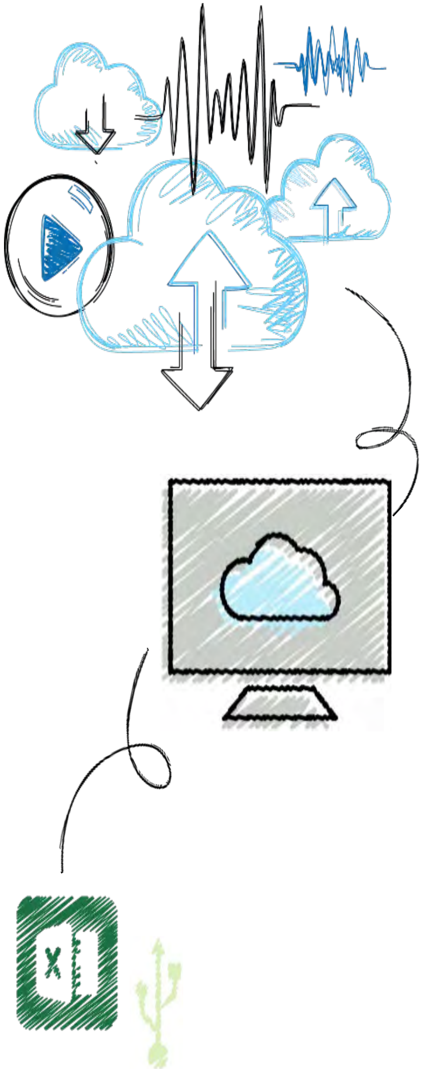
CompTIA Security+

Chapter 15

Risk Mitigation



Objectives

15.1 Explain how to manage risk

15.2 Describe strategies for reducing risk

15.3 List practices for mitigating risk

15.4 Describe common security issues

Managing Risk

- Risk
  - A situation that involves exposure to some type of danger
- Managing risk
  - To create a level of protection that mitigates the vulnerabilities to the threats and reduces the potential consequences
  - Involves:
    - Knowing what threats are being faced
    - Assessing those risks

Threat Assessment (1 of 3)

- Threat assessment
  - A formal process of examining the seriousness of a potential threat as well as the likelihood that it will be carried out
- Three categories of threats:
  - Environmental
  - Manmade
  - Internal vs. external

Threat Assessment (2 of 3)

Threat category	Description	Example
Strategic	Action that affects the long-term goals of the organization	Theft of intellectual property, not pursuing a new opportunity, loss of a major account, competitor entering the market
Compliance	Following (or not following) a regulation or standard	Breach of contract, not responding to the introduction of new laws
Financial	Impact of financial decisions or market factors	Increase in interest rates, global financial crisis
Operational	Events that impact the daily business of the organization	Fire, hazardous chemical spill, power blackout
Technical	Events that affect information technology systems	Denial of service attack, SQL injection attack, virus
Managerial	Actions related to the management of the organization	Long-term illness of company president, key employee resigning

Threat Assessment (3 of 3)

- A threat assessment should be used to determine the asset value
  - Relative worth of an asset that is at risk
- Supply chain assessment
  - Supply chain – a network that moves a product from the supplier to the customer
  - Should be viewed as assets to the enterprise and their threats should be cataloged
- Assessing threats is not always a straightforward exercise

Risk Assessment

- Risk assessment involves:
  - Testing
  - Change management
  - Privilege management
  - Incident management
  - Risk calculations
  - Representing risk information

Testing (1 of 2)

- Technology assets should be tested to identify any vulnerabilities
  - Involves an automated software vulnerability scan through a system
- Intrusive vulnerability scan
  - Attempts to actually penetrate the system to perform a simulated attack
- Non-intrusive vulnerability scan
  - Uses only available information to hypothesize the status of the vulnerability
- Penetration test (pentest)
  - Designed to exploit any weaknesses in systems that are vulnerable
  - Penetration testing authorization should be obtained

Testing (2 of 2)

- Reasons authorization should be obtained:
  - Legal authorization
  - Indemnification
  - Limit retaliation

Change Management (1 of 2)

- Change management
  - Methodology for making modifications and keeping track of changes
  - Ensures proper documentation of changes so future changes have less chance of creating a vulnerability
  - Involves all types of changes to information systems
- Two major types of changes that need proper documentation
  - Changes to system architecture
  - Changes to file or document classification

