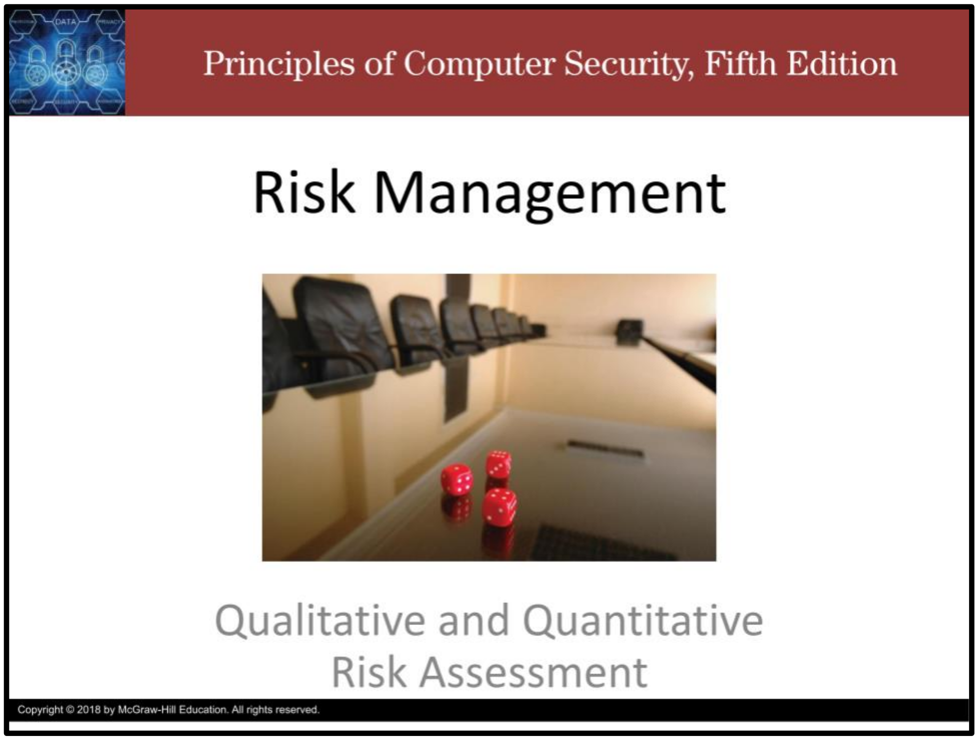
- The course slides are based on slides developed by the textbook authors, W. “Art” Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.
- There have been some changes to the slide deck.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Thank you and take care.

Risk Management: Qualitative and Quantitative Risk Assessment

Slide 1



Principles of Computer Security, Fifth Edition

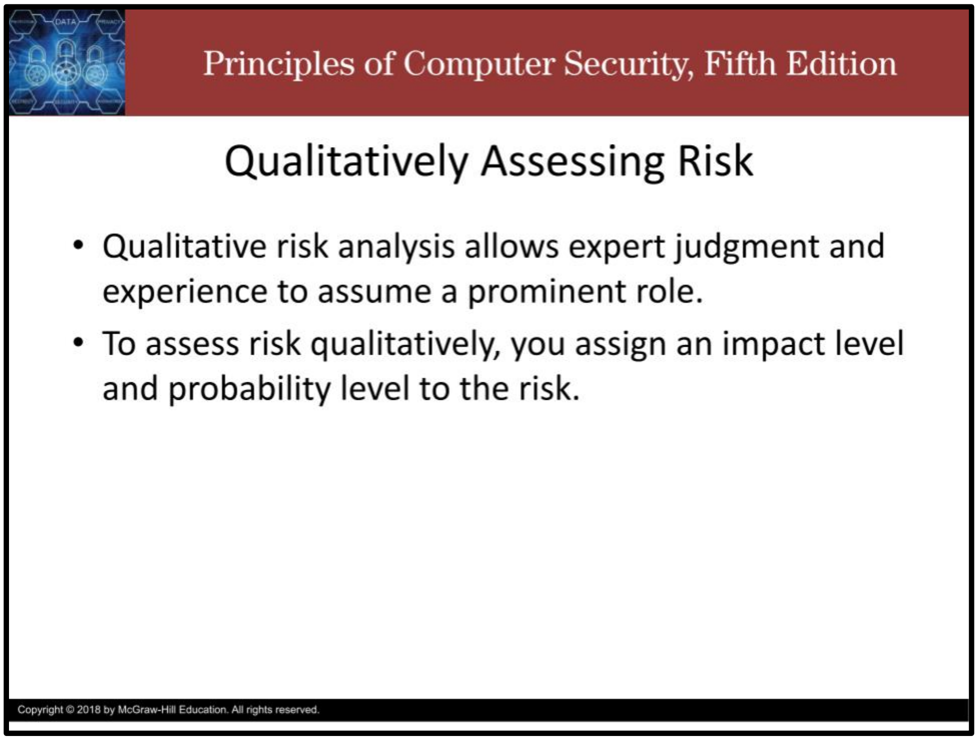
Risk Management

Qualitative and Quantitative Risk Assessment

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Howdy! In this video, we discuss qualitative and quantitative risk assessment.

Slide 2



Principles of Computer Security, Fifth Edition

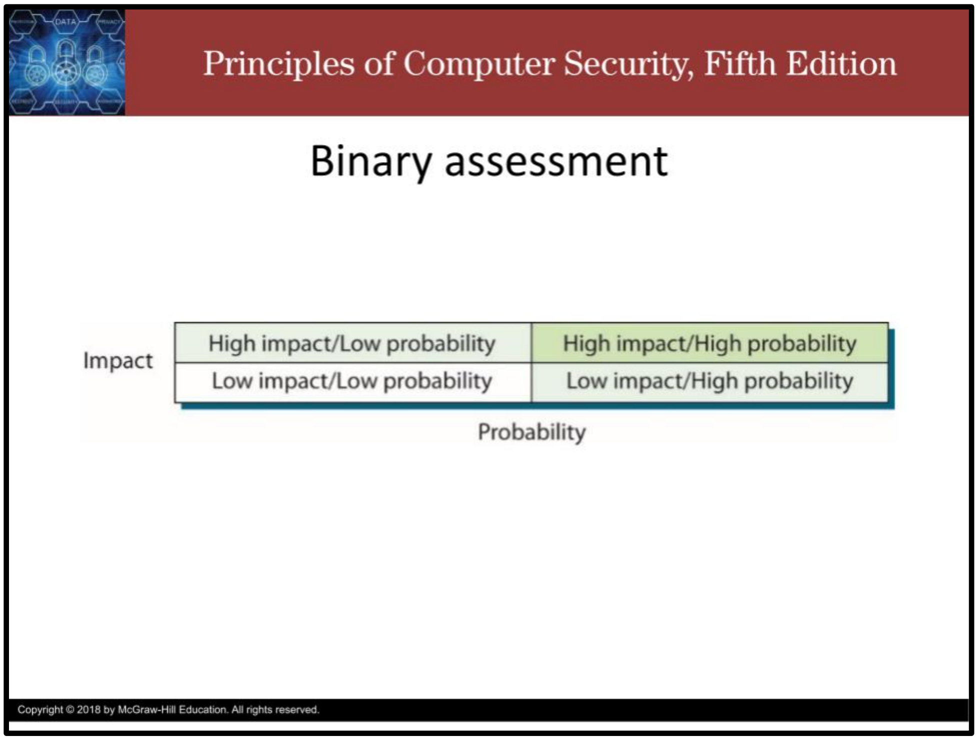
Qualitatively Assessing Risk

- Qualitative risk analysis allows expert judgment and experience to assume a prominent role.
- To assess risk qualitatively, you assign an impact level and probability level to the risk.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Qualitative risk analysis allows expert judgment and experience to assume a prominent role. To assess risk qualitatively, you assign an impact level and probability level to the risk.

Slide 3



Principles of Computer Security, Fifth Edition

Binary assessment

Impact	High impact/Low probability	High impact/High probability
	Low impact/Low probability	Low impact/High probability

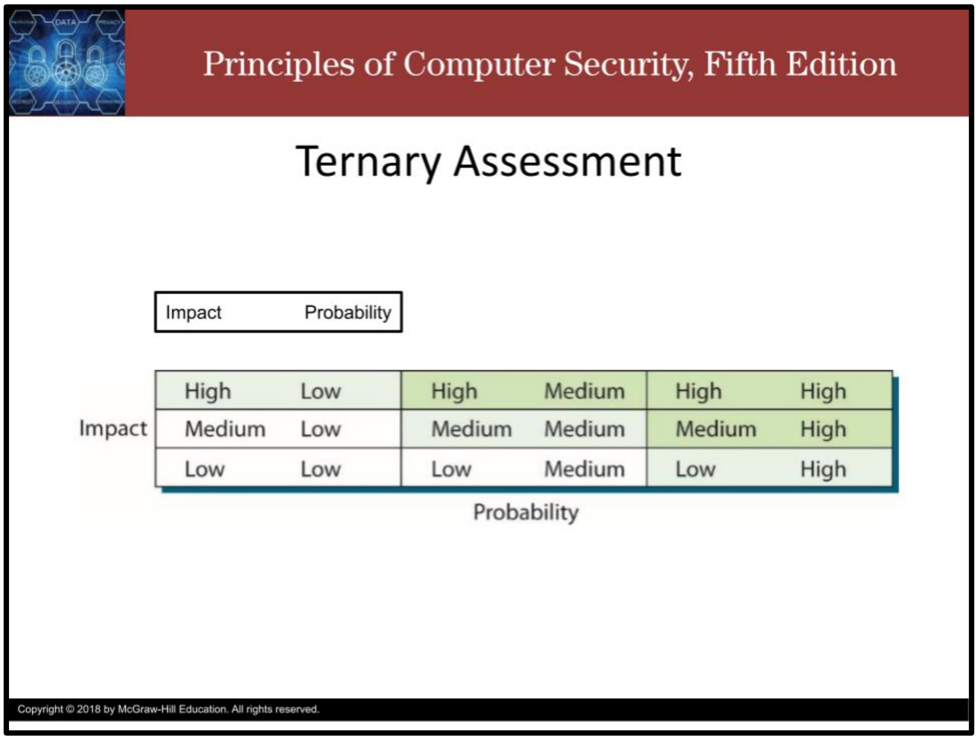
Probability

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

The figure shows an example of a binary assessment, where only two outcomes are possible each for impact and probability. Either it will have an impact or it will not (or it will have a low or high impact), and it will occur or it won't (or it will have a high probability of occurring or a low probability of occurring).

For example, if a threat has a high impact and a high probability of occurring, the risk exposure is high and probably requires some action to reduce this threat (the green box in the figure). Conversely, if the impact is low with a low probability, the risk exposure is low and no action may be required to reduce the likelihood of the occurrence or impact of this threat (the white box in the figure). In reality, a few threats can usually be identified as presenting high-risk exposure and a few threats present low-risk exposure. The threats that fall somewhere between (the pale green boxes on the diagonal in the figure) will have to be evaluated by judgment and management experience.

