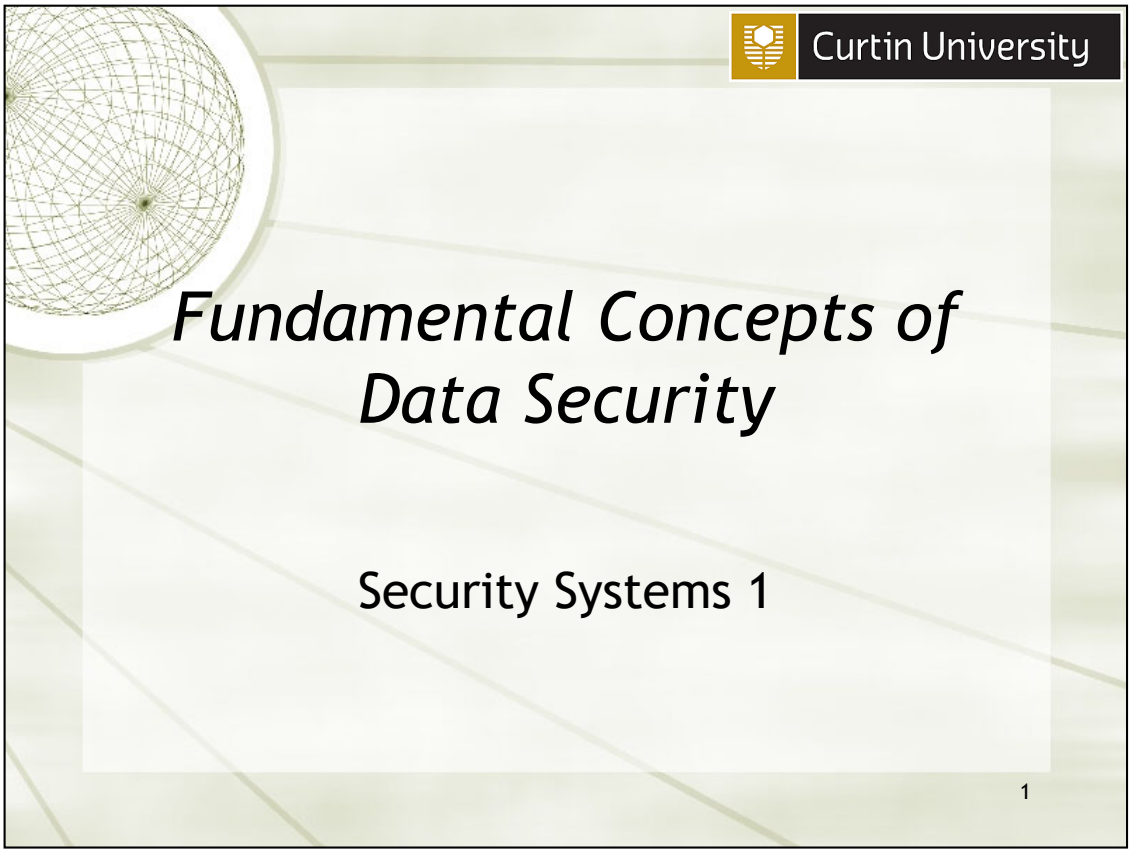
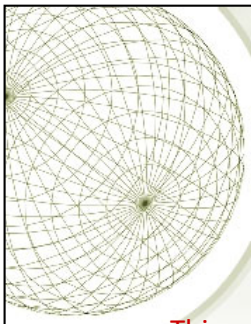


Note: This is expected to be delivered over three lectures/workshops



Security management relies on properly identifying and valuing a company's assets, and then implementing security policies, procedures, standards, and guidelines to provide integrity, confidentiality, and availability for those assets. Various management tools are used to classify data and perform risk analysis and assessments. These tools identify vulnerabilities and exposure rates and rank the severity of identified vulnerabilities so that effective countermeasures can be implemented to mitigate risk in a cost-effective manner. Management's responsibility is to provide protection for the resources it is responsible for and the company overall. These resources come in human, capital, hardware, and informational forms. Management must concern itself with ensuring that a security program is set up that recognizes the threats that can affect these resources and be assured that the necessary protective measures are put into effect.

The necessary resources and funding need to be available, and strategic representatives must be ready to participate in the security program. Management must assign responsibility and identify the roles necessary to get the security program off the ground and to keep it thriving and evolving as the environment changes. Management must also integrate the program into the current business environment and monitor its accomplishments. Management's support is one of the most important pieces of a security program. A simple nod and a wink will not provide the amount of support required.