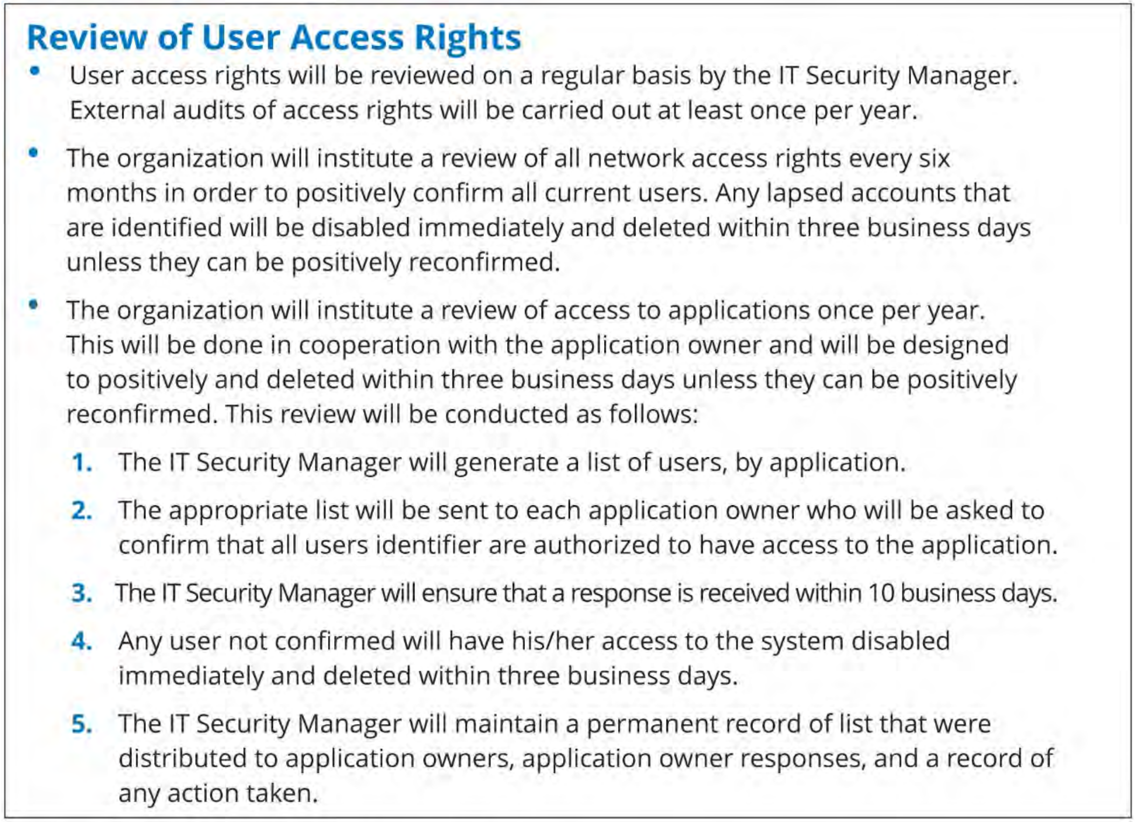
Change Management (2 of 2)

- Change management team (CMT)
  - Body responsible for overseeing the changes
  - Composed of representatives from all areas of IT, network security, and upper management
  - Proposed changes must first be approved by CMT
- CMT duties
  - Review proposed changes
  - Ensure risk and impact of planned change are understood
  - Recommend approval, disapproval, deferral, or withdrawal of a requested change
  - Communicate proposed and approved changes to coworkers

Privilege Management (1 of 2)

- Privilege
  - Subject’s access level over an object, such as a file
- Privilege management
  - Process of assigning and revoking privileges to objects
- Privilege auditing
  - Periodically reviewing a subject’s privileges over an object
  - Objective: determine if subject has the correct privileges

Privilege Management (2 of 2)



Review of User Access Rights

- User access rights will be reviewed on a regular basis by the IT Security Manager. External audits of access rights will be carried out at least once per year.
- The organization will institute a review of all network access rights every six months in order to positively confirm all current users. Any lapsed accounts that are identified will be disabled immediately and deleted within three business days unless they can be positively reconfirmed.
- The organization will institute a review of access to applications once per year. This will be done in cooperation with the application owner and will be designed to positively and deleted within three business days unless they can be positively reconfirmed. This review will be conducted as follows:
    1. The IT Security Manager will generate a list of users, by application.
    2. The appropriate list will be sent to each application owner who will be asked to confirm that all users identifier are authorized to have access to the application.
    3. The IT Security Manager will ensure that a response is received within 10 business days.
    4. Any user not confirmed will have his/her access to the system disabled immediately and deleted within three business days.
    5. The IT Security Manager will maintain a permanent record of list that were distributed to application owners, application owner responses, and a record of any action taken.

