Chapter 2 - Personnel Security and Risk Management Concepts

* People are the weakest link of security.
* When several people work together to perpetrate a crime, it’s called collusion. Employing

the principles of separation of duties, restricted job responsibilities, mandatory vacations, job rotation, and cross-training reduces the likelihood that a coworker will be willing to collaborate on an illegal or abusive scheme because of the higher risk of detection.

* The primary goal of risk management is to reduce risk to an acceptable level. What that

level actually is depends on the organization, the value of its assets, the size of its budget, and many other factors

* Risk management is composed of two primary elements: risk assessment and

risk response.

* A concept related to risk management is risk awareness. Risk awareness is the effort

to increase the knowledge of risks within an organization.

* Valid definitions for risk
  + risk = threat \* vulnerability
  + A risk is a calculation of the probability of occurrence and the level of damage that could be caused if an exposure is realized.
  + The presence of a vulnerability when a related threat exists is an exposure. Every instance of exposure introduces risk.
* Thus, addressing either the threat or threat agent or the vulnerability directly results in

a reduction in risk. This activity is known as risk reduction or risk mitigation, which is the

overall goal of risk management.

* Inherent risk is the level of natural, native, or default risk that exists in an environment, system, or product prior to any risk management efforts being performed.
* A malicious event does not need to succeed in violating security to be considered an attack.
* A breach, intrusion, or penetration is the occurrence of a security mechanism

being bypassed or thwarted by a threat agent. A breach is a successful attack.

* There are many approaches to risk assessment. Some are initiated by evaluating all the threats and then pairing with the assets, whereas others focus on risks associated with the inventory of assets. In both approaches, asset-threat pairing is done. Second approach is usually preferred.
* The goal of asset valuation is to assign to an asset a specific dollar value that encompasses tangible costs as well as intangible ones.
* Once an inventory of threats and assets (or assets and threats) is developed, then

each asset-threat pairing must be individually evaluated and its related risk calculated or

assessed. There are two primary risk assessment methodologies: quantitative and qualitative.

* Many times qualitative risk analysis is done to determine whether quantitative analysis is required or not. The method of combining quantitative and qualitative analysis into a final assessment of organizational risk is known as hybrid assessment or hybrid analysis.
* Scenarios and the Delphi technique are two very common methods for qualitative risk analysis.
  + In scenarios, a written scenario for a major threat is created. Threat levels, potential loss and safeguard benefits are then assigned to a scenario, for eg- rating system from 1 to 10. Participants are asked to provide responses and the collective response is presented to the upper management.
  + The Delphi technique is simply an anonymous feedback-and-response process used to enable a group to reach an anonymous consensus. Its primary purpose is to elicit honest and uninfluenced responses from all participants
* The six major elements of quantitative risk analysis are:
  + Assign asset value (AV)
  + Calculate exposure factor (EF)
  + Calculate single loss expectancy (SLE)
  + Assess the annualized rate of occurrence (ARO)
  + Derive the annualized loss expectancy (ALE)
  + Perform cost/benefit analysis of countermeasures
* The exposure factor (EF) or loss potential represents the percentage of loss that an organization would experience if a specific asset were violated by a realized risk.
* SLE = asset value (AV) \* exposure factor (EF)
* ALE = single loss expectancy (SLE) \* annualized rate of occurrence (ARO)
* Once an ALE is calculated for each asset-threat pairing, then the entire collection should be sorted from largest ALE to smallest. The largest ALE is the biggest problem the organization is facing and thus the first risk to be addressed in risk response.
* Risk Responses
  + Reducing risk, or risk mitigation, is the implementation of safeguards, security controls, and countermeasures to reduce and/or eliminate vulnerabilities or block threats.
  + Assigning risk or transferring risk is the placement of the responsibility of loss due to a risk onto another entity or organization.
  + Risk deterrence is the process of implementing deterrents to would-be violators of security and policy. The goal is to discourage a threat agent not to attack.
  + Some examples include implementing auditing, security cameras, and warning banners; using security guards.
  + Risk avoidance is the process of selecting alternate options or activities that have less associated risk than the default, common, expedient, or cheap option.
  + Accepting risk, or acceptance of risk, is the result after a cost/benefit analysis shows countermeasure costs would outweigh the possible cost of loss due to a risk. It also means that management has agreed to accept the consequences and the loss if the risk is realized.
  + An unacceptable possible response to risk is to reject risk or ignore risk.
* Total risk is the amount of risk an organization would face if no safeguards were implemented.
* threats \* vulnerabilities \* asset value = total risk
* The difference between total risk and residual risk is known as the controls gap. The controls gap is the amount of risk that is reduced by implementing safeguards.
* total risk – controls gap = residual risk
* [ALE pre-safeguard – ALE post-safeguard] – annual cost of safeguard (ACS) = value of