Slide 4



Principles of Computer Security, Fifth Edition

Ternary Assessment

Impact	Probability

	High Low	High Medium	High High
Impact	Medium Low	Medium Medium	Medium High
	Low Low	Low Medium	Low High
		Probability	

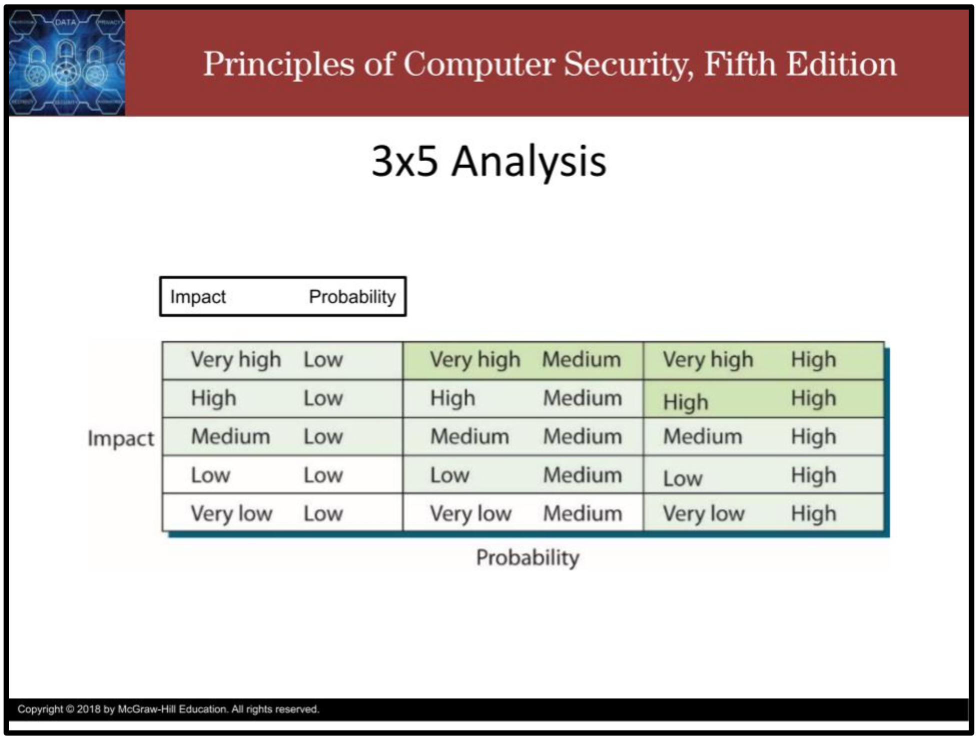
Copyright © 2018 by McGraw-Hill Education. All rights reserved.

If the analysis is more complex, requiring three levels of analysis, such as low-medium-high or green-yellow-red nine combinations are possible.

Again, the green boxes probably require action, the white boxes may or may not require action, and the pale green boxes require judgment.

In the figure, the first term in each box refers to the magnitude of the impact, and the second term refers to the probability of the threat occurring.

Slide 5



Principles of Computer Security, Fifth Edition

3x5 Analysis

Impact	Probability

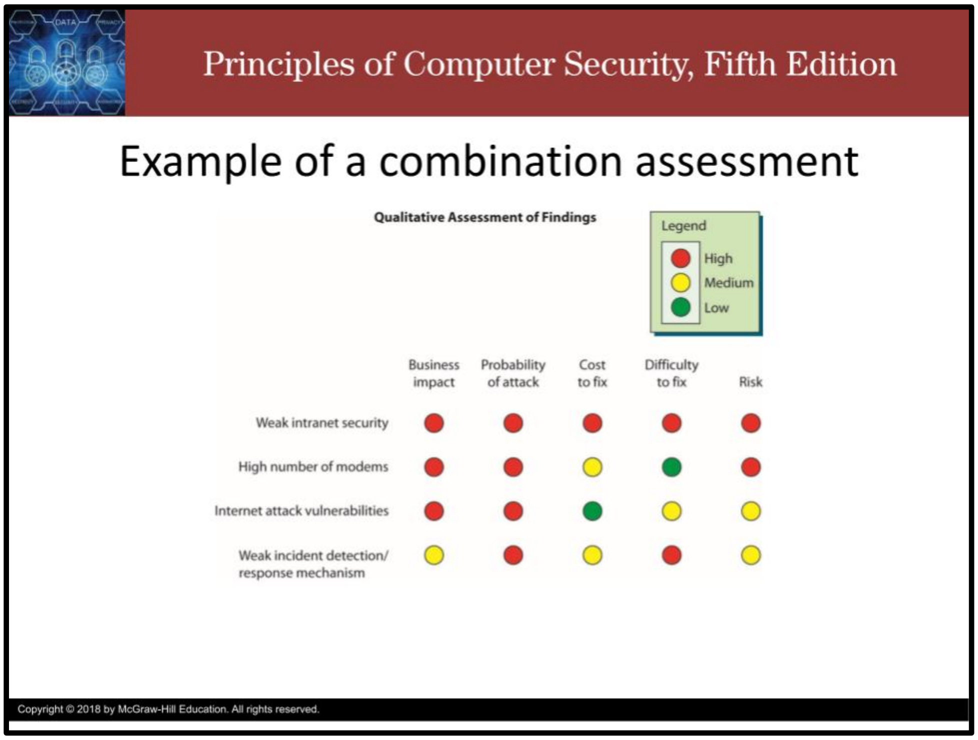
	Very high	Low	Very high	Medium	Very high	High
	High	Low	High	Medium	High	High
Impact	Medium	Low	Medium	Medium	Medium	High
	Low	Low	Low	Medium	Low	High
	Very low	Low	Very low	Medium	Very low	High

Probability

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Other levels of complexity are possible. The matrix does not have to be symmetrical. For example, if the probability is assessed with three values (low, medium, high) and the impact has five values (very low, low, medium, high, very high), the 15 analysis categories would be as shown in the figure. The green boxes probably require action, the white boxes may or may not require action, and the rest require judgment.

Slide 6



Principles of Computer Security, Fifth Edition

Example of a combination assessment

Qualitative Assessment of Findings

Legend

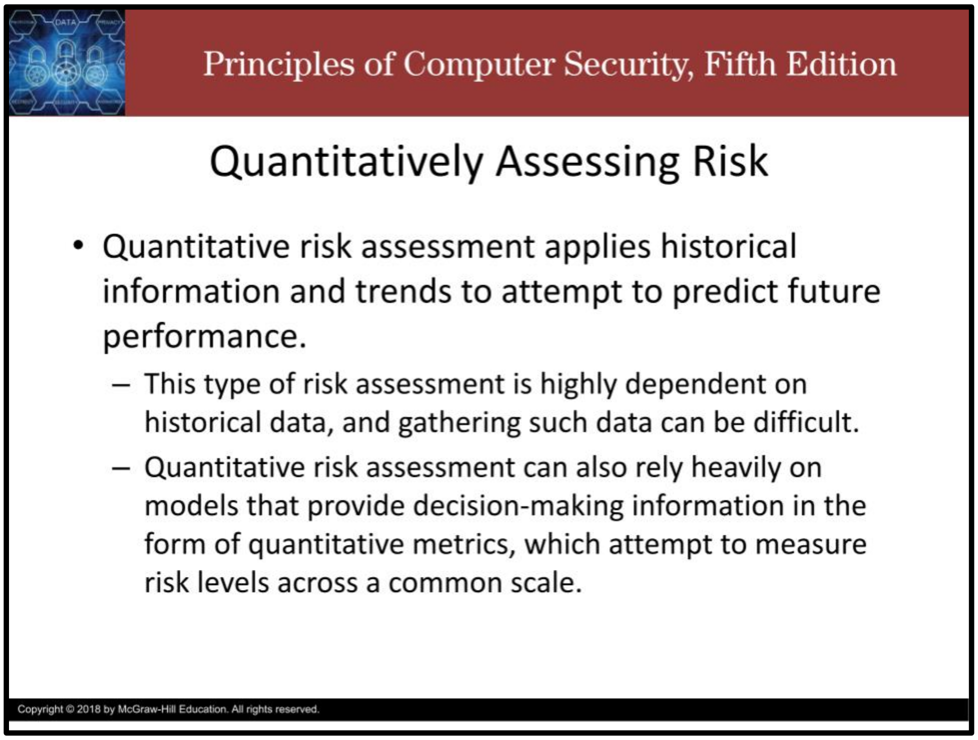
🔴	High
🟡	Medium
🟢	Low

	Business impact	Probability of attack	Cost to fix	Difficulty to fix	Risk
Weak intranet security	🔴	🔴	🔴	🔴	🔴
High number of modems	🔴	🔴	🟡	🟢	🔴
Internet attack vulnerabilities	🔴	🔴	🟢	🟡	🟡
Weak incident detection/ response mechanism	🟡	🔴	🟡	🔴	🟡

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

So far, the examples have focused on assessing likelihood versus impact. Qualitative risk assessment can be adapted to a variety of attributes and situations in combination with each other. For example, this shows the comparison of some specific risks that have been identified during a security assessment. The assessment identified the risk areas listed in the first column (weak intranet security, high number of modems, Internet attack vulnerabilities, and weak incident detection and response mechanism). The assessment also identified various potential impacts, listed across the top (business impact, probability of attack, cost to fix, and difficulty to fix). Each of the impacts has been assessed as low, medium, or high—depicted using green, yellow, and red, respectively. Each of the risk areas has been assessed with respect to each of the potential impacts, and an overall risk assessment has been determined in the last column.

Slide 7



Principles of Computer Security, Fifth Edition

Quantitatively Assessing Risk

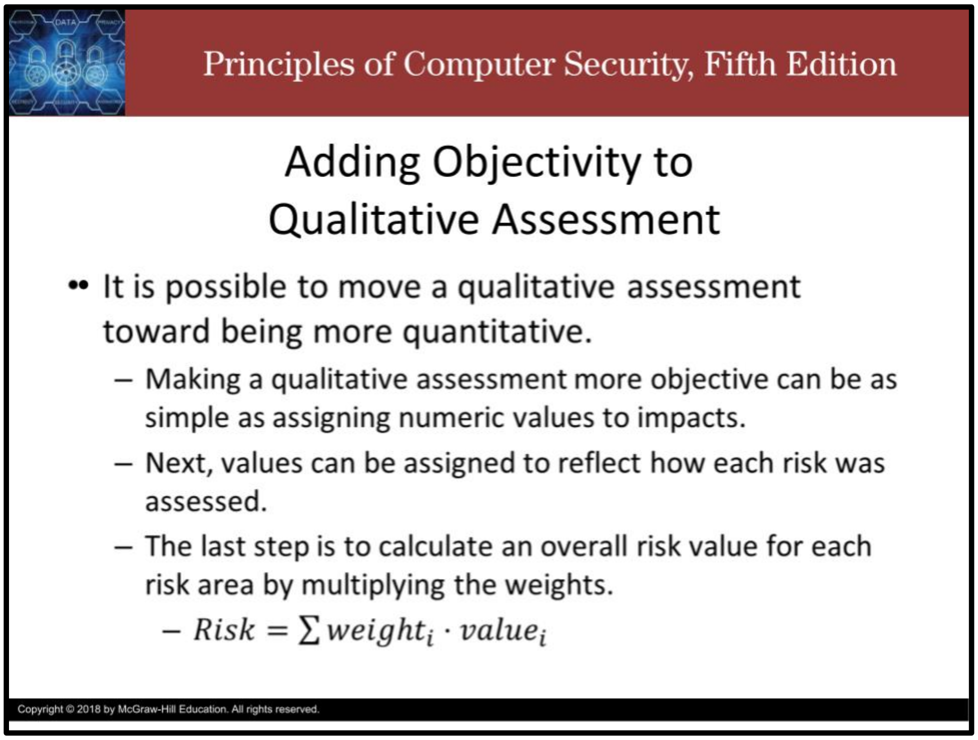
- Quantitative risk assessment applies historical information and trends to attempt to predict future performance.
  - This type of risk assessment is highly dependent on historical data, and gathering such data can be difficult.
  - Quantitative risk assessment can also rely heavily on models that provide decision-making information in the form of quantitative metrics, which attempt to measure risk levels across a common scale.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Qualitative risk assessment relies on judgment and experience. Quantitative risk assessment applies historical information and trends to attempt to predict future performance. This type of risk assessment is highly dependent on historical data and gathering such data can be difficult. It can also rely heavily on models that provide decision-making information in the form of quantitative metrics, which attempt to measure risk levels across a common scale.