Figure 15-1 Sample user access rights review

Incident Management

- Incident response
  - Components required to identify, analyze, and contain an incident
- Incident handling
  - Planning, coordination, communications, and planning functions needed to resolve incident
- Incident management
  - The “framework” and functions required to enable incident response and incident handling within an organization
  - Objective: To restore normal operations as quickly as possible with least impact to business or users

Risk Calculation (1 of 6)

- Two approaches to risk calculation:
  - Qualitative risk calculation - uses an “educated guess” based on observation
    - Typically assigns a numeric value (1-10) or label (High, Medium, or Low) that represents the risk
  - Quantitative risk calculation - attempts to create “hard” numbers associated with the risk of an element in a system by using historical data
    - Can be divided into the likelihood of a risk and the impact of a risk being successful

Risk Calculation (2 of 6)

- Risk Likelihood
  - Several quantitative tools can be used to predict the likelihood of the risk
    - Mean Time Between Failure (MTBF)
    - Mean Time To Recovery (MTTR)
    - Mean Time To Failure (MTTF)
    - Failure In Time (FIT)
  - Historical data can be used to determine the likelihood of a risk occurring within a year
    - Known as Annualized Rate of Occurrence (ARO)

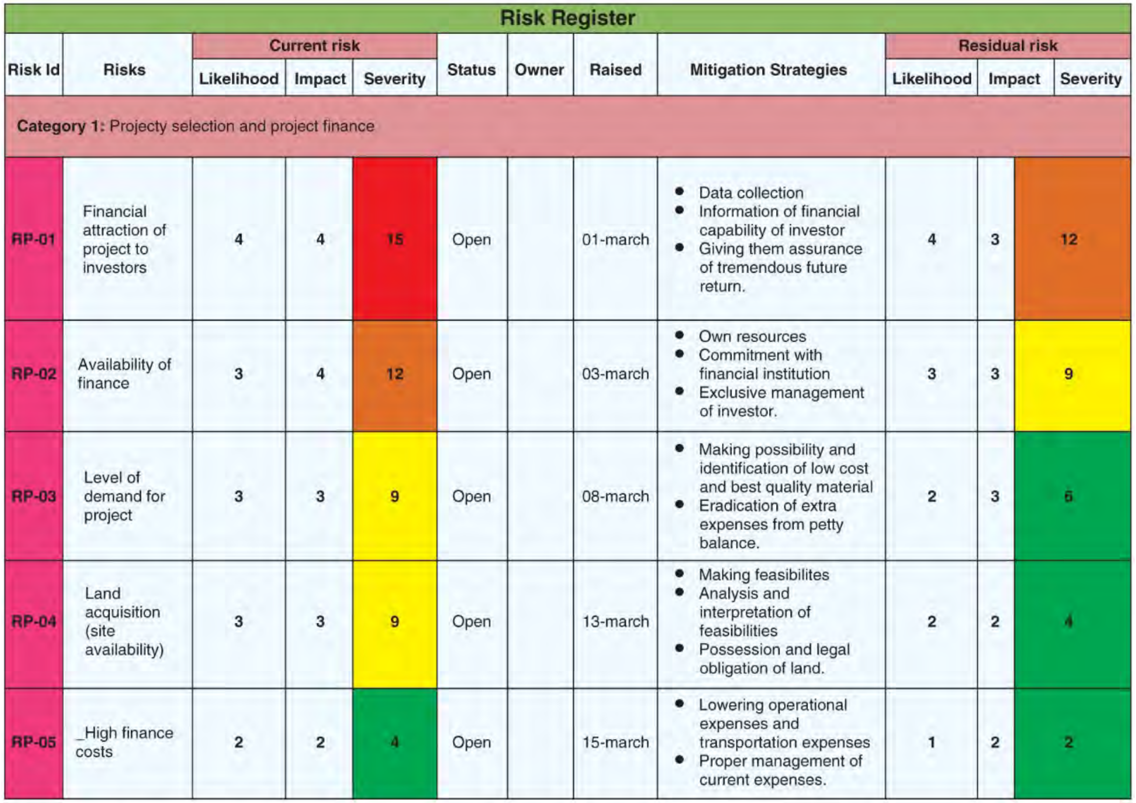
Risk Calculation (3 of 6)