the safeguard to the company

* Categories of security controls in a defense-in-depth implementation:
  + Physical controls are security mechanisms focused on providing protection to the facility and real-world objects.
  + The category of technical controls or logical controls involves the hardware or software mechanisms used to manage access and provide protection for IT resources and systems.
  + The category of administrative controls are the policies and procedures defined by an organization’s security policy and other regulations or requirements. They are sometimes referred to as management controls, managerial controls, or procedural controls.
* Types of Security controls
  + A preventive control (aka preventative control) is deployed to thwart or stop unwanted or unauthorized activity from occurring.
  + A deterrent control is deployed to discourage security policy violations. Deterrent and preventive controls are similar, but deterrent controls often depend on individuals being convinced not to take an unwanted action.
  + A detective control is deployed to discover or detect unwanted or unauthorized activity.
  + A compensation control is deployed to provide various options to other existing controls to aid in enforcement and support of security policies. They can be any controls used in addition to, or in place of, another control.
  + A corrective control modifies the environment to return systems to normal after an unwanted or unauthorized activity has occurred. It attempts to correct any problems resulting from a security incident. Corrective controls can be simple, such as terminating malicious activity or rebooting a system.
  + Recovery controls are an extension of corrective controls but have more advanced or complex abilities. A recovery control attempts to repair or restore resources, functions, and capabilities after a security policy violation. Recovery controls typically address more significant damaging events compared to corrective controls.
  + A directive control is deployed to direct, confine, or control the actions of subjects. Eg includes security policy requirements, escape route signs, etc.
* Risk Maturity Model (RMM) assesses the key indicators and activities of a mature, sustainable, and repeatable risk management process. It relates to CMM and has a five-levels model.
  + Ad hoc, preliminary, defined, Integrated, and optimized
* A risk framework is a guideline or recipe for how risk is to be assessed, resolved, and monitored.
* Social engineering principles
  + Authority, Intimidation, Trust, Consensus, Familiarity, Scarcity, Urgency
* Spear phishing is a more targeted form of phishing where the message is crafted and directed specifically to a group of individuals.
* Whaling is a form of spear phishing that targets specific high-value individuals such as the CEO or other C-level executives, administrators, or high-net-worth clients.
* Short Message Service (SMS) phishing or smishing
* Vishing (i.e., voiced-based phishing)
* Spam is any type of email that is undesired and/or unsolicited.
* Shoulder surfing occurs when someone is able to watch a user’s keyboard or view their display.
* A hoax is a form of social engineering designed to convince targets to perform an action that will cause problems or reduce their IT security. Eg - mail asking to change browser configurations.
* Impersonation is the act of taking on the identity of someone else. Also known as masquerading, spoofing, and identity fraud.
* Tailgating is an attack that does not depend on the consent of the victim— the attacker just walks behind the victim as they walk into a building. Whereas in piggybacking they trick victims to provide consent by holding a large box during entry, etc.
* Baiting is when the attacker drops USB sticks, optical discs, or even wallets in a location that a worker is likely to encounter it. The hope is the worker will plug the USB drive or insert the disc into a work computer where the malware will auto-infect the system.
* Dumpster diving is the act of digging through trash, discarded equipment, or abandoned locations in order to obtain useful information.
* Typo squatting is a practice employed to capture and redirect traffic when a user mistypes the domain name or IP address of an intended resource.
* The first step in hiring new employees is to create a job description.Crafting job descriptions is the first step in defining security needs.
* Security champions are often non-security employees who take up the charge to encourage others to support and adopt more security practices and behaviors.