It is important to understand that key assumptions underlie any model, and different models will produce different results even when given the same input data. Although significant research and development have been invested in improving and refining the various risk analysis models, expert judgment and experience must still be considered an essential part of any risk assessment process. Models can never replace judgment and experience, but they can significantly enhance the decision-making process.

Slide 8



Principles of Computer Security, Fifth Edition

Adding Objectivity to Qualitative Assessment

- It is possible to move a qualitative assessment toward being more quantitative.
  - Making a qualitative assessment more objective can be as simple as assigning numeric values to impacts.
  - Next, values can be assigned to reflect how each risk was assessed.
  - The last step is to calculate an overall risk value for each risk area by multiplying the weights.
    - $Risk = \sum weight_i \cdot value_i$

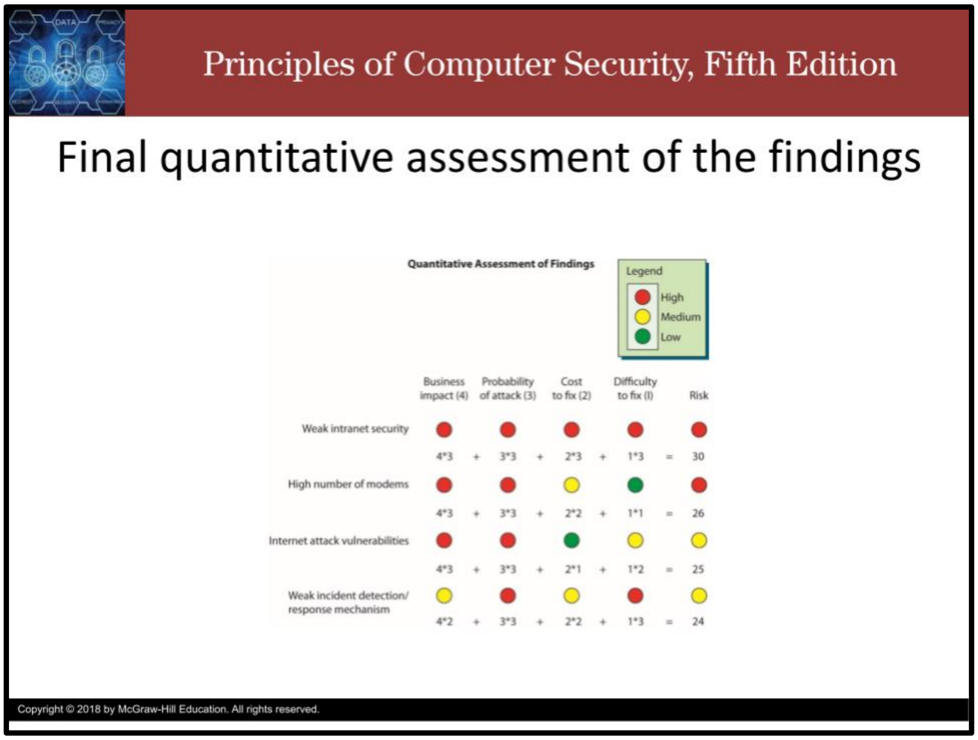
Copyright © 2018 by McGraw-Hill Education. All rights reserved.

It is possible to move a qualitative assessment toward being more quantitative. Making a qualitative assessment more objective can be as simple as assigning numeric values to one of the tables shown on the previous slides. For example, the impacts listed in the example of a combination assessment (with the traffic light values) can be prioritized from highest to lowest and then weighted. Maybe business impact would be weighted the most and difficulty to fix weighted least.

Next, values can be assigned to reflect how each risk was assessed. The analysis can thus be made more objective by assigning a value to each color that represents an assessment. For example, a red assessment indicates many critical, unresolved issues, and this will be given an assessment value of 3. Green means few issues are unresolved, so it is given a value of 1.

The last step is to calculate an overall risk value for each risk area by multiplying the weights by the assessed values and summing the products:

Slide 9



Principles of Computer Security, Fifth Edition

Final quantitative assessment of the findings

Quantitative Assessment of Findings

Legend

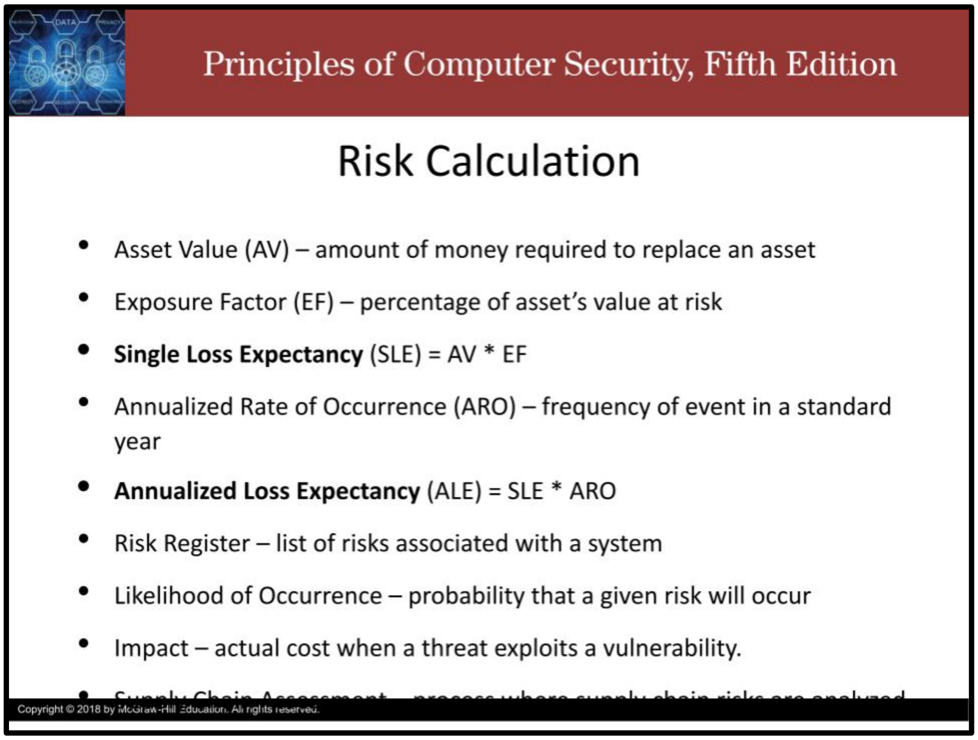
🔴	High
🟡	Medium
🟢	Low

	Business impact (4)		Probability of attack (3)		Cost to fix (2)		Difficulty to fix (I)		Risk
Weak intranet security	🔴		🔴		🔴		🔴		🔴
	4*3	+	3*3	+	2*3	+	1*3	=	30
High number of modems	🔴		🔴		🟡		🟢		🔴
	4*3	+	3*3	+	2*2	+	1*1	=	26
Internet attack vulnerabilities	🔴		🔴		🟢		🟡		🟡
	4*3	+	3*3	+	2*1	+	1*2	=	25
Weak incident detection/ response mechanism	🟡		🔴		🟡		🔴		🟡
	4*2	+	3*3	+	2*2	+	1*3	=	24

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

The risk calculation and final risk value for each risk area listed in the example are shown in this figure. The assessed areas can then be ordered from highest to lowest based on the calculated risk value to aid management in focusing on the risk areas with the greatest risk.

Slide 10



Principles of Computer Security, Fifth Edition

Risk Calculation

- Asset Value (AV) – amount of money required to replace an asset
- Exposure Factor (EF) – percentage of asset's value at risk
- **Single Loss Expectancy** (SLE) = AV * EF
- Annualized Rate of Occurrence (ARO) – frequency of event in a standard year
- **Annualized Loss Expectancy** (ALE) = SLE * ARO
- Risk Register – list of risks associated with a system
- Likelihood of Occurrence – probability that a given risk will occur
- Impact – actual cost when a threat exploits a vulnerability.
- Supply Chain Assessment – process where supply chain risks are analyzed

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

More complex models permit a variety of analyses based on statistical and mathematical models.
A common method is the calculation of the annualized loss expectancy. Calculating the ALE creates a monetary value of the impact. This calculation begins by calculating a single loss expectancy.

For example, assume the asset value of a small office building and its contents is $2 million. Also assume that this building houses the call center for a business, and the complete loss of the center would take away about half of the capability of the company. Therefore, the exposure factor is 50 percent and the SLE is $2 million × 0.5 = $1 million.

The ALE is then calculated simply by multiplying the SLE by the number of times the event is expected to occur in a year, which is called the annualized rate of occurrence.
If the event is expected to occur once in 20 years, then the ARO is 1/20 or 0.05.
Typically the ARO is defined by historical data, either from a company's own experience or from industry surveys.

Continuing our example, assume that a fire at this business's location is expected to occur about once in 20 years. Given this information, the ALE is
$1 million × 1/20 = $50,000

The ALE determines a threshold for evaluating the cost/benefit ratio of a given countermeasure. Therefore, a countermeasure to protect this business adequately should cost no more than the calculated ALE of $50,000 per year.

A risk register is a list of the risks associated with a system.

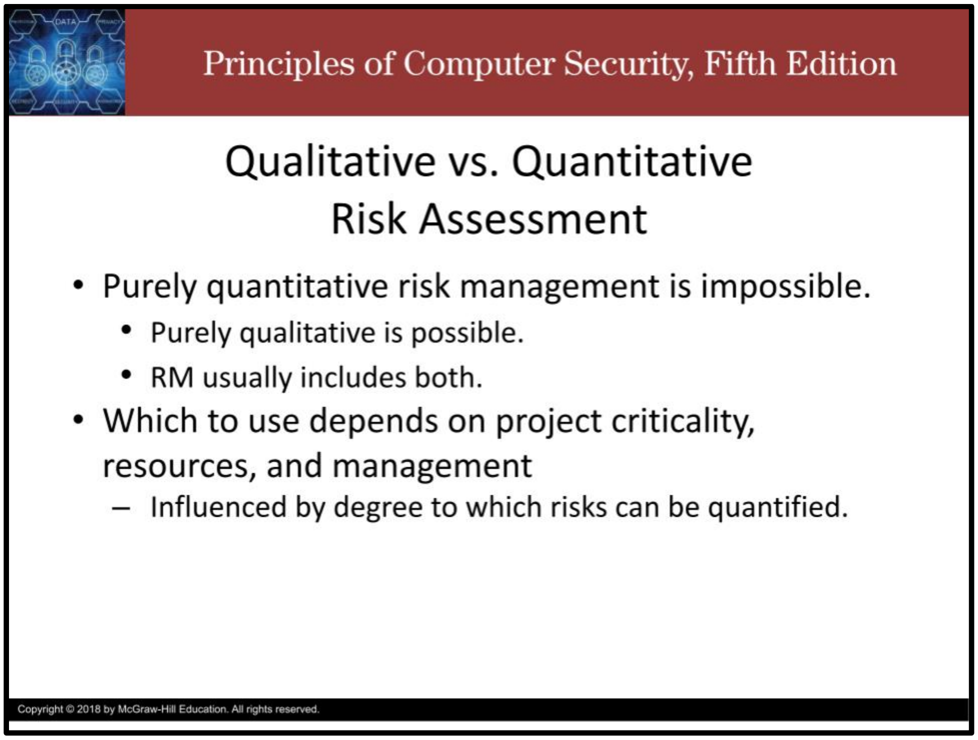
It can also contain information such as the category of risk, probability of occurrence, impact, mitigation factors, and other data.