Source	Explanation
Police departments	Crime statistics on the area of facilities to determine the probability of vandalism, break-ins, or dangers potentially encountered by personnel
Insurance companies	Risks faced by other companies and the amounts paid out when these risks became reality
Computer incident monitoring organization	Data regarding a variety of technology-related risks, failures, and attacks

Risk Calculation (4 of 6)

- Risk Impact
  - Comparing the monetary loss associated with an asset in order to determine the amount of money that would be list if the risk occurred
  - Two risk calculation formulas are used to calculate expected losses:
    - Single Loss Expectancy (SLE) - expected monetary loss every time a risk occurs
    - Annualized Loss Expectancy (ALE) - expected monetary loss that can be expected for an asset due to risk over a one-year period
- Representing Risks
  - Risk register – a list of potential threats and associated risks
  - Risk matrix – a visual color-coded tool that lists the impact and likelihood of risks

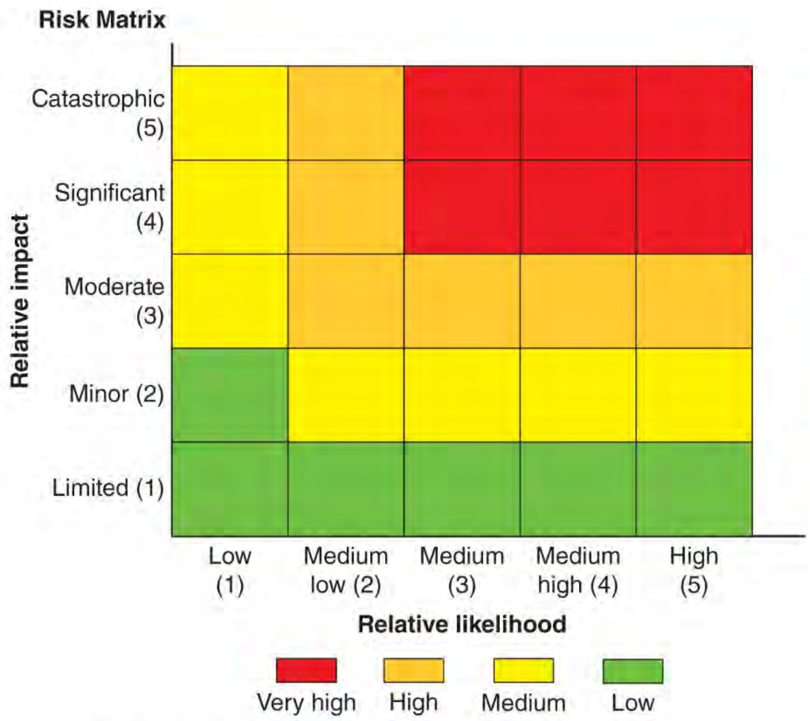
Risk Calculation (5 of 6)



Risk Register											
Risk Id	Risks	Current risk			Status	Owner	Raised	Mitigation Strategies	Residual risk		
		Likelihood	Impact	Severity					Likelihood	Impact	Severity
Category 1: Projecty selection and project finance											
RP-01	Financial attraction of project to investors	4	4	15	Open		01-march	• Data collection • Information of financial capability of investor • Giving them assurance of tremendous future return.	4	3	12
RP-02	Availability of finance	3	4	12	Open		03-march	• Own resources • Commitment with financial institution • Exclusive management of investor.	3	3	9
RP-03	Level of demand for project	3	3	9	Open		08-march	• Making possibility and identification of low cost and best quality material • Eradication of extra expenses from petty balance.	2	3	6
RP-04	Land acquisition (site availability)	3	3	9	Open		13-march	• Making feasibilites • Analysis and interpretation of feasibilities • Possession and legal obligation of land.	2	2	4
RP-05	_High finance costs	2	2	4	Open		15-march	• Lowering operational expenses and transportation expenses • Proper management of current expenses.	1	2	2

Figure 15-2 Risk register

Risk Calculation (6 of 6)



Risk Matrix

Relative impact	Low (1)	Medium low (2)	Medium (3)	Medium high (4)	High (5)
Catastrophic (5)	🟨	🟧	🟥	🟥	🟥
Significant (4)	🟨	🟧	🟥	🟥	🟥
Moderate (3)	🟨	🟧	🟧	🟧	🟧
Minor (2)	🟩	🟨	🟨	🟨	🟨
Limited (1)	🟩	🟩	🟩	🟩	🟩

Relative likelihood

🟥 Very high 🟧 High 🟨 Medium 🟩 Low

Figure 15-3 Risk matrix

Strategies for Reducing Risk

- Approaches for reducing risk:
  - Using control types
  - Distributing allocation
  - Implementing automation

Using Control Types (1 of 2)

- Security control
  - Any device or process that is used to reduce risk
- Two levels of security controls:
  - Administrative controls – processes for developing and ensuring that policies and procedures are carried out
  - Technical controls – security controls carried out or managed by devices

Using Control Types (2 of 2)

- Subtypes of controls that can be either technical or administrative:
  - Deterrent controls
  - Preventative controls
  - Physical controls
  - Detective controls
  - Compensating controls
  - Corrective controls

Distributing Allocation

- Distributive allocation refers to “spreading” the risk
- Ways to distribute risk include:
    - Transference - makes a third party responsible for the risk
    - Risk avoidance - involves identifying the risk and making the decision to not engage in the activity
    - Mitigation - the attempt to address the risk by making it less serious

Implementing Technology

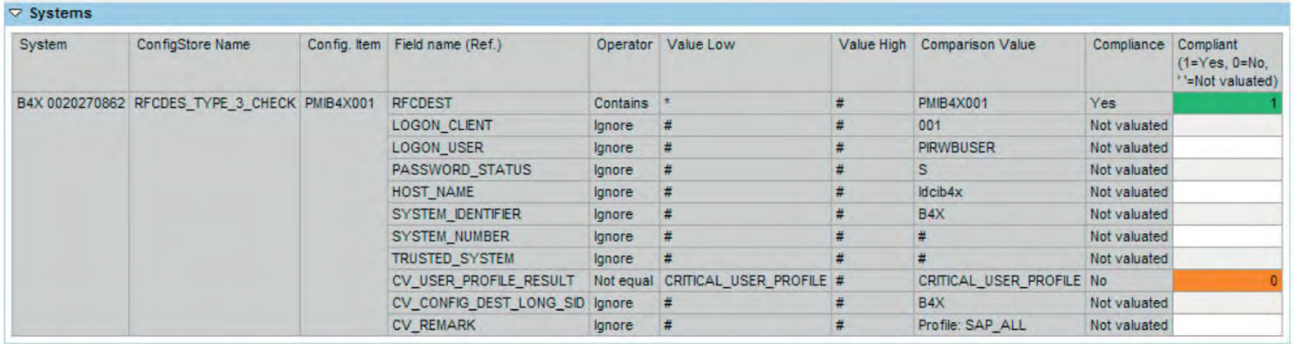
- Risk is often introduced through human error
- Using technology as a strategy for reducing risk can minimize these errors
- Implementing technology involves using:
  - Automation
  - Images and templates
  - Non-persistence tools

Automation (1 of 2)

- **Automation**
  - Can be defined as that which replaces human physical activity
- **Automated courses of action**
  - Using technology to automate IT processes
- It automation can provide:
  - **Scalability -** the ability to continue to function as the size or volume of the enterprise data center expands to meet the growing demands
  - **Elasticity** – the ability to revert to its former size after expanding
  - **Continuous monitoring** – sustained and continual surveillance

Automation (2 of 2)

- **Secure configuration guides** – available to help IT security personnel configure hardware devices and software to repel attacks
  - Vendor-specific guides – useful for configuring web servers, OSs, application servers, and network infrastructure devices
- Configuration validation
  - Reviewing the configuration of systems to determine if security settings are correct