The likelihood of occurrence is the probability that a particular risk will occur. This measure can be qualitative or quantitative. For qualitative measures, it is typically defined on an annual basis. If defined quantitatively, it is used to create rank order outcomes.

The impact of an event is a measure of the actual loss when a threat exploits a vulnerability. The impact needs to be defined in terms of the context of each organization, as what is high for some firms may be low for much larger firms. A common method is to define the impact levels in terms of important business criteria. Impacts can be in terms of dollar cost, performance (such as a service level agreement or other requirements), schedule, or any other important item. Impact can also be categorized in terms of the security goal that is relevant to the problem: one of the CIA or triple A goals.

The analysis of risk in a supply chain is an important issue. One needs to consider not just the risk associated with a system but the risk embedded in a system as a result of its creation, which includes risks from the supply chain associated with elements inside a system. *Supply chain assessment* is the process where these risks are determined and explored.

Slide 11



Principles of Computer Security, Fifth Edition

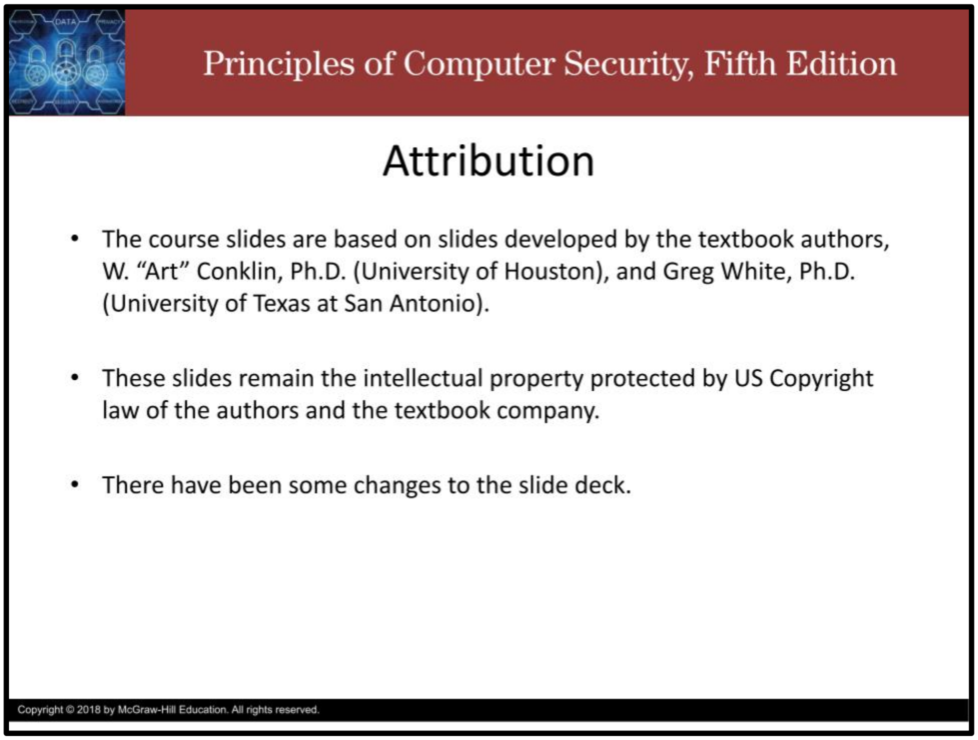
Qualitative vs. Quantitative Risk Assessment

- Purely quantitative risk management is impossible.
  - Purely qualitative is possible.
  - RM usually includes both.
- Which to use depends on project criticality, resources, and management
  - Influenced by degree to which risks can be quantified.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

It is generally accepted that it is impossible to conduct purely quantitative risk management. However, it is possible to accomplish purely qualitative risk management. Usually risk management includes both qualitative and quantitative elements, requiring both analysis and judgment or experience. The decision to use qualitative versus quantitative risk management depends on the criticality of the project, the resources available, and the management style. The decision will be influenced by the degree to which the fundamental risk management metrics can be quantified.

Slide 12



Principles of Computer Security, Fifth Edition

Attribution

- The course slides are based on slides developed by the textbook authors, W. “Art” Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.
- There have been some changes to the slide deck.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Thank you and take care.

Risk Management: Testing

Slide 1

Principles of Computer Security, Fifth Edition

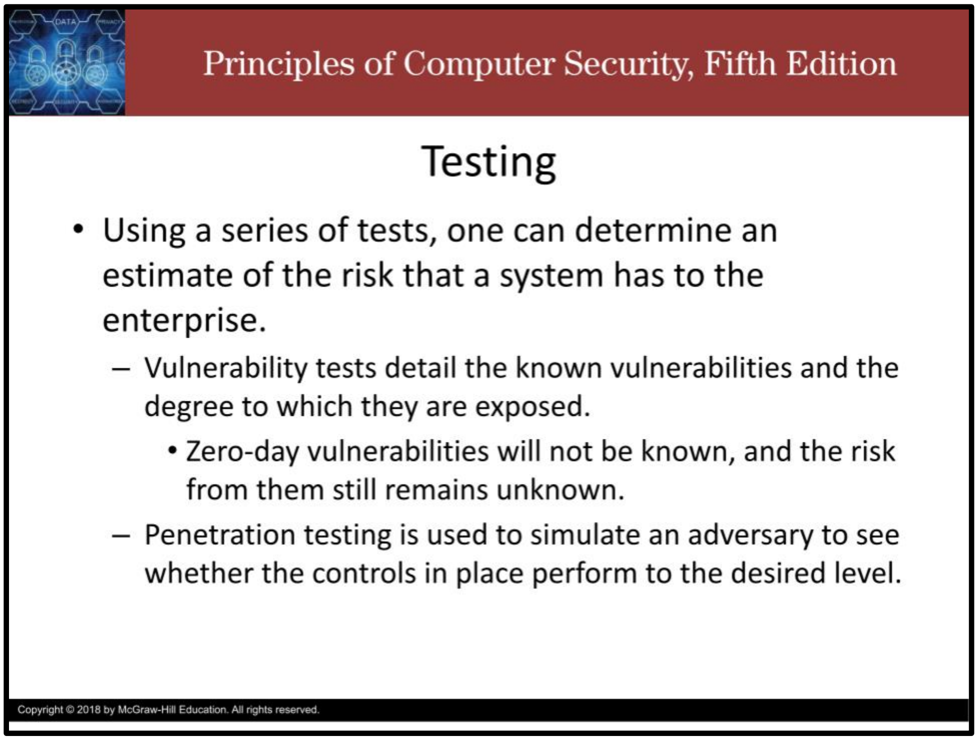
Risk Management

Testing

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Howdy! In this video, we discuss testing.

Slide 2



Principles of Computer Security, Fifth Edition

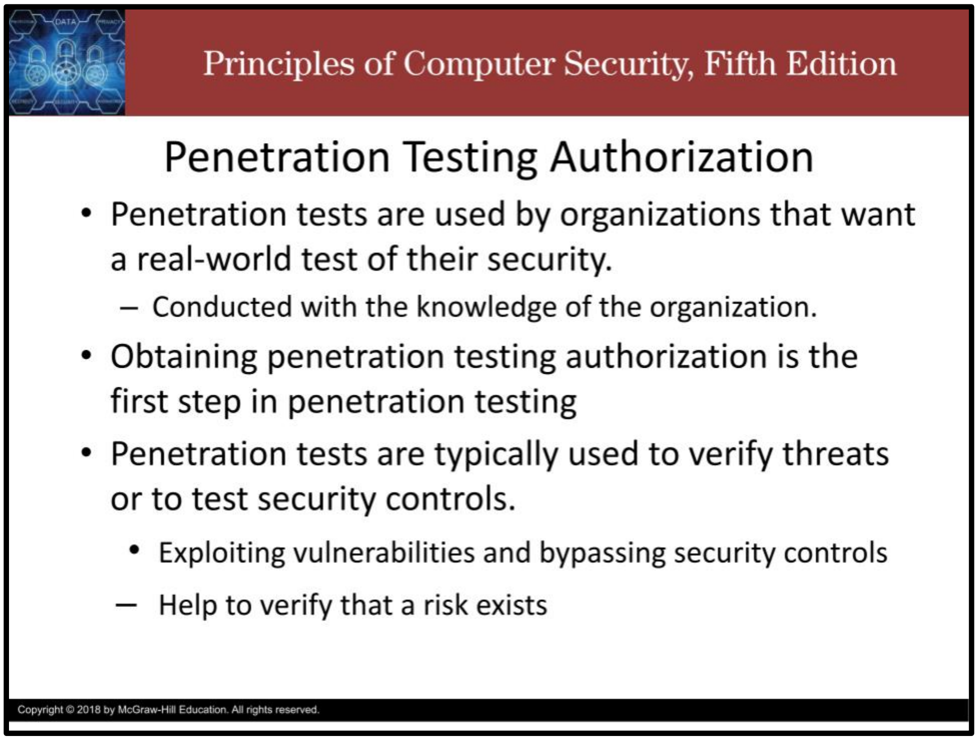
Testing

- Using a series of tests, one can determine an estimate of the risk that a system has to the enterprise.
  - Vulnerability tests detail the known vulnerabilities and the degree to which they are exposed.
    - Zero-day vulnerabilities will not be known, and the risk from them still remains unknown.
  - Penetration testing is used to simulate an adversary to see whether the controls in place perform to the desired level.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Understanding a system's risk exposure is no simple task. Using a series of tests, one can estimate the risks that a system poses to the enterprise. Vulnerability tests detail the known vulnerabilities and the degree to which they are exposed. By definition, zero-day vulnerabilities will not be known, and the risk from them will remain unknown. Penetration testing is used to simulate an adversary to see whether the controls in place perform to the desired level.

Slide 3



Principles of Computer Security, Fifth Edition

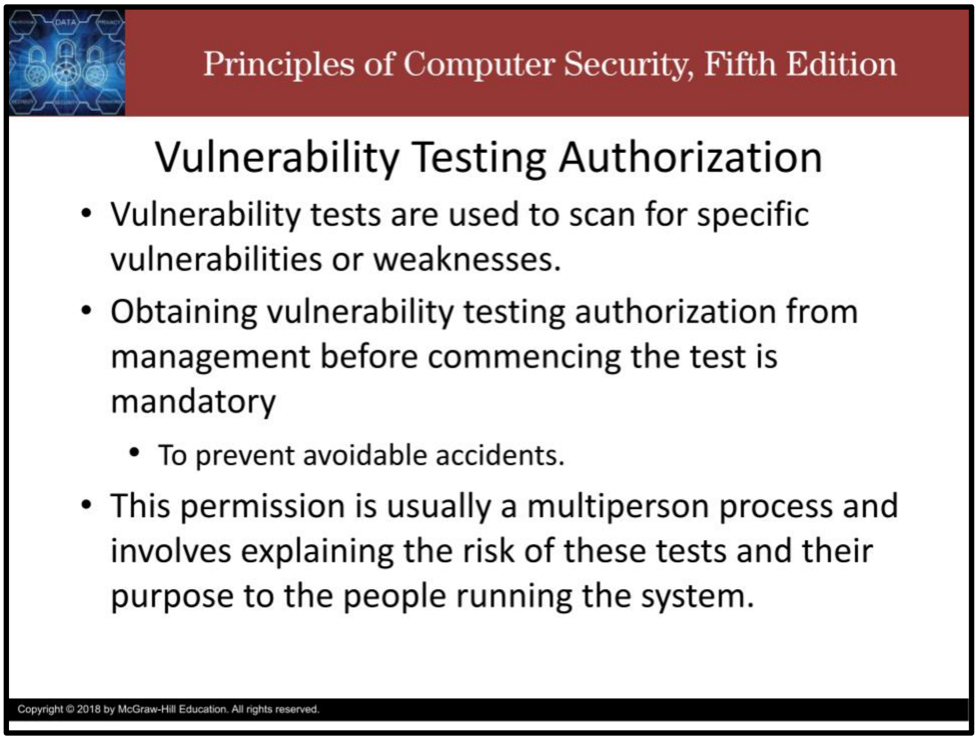
Penetration Testing Authorization

- Penetration tests are used by organizations that want a real-world test of their security.
  - Conducted with the knowledge of the organization.
- Obtaining penetration testing authorization is the first step in penetration testing
- Penetration tests are typically used to verify threats or to test security controls.
  - Exploiting vulnerabilities and bypassing security controls
  - Help to verify that a risk exists

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Penetration tests are used by organizations that want a real-world test of their security. Pen tests are always and only conducted with the knowledge of the organization. Obtaining authorization is the first step in pen testing. Pen tests are typically used to verify threats or to test security controls by exploiting vulnerabilities and bypassing security controls, and this helps to verify that a risk exists.