▽ Systems

System	ConfigStore Name	Config. Item	Field name (Ref.)	Operator	Value Low	Value High	Comparison Value	Compliance	Compliant (1=Yes, 0=No, ' '=Not valuated)
B4X 0020270862	RFCDES_TYPE_3_CHECK	PMIB4X001	RFCDEST	Contains	*	#	PMIB4X001	Yes	1
			LOGON_CLIENT	Ignore	#	#	001	Not valuated	
			LOGON_USER	Ignore	#	#	PIRWBUSER	Not valuated	
			PASSWORD_STATUS	Ignore	#	#	S	Not valuated	
			HOST_NAME	Ignore	#	#	ldcib4x	Not valuated	
			SYSTEM_IDENTIFIER	Ignore	#	#	B4X	Not valuated	
			SYSTEM_NUMBER	Ignore	#	#	#	Not valuated	
			TRUSTED_SYSTEM	Ignore	#	#	#	Not valuated	
			CV_USER_PROFILE_RESULT	Not equal	CRITICAL_USER_PROFILE	#	CRITICAL_USER_PROFILE	No	0
			CV_CONFIG_DEST_LONG_SID	Ignore	#	#	B4X	Not valuated	
			CV_REMARK	Ignore	#	#	Profile: SAP_ALL	Not valuated	

Figure 15-4 Configuration validation report

Source: SAP

Images and Templates

- **Master image**
  - A copy of a properly configured and secured computer software system that can be replicated to other computers
  - Eliminates the need for configuring individualized security settings
- **Template**
  - A type of document in which the standardized content has already been created
  - The user needs only to enter specialized and variable components
  - Reduces the amount of data to be entered and helps minimize errors that could introduce a risk

Non-Persistence Tools

- Non-persistence tools – used to ensure that unwanted data is not carried forward (clean image is used)

Tool name	Description	How used
Live boot media	A “lightweight” bootable image on a USB flash drive or optical media	Temporarily creates a secure, non-persistent client for use on a public computer for accessing a secure remote network
Revert to a known state	Restore device to a previous secure condition	Used to reset a device to a stable and secure setting
Rollback to known configuration	Undo recent changes that cause errors or weaken security	Can restore a device to a previous configuration
Snapshot	An instance (image) of a virtual machine	Used to replace a corrupted or infected virtual machine

Practicing for Reducing Risk

- Practices for reducing risk:
  - Security policies
  - Awareness and training
  - Agreements
  - Personnel management

Security Policies

- Definition of a Policy
  - Communicates a consensus of judgment
  - Defines appropriate behavior for users
  - Identifies what tools and procedures are needed
  - Provides directives for Human Resources action in response to inappropriate behavior
  - May be helpful if it is necessary to prosecute violators

What is a Security Policy? (1 of 3)

- Security Policy
  - A written document that states how an organization plans to protect the company‘s information technology assets
  - Outlines the protections that should be enacted to ensure the organization’s assets face minimal risk
  - Having a written security policy empowers an organization to take appropriate action to safeguard its data

What is a Security Policy? (2 of 3)

- Security policy functions
  - An overall intention and direction, formally expressed by the organization’s management
  - Details specific risks and how to address them
  - Provides controls to direct employee behavior
  - Helps create a security-aware organizational culture
  - Helps ensure employee behavior is directed and monitored in compliance with security requirements

What is a Security Policy? (3 of 3)

- An effective security policy must balance: trust and control
- Three approaches to trust
  - Trust everyone all of the time
  - Trust no one at any time
  - Trust some people some of the time
- Security policy attempts to provide right amount of trust
  - Trust some people some of the time
  - Builds trust over time
- Level of control must also be balanced
  - Influenced by security needs and organization’s culture

Types of Security Policies (1 of 4)

- A security policy is comprehensive and often detailed
  - Many organizations break the security policy down into smaller “subpolicies”
- Examples:
  - Acceptable encryption policy
  - Antivirus policy
  - Database credentials coding policy
  - Email policy
  - Extranet policy
  - Router security policy
  - Server security policy
  - VPN security policy
  - Wireless communication policy

Types of Security Policies (2 of 4)

- **Acceptable Use Policy (AUP)**
  - Policy that defines actions users may perform while accessing systems
  - Users include employees, vendors, contractors, and visitors
  - Typically covers all computer use, including mobile devices
  - Unacceptable use may also be outlined by the AUP
  - Generally considered most important information security policy

Types of Security Policies (3 of 4)

- **Personal Email Policy**
  - Generally covers three important elements:
    - Using company email to send personal email messages
    - Accessing personal email at a place of employment
    - Forwarding company emails to a personal account
- **Social Media Policy**
  - Social media network – grouping individuals and organizations into clusters or groups based on some sort of affiliation
  - Risks of social media:
    - Personal data can be used maliciously
    - Users may be too trusting
    - Accepting friends may have unforeseen consequences
    - Social media security is lax or confusing

Types of Security Policies (4 of 4)

- **Social Media Policy** (continued)
  - Social media policy – outlines acceptable employee use of social media be enforced
  - Reasons for a social media policy:
    - Setting standards for employee use
    - Defining limitations
    - Protecting the enterprise’s reputation
    - Creating consistency across channels

Awareness and Training (1 of 4)

- A key defense in information security:
  - Providing security awareness and training to users (sometimes called continuing education)
- All users need continuous training in the new security defenses and be reminded of company security policies and procedures
- Opportunities for security training:
  - When a new employee is hired
  - After a computer attack has occurred
  - When an employee promoted
  - During an annual department retreat
  - When new user software is installed
  - When user hardware is upgraded

Awareness and Training (2 of 4)

Year born	**Traits**	**Number in U.S. population**
Prior to 1946	Patriotic, loyal, faith in institutions	75 million
1946-1964	Idealistic, competitive, question authority	80 million
1965-1981	Self-reliant, distrustful of institutions, adaptive to technology	46 million
1982-2000	Pragmatic, globally concerned, computer literate, media savvy	76 million

Awareness and Training (3 of 4)

Subject	Pedagogical approach	Andragogical approach
Desire	Motivated by external pressures to get good grades or pass on to the next grade	Motivated by higher self-esteem, more recognition, desire for better quality of life
Student	Dependent on teacher for all learning	Self-directed and responsible for own learning
Subject matter	Defined by what the teacher wants to give	Learning is organized around situations in life or at work
Willingness to learn	Students are informed about what they must learn	A change triggers a readiness to learn or students perceive a gap between where they are and where they want to be

Awareness and Training (4 of 4)

- In addition to training styles, there are different learning styles
  - Visual
  - Auditory
  - Kinesthetic
- Training styles impact how people learn
  - Role-based training
    - Involves specialized training that is customized to the specific role that an employee holds in the organization

Agreements (1 of 2)

- Risks of third-party integration:
  - On-boarding and off-boarding
  - Application and social media network sharing
  - Privacy and risk awareness
  - Data considerations
- Interoperability **agreements**
  - Formal contractual relationships as they related to security policy and procedures
  - Part of the **standard operating procedures**, or those actions and conduct that are considered normal

Agreements (2 of 2)

- Agreements that should be regularly reviewed to verify compliance and performance standards include:
  - **Service Level Agreement (SLA)** – specifies what services will be provided and the responsibilities of each party
  - **Blanket Purchase Agreement (BPA)** – a prearranged purchase or sale agreement between a government agency and a business
  - **Memorandum of Understanding (MOU)** – describes an agreement between two or more parties
  - **Interconnection Security Agreement (ISA)** – an agreement that is intended to minimize security risks for data transmitted across a network
  - **Non-disclosure agreement (NDA)** – a legal contract that specifies how confidential material will be shared between parties but restricted to others

Personnel Management

- When hiring, a **background check** should be conducted
  - The process of authenticating the information supplied to a potential employer by a job applicant in the applicant’s resume, application, and interviews
- When an employee leaves, an **exit interview** is usually conducted
  - A “wrap-up” meeting between management representatives and the person leaving an organization either voluntarily or through termination

Troubleshooting Common Security Issues (1 of 2)

- Security professionals should have the knowledge and skill to troubleshoot common security issues, including:
  - Access violations
  - Asset management
  - Authentication issues
  - Baseline deviation
  - Certificate issues
  - Data exfiltration
  - License compliance violation
  - Logs and events anomalies
  - Misconfigured devices

Troubleshooting Common Security Issues (2 of 2)

- Security professionals should have the knowledge and skill to troubleshoot common security issues, including (continued):
  - Permission issues
  - Personnel issues
  - Unauthorized software
  - Unencrypted credentials
  - Weak security configurations

Review Questions

Which of the following covers the procedures of managing object authorizations?

A. Asset management

B. Task management

C. Privilege management

D. Threat management

Review Questions

Which of the following covers the procedures of managing object authorizations?

A. Asset management

B. Task management

C. **Privilege management**

D. Threat management

Review Questions

What is a collection of suggestions that should be implemented?

A. Policy

B. Guideline

C. Standard

D. Code

Review Questions

What is a collection of suggestions that should be implemented?

A. Policy

B. **Guideline**

C. Standard

D. Code

Coming Up Next…

CompTIA Security+ Exam

GOOD LUCK!