Slide 4



Principles of Computer Security, Fifth Edition

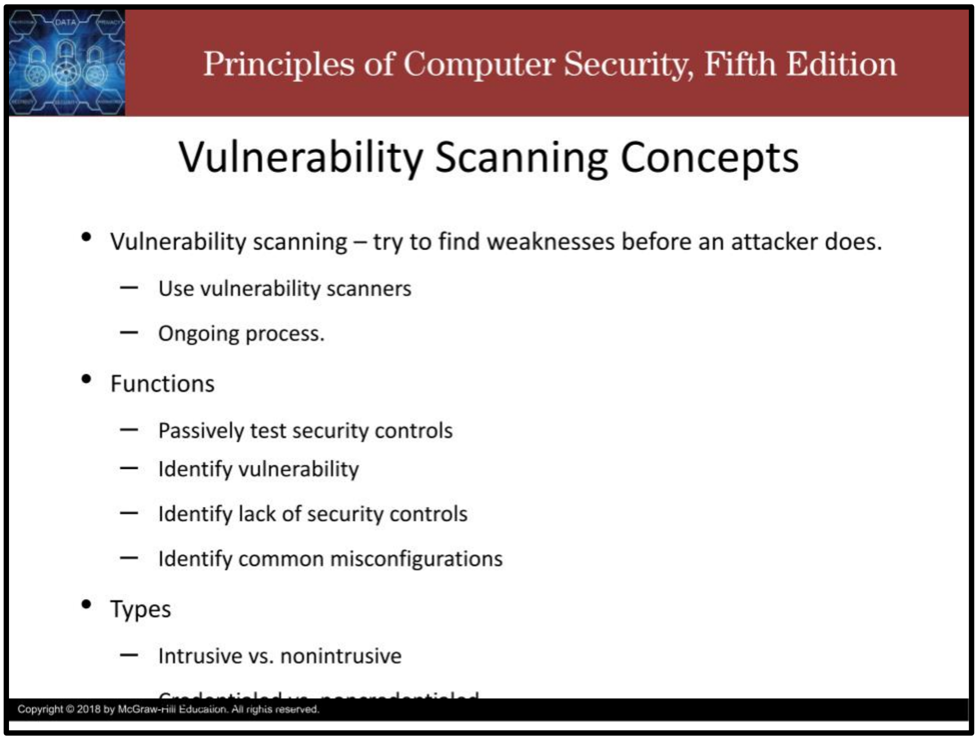
Vulnerability Testing Authorization

- Vulnerability tests are used to scan for specific vulnerabilities or weaknesses.
- Obtaining vulnerability testing authorization from management before commencing the test is mandatory
  - To prevent avoidable accidents.
- This permission is usually a multiperson process and involves explaining the risk of these tests and their purpose to the people running the system.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Vulnerability tests are used to scan for specific vulnerabilities or weaknesses. Obtaining vulnerability testing authorization from management before commencing the test is a mandatory step to prevent avoidable accidents. Authorization usually entails a multiperson process and involves explaining the risk of these tests and their purpose to the people running the system.

Slide 5



Principles of Computer Security, Fifth Edition

Vulnerability Scanning Concepts

- Vulnerability scanning – try to find weaknesses before an attacker does.
  - Use vulnerability scanners
  - Ongoing process.
- Functions
  - Passively test security controls
  - Identify vulnerability
  - Identify lack of security controls
  - Identify common misconfigurations
- Types
  - Intrusive vs. nonintrusive
  - Credentialed vs. noncredentialed

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Vulnerability scanning is the process of examining your systems and network devices for holes, weaknesses, and issues and finding them before a potential attacker does. Specialized tools called vulnerability scanners are designed to help administrators discover and address vulnerabilities. Most organizations look at vulnerability scanning as an ongoing process.

When an automated vulnerability scanner is used to examine a system, one of the side effects is the passive testing of security controls. We say passive testing because the target of the scanner is the system, not the controls. If the controls are effective, then the scan may report vulnerabilities that are not exploitable. (this is a good thing, but you need to be able to recognize such cases),

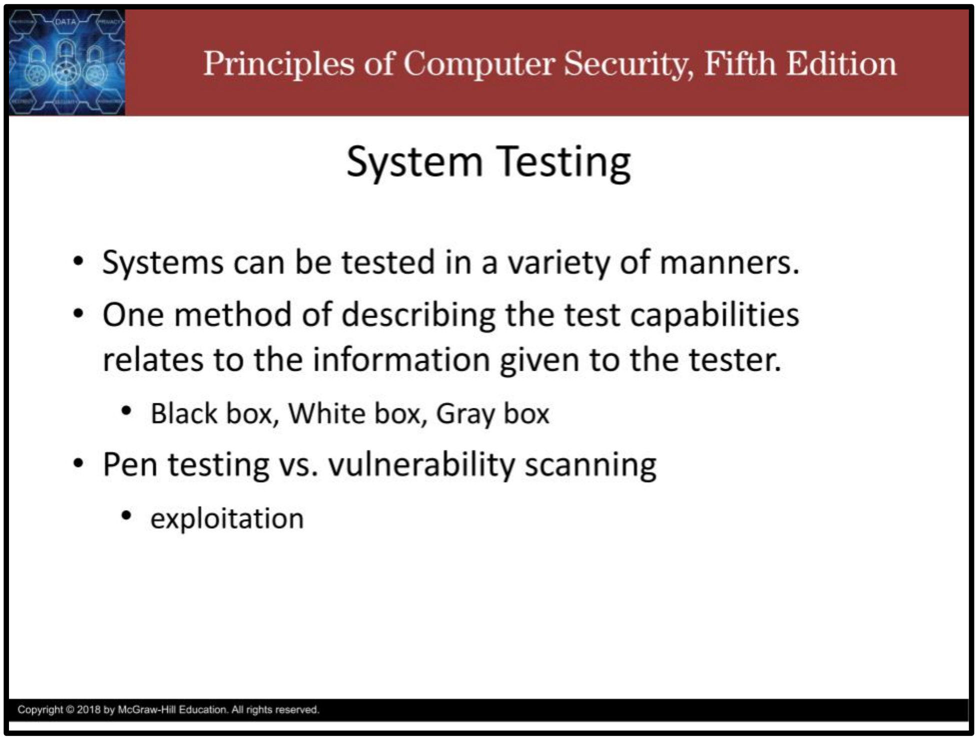
When a scanner finds a vulnerability, it logs which one and where it was found. An enumeration of the vulnerabilities identified is part of the vulnerability analysis report. Every vulnerability discovered by the scan should have a security control to protect against exploitation. Part of the function of the scan is to learn where controls are missing or ineffective. Vulnerability scanners can look for and report on common misconfigurations in systems, which could be sources or amplifiers of vulnerabilities.

In order to verify that a vulnerability is present and exploitable, scanners can perform either an intrusive or non-intrusive test. An intrusive test changes the state of the system. A nonintrusive test is less accurate but does not change the system's state. Nonintrusive tests are therefore preferred when scanning a live system.

Vulnerability scanners can be given authentication credentials so that they can have the same level of access as an authorized user. It is important to run both credentialed and noncredentialled scans to get a picture of what insiders can do and what outsiders can do.

Like any decision-making tool, vulnerability scanners can make mistakes. A false positive is an incorrect finding of a vulnerability which does not exist in the system. These are annoying since it takes time and effort to verify that it really was a false positive. A false negative is an incorrect finding, or rather an incorrect failure to find a vulnerability that does exist in the system but was not reported. These are the bigger problem since you cannot fix vulnerabilities that you cannot find and do now know about. One way to mitigate the risk of false negatives is to use several different vulnerability scanners and to employ pen testing teams to actively search for vulnerabilities.

Slide 6



Principles of Computer Security, Fifth Edition

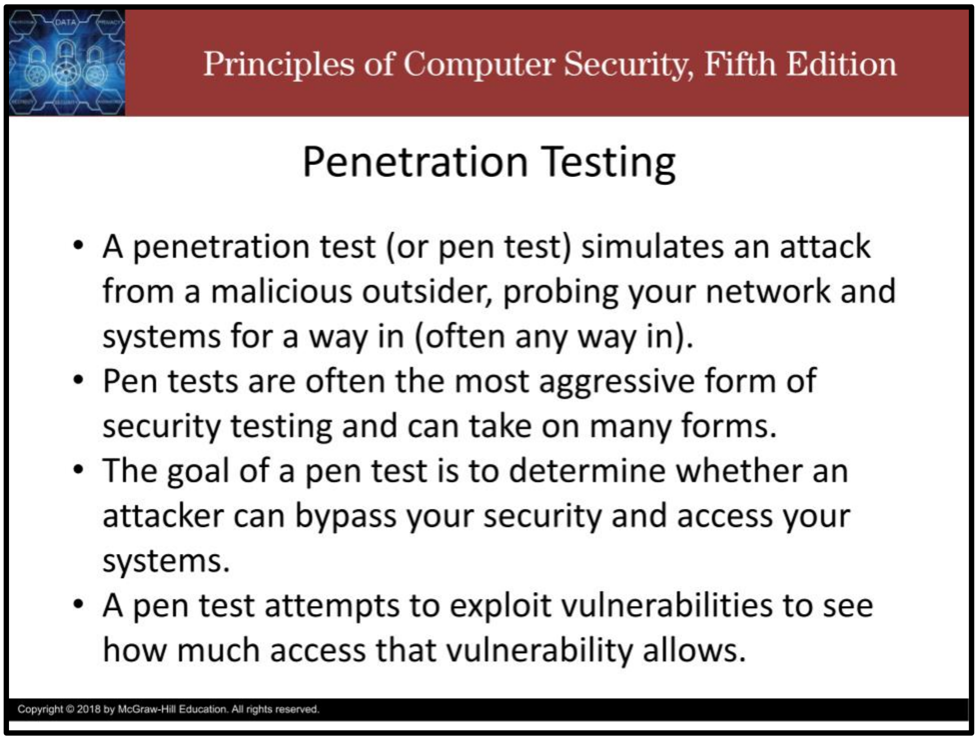
System Testing

- Systems can be tested in a variety of manners.
- One method of describing the test capabilities relates to the information given to the tester.
  - Black box, White box, Gray box
- Pen testing vs. vulnerability scanning
  - exploitation

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Systems can be tested in a variety of manners. One method of describing the test capabilities relates to the information given to the tester. In a black box test, the tester has no knowledge of how the system operates. In a white box test, the tester has complete knowledge of the system. Such as access to source code and binaries. In a gray box test, the tester has some incomplete knowledge of the system. Pen testing and vulnerability scanning are not synonymous. Vulnerability scanning is typically only part of a pen test. A pen test is an active exploration and, crucially, exploitation, of vulnerabilities.

Slide 7



Principles of Computer Security, Fifth Edition

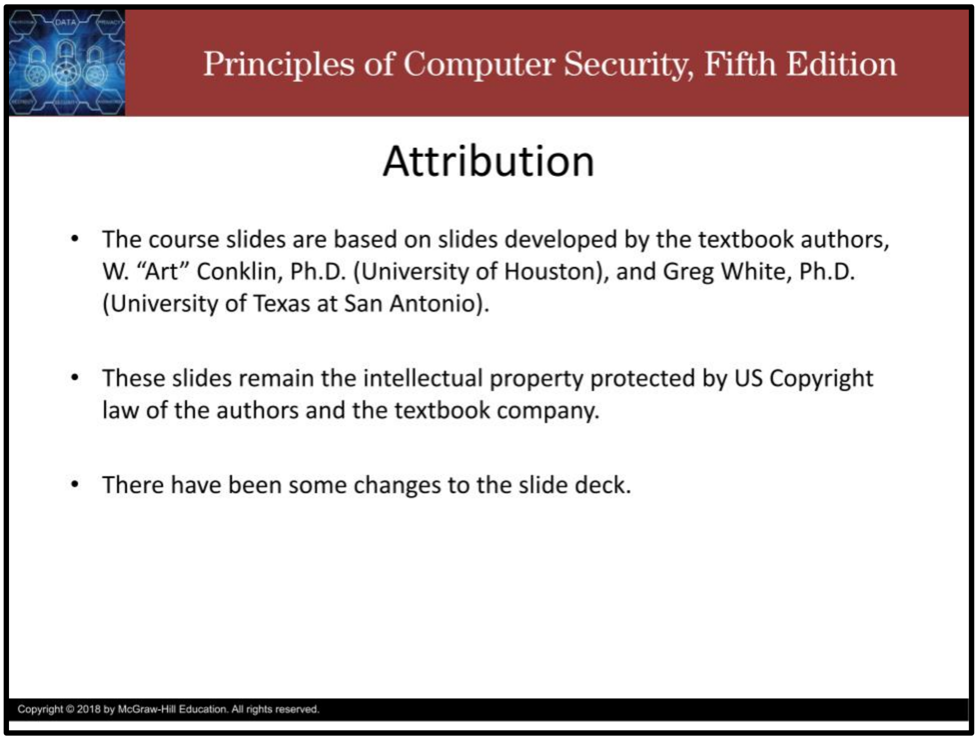
Penetration Testing

- A penetration test (or pen test) simulates an attack from a malicious outsider, probing your network and systems for a way in (often any way in).
- Pen tests are often the most aggressive form of security testing and can take on many forms.
- The goal of a pen test is to determine whether an attacker can bypass your security and access your systems.
- A pen test attempts to exploit vulnerabilities to see how much access that vulnerability allows.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

A penetration test (or pen test) simulates an attack from a malicious outsider, probing your network and systems for a way in (often any way in). Pen tests are often the most aggressive form of security testing and can take on many forms. The goal of a pen test is to determine whether an attacker can bypass your security and access your systems. A pen test attempts to exploit vulnerabilities to see how much access that vulnerability allows.

Slide 8



Principles of Computer Security, Fifth Edition

Attribution

- The course slides are based on slides developed by the textbook authors, W. “Art” Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.
- There have been some changes to the slide deck.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Thank you and take care.

Risk Management: Tools

Slide 1

Principles of Computer Security, Fifth Edition

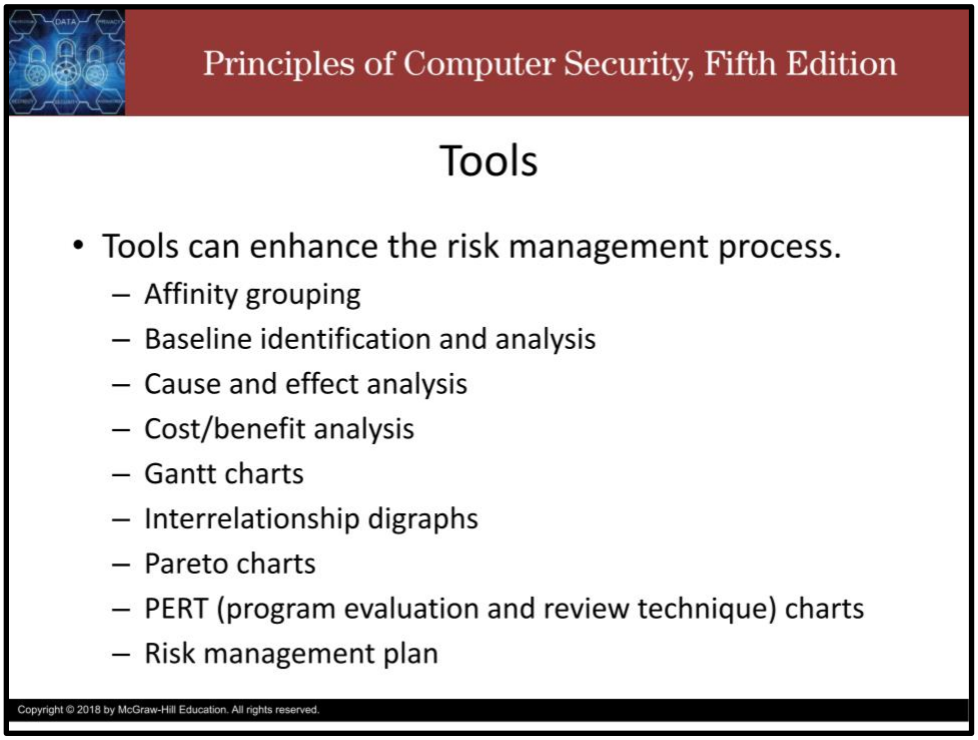
Risk Management

Tools

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Howdy! In this video, we introduce some tools that can be used for risk management.

Slide 2



Principles of Computer Security, Fifth Edition

Tools

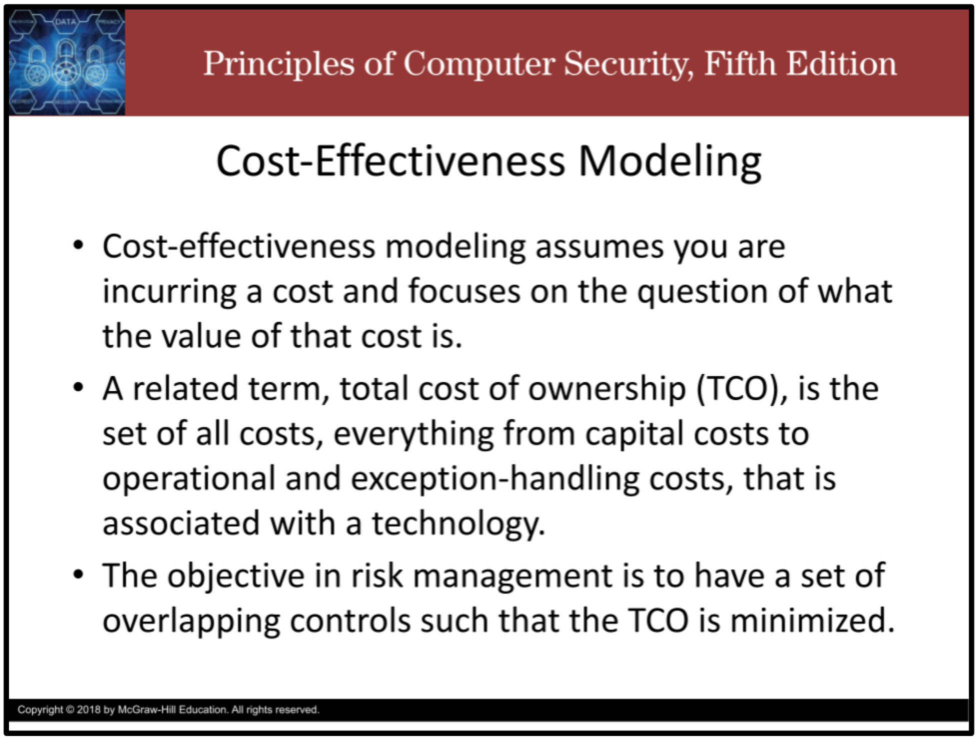
- Tools can enhance the risk management process.
    - Affinity grouping
    - Baseline identification and analysis
    - Cause and effect analysis
    - Cost/benefit analysis
    - Gantt charts
    - Interrelationship digraphs
    - Pareto charts
    - PERT (program evaluation and review technique) charts
    - Risk management plan

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

There are many tools that can enhance the risk management process.

Affinity grouping is A method of identifying items that are related and then identifying the principle that ties them together. **Baseline identification and analysis** is the process of establishing a baseline set of risks. It produces a "snapshot" of all the identified risks at a given point in time. **Cause and effect analysis** means Identifying relationships between a risk and the factors that can cause it. **Cost/benefit analysis** is a straightforward method for comparing cost estimates with the benefits of a mitigation strategy. **Gantt charts** are a management tool for diagramming schedules, events, and activity duration. **Interrelationship digraphs** are A method for identifying cause-and-effect relationships by clearly defining the problem to be solved, identifying the key elements of the problem, and then describing the relationships between each of the key elements. **Pareto charts** are histograms that rank the categories in a chart from most frequent to least frequent, thus facilitating risk prioritization. **PERT (program evaluation and review technique) charts** are diagrams depicting interdependencies between project activities, showing the sequence and duration of each activity. When complete, the chart shows the time necessary to complete the project and the activities that determine that time (the critical path). **Risk management plan** is A comprehensive plan documenting how risks will be managed on a given project. It contains processes, activities, milestones, organizations, responsibilities, and details of each major risk management activity and how it is to be accomplished. It is an integral part of the project management plan.

Slide 3



Principles of Computer Security, Fifth Edition

Cost-Effectiveness Modeling

- Cost-effectiveness modeling assumes you are incurring a cost and focuses on the question of what the value of that cost is.
- A related term, total cost of ownership (TCO), is the set of all costs, everything from capital costs to operational and exception-handling costs, that is associated with a technology.
- The objective in risk management is to have a set of overlapping controls such that the TCO is minimized.

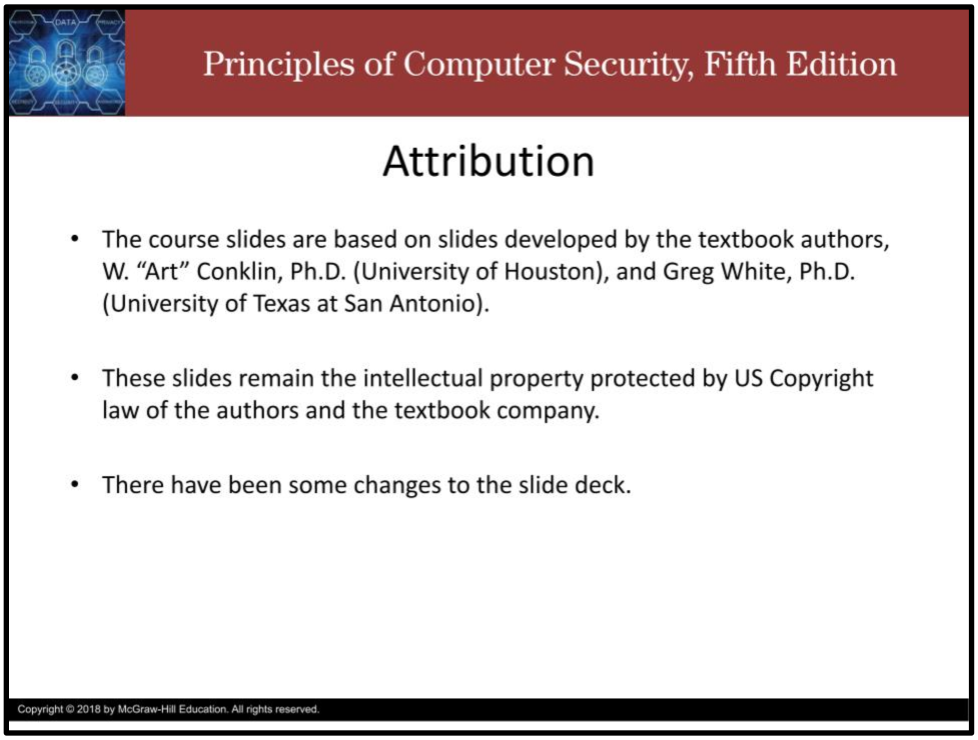
Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Cost-effectiveness modeling assumes you are incurring a cost and focuses on the question of what the value of that cost is. This is a rational means of economic analysis used to determine the utility of a specific strategy. It is a nearly foregone conclusion you will be spending resources on security; this just reframes the question to one of utility and outcome from the activity.

A related term, total cost of ownership (TCO), is the set of all costs, everything from capital costs to operational and exception-handling costs, that is associated with a technology. There are a lot of arguments over how to calculate TCO, typically to favor one solution over another, but that is not important in this instance. It is important to note the differences between normal operational costs and exception handling. Exception handling is always more expensive.

The objective in risk management is to have a set of overlapping controls such that the TCO is minimized. This means that the solution has a measured effectiveness across the risk spectrum and that exceptions are minimalized. This is where the compliance versus security debate becomes interesting. We establish compliance rules for a variety of reasons, but once established, their future effectiveness depends upon the assumption that the same risk environment exists as when they were created. Should the risk, the value, or the impact change over time, the cost effectiveness of the compliance-directed control can shift, frequently in a negative fashion.

Slide 4



Principles of Computer Security, Fifth Edition

Attribution

- The course slides are based on slides developed by the textbook authors, W. "Art" Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.
- There have been some changes to the slide deck.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Thank you and take care.

Risk Management: Best Practices

Slide 1

Principles of Computer Security, Fifth Edition

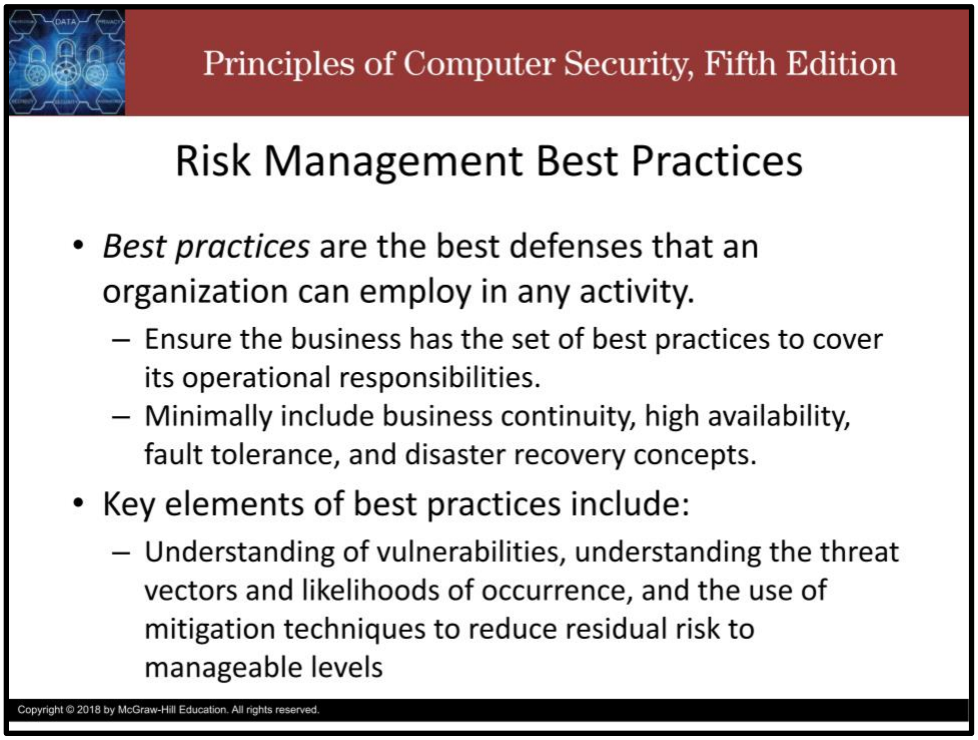
Risk Management

Risk Management Best Practices

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Howdy! In this video, we introduce some risk management best practices.

Slide 2



Principles of Computer Security, Fifth Edition

Risk Management Best Practices

- *Best practices* are the best defenses that an organization can employ in any activity.
  - Ensure the business has the set of best practices to cover its operational responsibilities.
  - Minimally include business continuity, high availability, fault tolerance, and disaster recovery concepts.
- Key elements of best practices include:
  - Understanding of vulnerabilities, understanding the threat vectors and likelihoods of occurrence, and the use of mitigation techniques to reduce residual risk to manageable levels

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

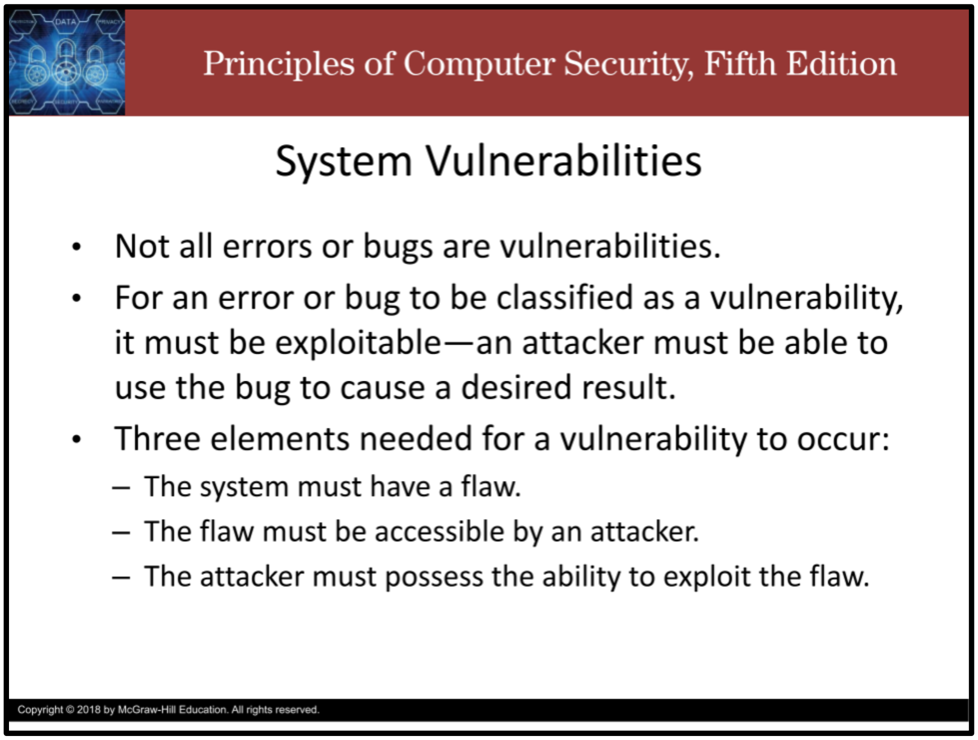
Best practices are the best defenses that an organization can employ in any activity.

One manner of examining best practices is to ensure that the business has the set of best practices to cover its operational responsibilities. At a deeper level, the details of these practices need to themselves be best practices if one is to get the best level of protection. At a minimum, risk mitigation best practices include business continuity, high availability, fault tolerance, and disaster recovery concepts.

None of these operate in isolation. In fact, they are all interconnected, sharing elements as they all work together to achieve a common purpose: the security of the data in the enterprise, which is measured in terms of risk exposure.

Key elements of best practices include understanding of vulnerabilities, understanding the threat vectors and likelihoods of occurrence, and the use of mitigation techniques to reduce residual risk to manageable levels.

Slide 3



Principles of Computer Security, Fifth Edition

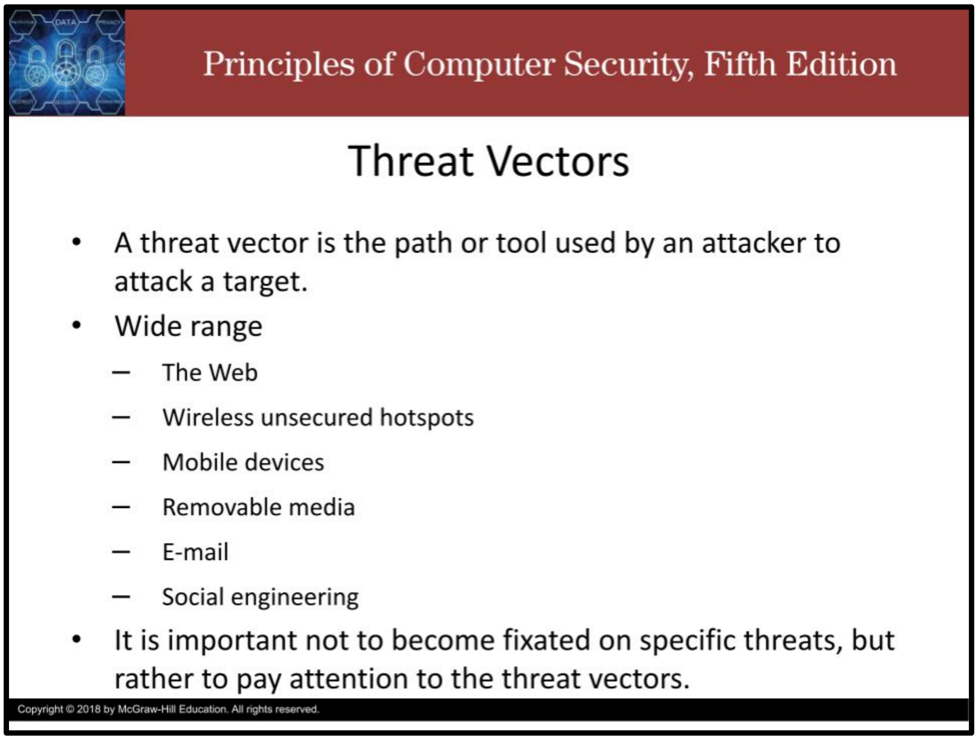
System Vulnerabilities

- Not all errors or bugs are vulnerabilities.
- For an error or bug to be classified as a vulnerability, it must be exploitable—an attacker must be able to use the bug to cause a desired result.
- Three elements needed for a vulnerability to occur:
  - The system must have a flaw.
  - The flaw must be accessible by an attacker.
  - The attacker must possess the ability to exploit the flaw.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

All systems have flaws. Every vulnerability is a flaw. But, not all flaws are vulnerabilities. For a flaw to be classified as a vulnerability, it must be exploitable. Vulnerabilities can exist in many levels and from many causes, such as design errors, coding errors, or unintended and untested interactions in complex systems. Vulnerabilities can exist in software, hardware, procedures. No matter why or where the vulnerability is, the result is the same: an exploitable weakness that increases the level of risk associated with the system.

Slide 4



Principles of Computer Security, Fifth Edition

Threat Vectors

- A threat vector is the path or tool used by an attacker to attack a target.
- Wide range
  - The Web
  - Wireless unsecured hotspots
  - Mobile devices
  - Removable media
  - E-mail
  - Social engineering
- It is important not to become fixated on specific threats, but rather to pay attention to the threat vectors.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

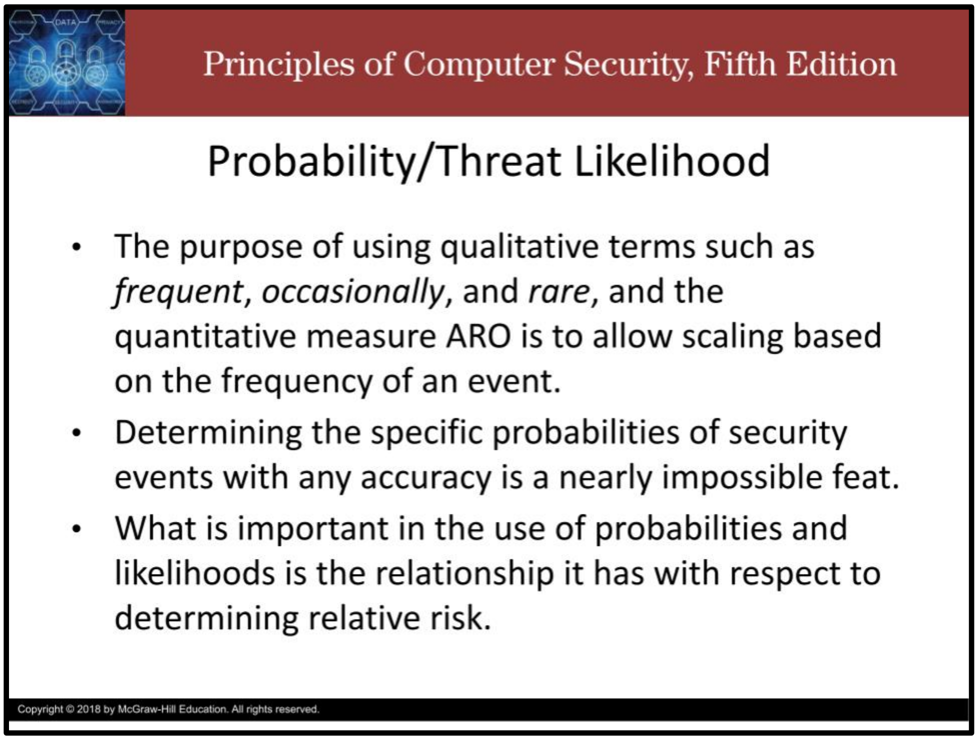
A threat vector is the path or tool used by an attacker to attack a target

There is a wide range of threat vectors that a security professional needs to understand:

- The Web (fake sites, session hijacking, malware, watering hole attacks)
- Wireless unsecured hotspots
- Mobile devices (iOS/Android)
- USB (removable) media
- E-mail (links, attachments, malware)
- Social engineering (deceptions, hoaxes, scams, and fraud)

This listing is merely a sample of threat vectors. From a defensive point of view, it is important not to become fixated on specific threats, but rather to pay attention to the threat vectors. If a user visits a web site that has malicious code, then the nature of the code, although important from a technical view in one respect, is not the primary concern. The primary issue is the malicious site, as this is the threat vector.

Slide 5



Principles of Computer Security, Fifth Edition

Probability/Threat Likelihood

- The purpose of using qualitative terms such as *frequent*, *occasionally*, and *rare*, and the quantitative measure ARO is to allow scaling based on the frequency of an event.
- Determining the specific probabilities of security events with any accuracy is a nearly impossible feat.
- What is important in the use of probabilities and likelihoods is the relationship it has with respect to determining relative risk.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

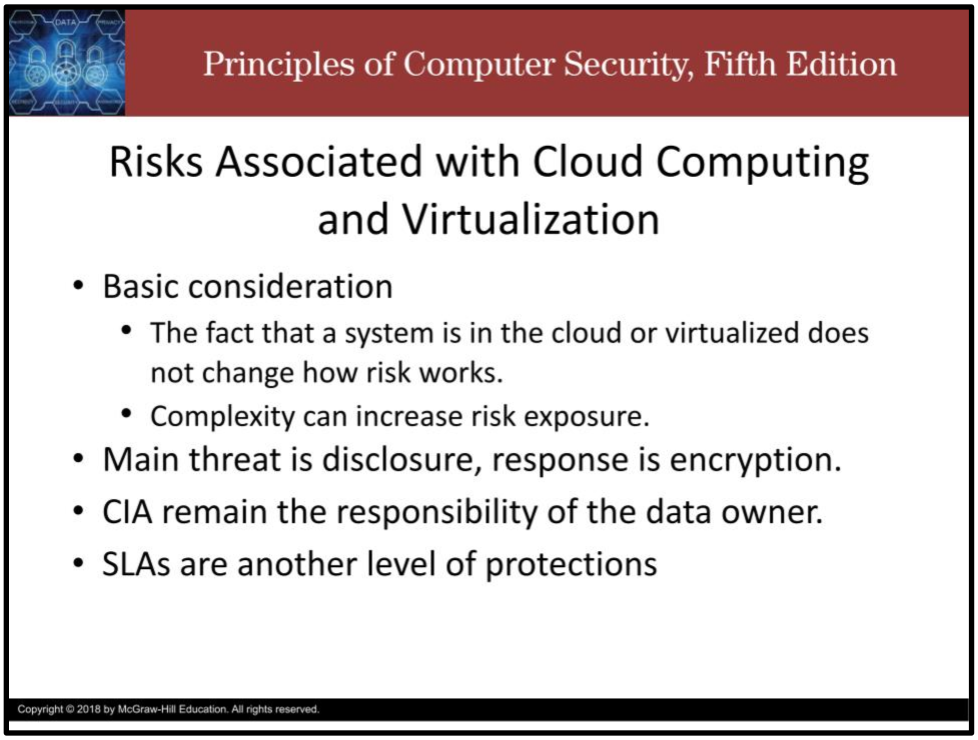
The purpose of using qualitative terms such as *frequent*, *occasionally*, and *rare*, and the quantitative measure ARO is to allow scaling based on the frequency of an event.

Accurately determining the specific probabilities of security events is a nearly impossible feat.
What is important in the use of probabilities and likelihoods is the relationship it has with respect to determining relative risk.

Just as an insurance company cannot tell you when you will have an accident, no one can predict when a security event will occur. What can be determined is that over some course of time—say, the next year—a significant number of users will click malicious links in e-mails. The threat likelihood of different types of attacks will change over time. Years ago, web defacements were all the rage. Today, spear phishing is more prevalent.

When examining risk, the probability or threat likelihood plays a significant role in the determination of risk and mitigation options. In many cases, the likelihood is treated as certain, and for repeat attacks, this may be appropriate, but it certainly is not universally true.

Slide 6



Principles of Computer Security, Fifth Edition

Risks Associated with Cloud Computing and Virtualization

- Basic consideration
  - The fact that a system is in the cloud or virtualized does not change how risk works.
  - Complexity can increase risk exposure.
- Main threat is disclosure, response is encryption.
- CIA remain the responsibility of the data owner.
- SLAs are another level of protections

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

When examining a complex system such as a cloud or virtual computing environment from a risk perspective, several basic considerations always need to be observed. First, the fact that a system is either in the cloud or virtualized does not change how risk works. Risk is everywhere, and changing a system to a new environment does not change the fact that there are risks.

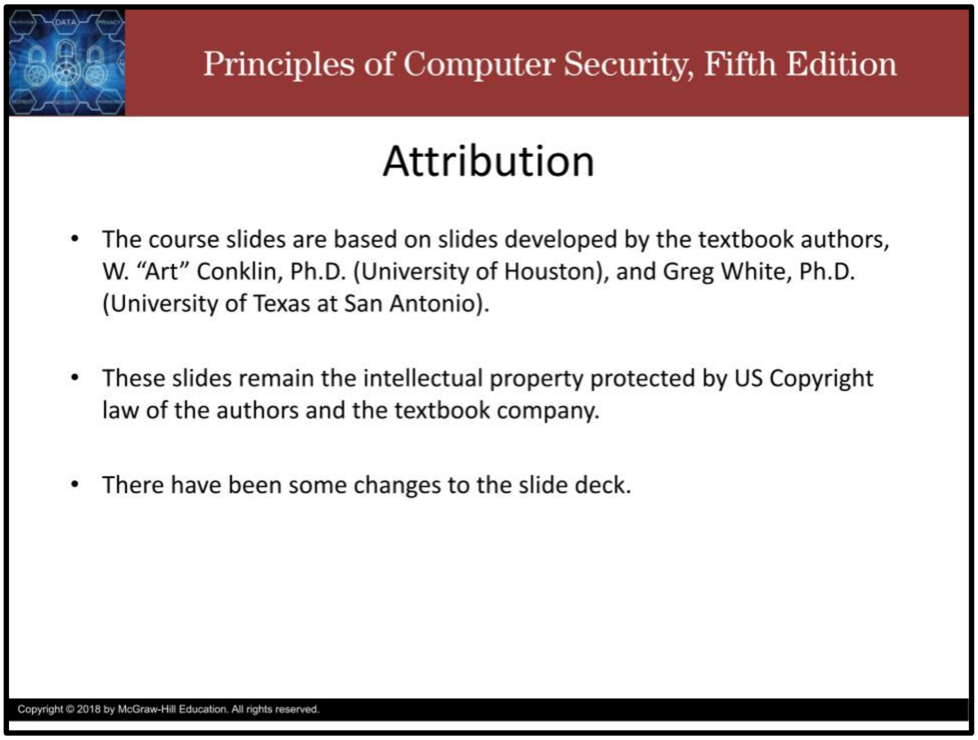
Second, complexity can increase risk exposure. There are specific risks associated with both virtualization and cloud environments. Having data and computing occur in environments that are not under the direct control of the data owner adds both a layer of complexity and a degree of risk. The potential for issues with confidentiality, integrity, and availability increases with the loss of direct control over the environment. The virtualization and cloud layers also present new avenues of attack into a system.

Security is a particular challenge when data and computation are handled by a remote party, as in cloud computing. The specific challenge is how to allow data outside your enterprise and yet remain in control over the use of the data. The common answer is encryption. Through the proper use of encryption of data before it leaves the enterprise, external storage can still be performed securely by properly employing cryptographic elements.

The security requirements associated with confidentiality, integrity, and availability remain the responsibility of the data owner, and measures must be taken to ensure that these requirements are met, regardless of the location or usage associated with the data.

Another level of protections is through the use of service level agreements (SLAs) with the cloud vendor, although these frequently cannot offer much remedy in the event of data loss.

Slide 7



Principles of Computer Security, Fifth Edition

Attribution

- The course slides are based on slides developed by the textbook authors, W. “Art” Conklin, Ph.D. (University of Houston), and Greg White, Ph.D. (University of Texas at San Antonio).
- These slides remain the intellectual property protected by US Copyright law of the authors and the textbook company.
- There have been some changes to the slide deck.

Copyright © 2018 by McGraw-Hill Education. All rights reserved.

Thank you and take care.