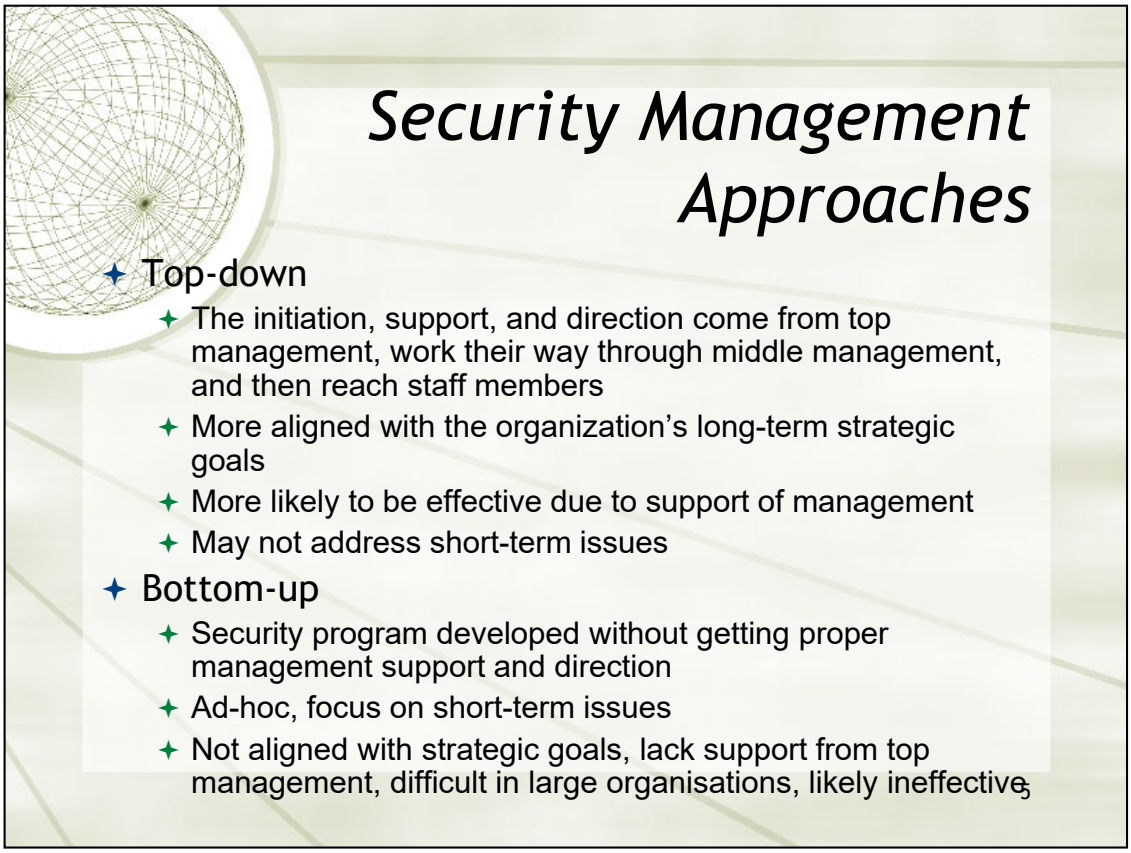
The security program needs to:

- Be driven by the management to have a better chance of being effective.
- To be developed in terms of the whole of the organization and then refined to fit the specific areas within the organization.

Security Management Responsibilities

In the world of security, management's functions involve determining objectives, scope, policies, priorities, and strategies. Management needs to define a clear scope and, before 100 people run off in different directions trying to secure the environment, to determine actual goals expected to be accomplished from a security program. Management also needs to evaluate business objectives, security risks, user productivity, and functionality requirements and objectives. Finally, management must define steps to ensure that all of these issues are accounted for and properly addressed.

Many companies look at the business and productivity elements of the equation only and figure that information and computer security fall within the IT administrator's responsibilities. In these situations, management is not taking computer and information security seriously, the consequence of which is that security will most likely remain underdeveloped, unsupported, underfunded, and unsuccessful. Security needs to be addressed at the highest levels of management. The IT administrator can consult with management on the subject, but the security of a company should not be delegated entirely to the IT or security administrator.



The Top-Down Approach to Security

When a house is built, the workers start with a blueprint of the structure, then pour the foundation, and then erect the frame. As the building of the house continues, the workers know what the end result is supposed to be, so they add the right materials, insert doors and windows as specified in the blueprints, erect support beams, provide sturdy ceilings and floors, and add the plaster and carpet and smaller details until the house is complete. Then inspectors come in to ensure that the structure of the house and the components used to make it are acceptable. If this process did not start with a blueprint and a realized goal, the house could end up with an unstable foundation and doors and windows that don't shut properly. As a result, the house would not pass inspection—meaning much time and money would have been wasted.

Building a security program is analogous to building a house. When designing and implementing a security program, the security professionals must determine the functionality and realize the end result expected. Many times, companies just start locking down computers and installing firewalls without taking the time to understand the overall security requirements, goals, and assurance levels they expect from security as a whole within their environment. The team involved in the process should start from the top with very broad ideas and terms and work its way down

to detailed configuration settings and system parameters. At each step, the team should keep in mind the overall security goals so each piece it adds will provide more granularity to the intended goal. This helps the team avoid splintering the main objectives by running in 15 different directions at once.

The next step is to develop and implement procedures, standards, and guidelines that support the security policy and to identify the security countermeasures and methods to be put into place. Once these items are developed, the security program increases in granularity by developing baselines and configurations for the chosen security controls and methods.

If security starts with a solid foundation and develops over time with understood goals and objectives, a company does not need to make drastic changes midstream. The process can be methodical, requiring less time, funds, and resources, and provide a proper balance between functionality and protection. This is not the norm, but with your insight, maybe you can help your company approach security in a more controlled manner. You could provide the necessary vision and understanding of how security should be properly planned and implemented, and how it should evolve in an organized manner, thereby helping the company avoid a result that is essentially a giant heap of disjointed, flawed security products.

A security program should use a top-down approach, meaning that the initiation, support, and direction come from top management, work their way through middle management, and then reach staff members. In contrast, a bottom-up approach refers to a situation in which the IT department tries to develop a security program without getting proper management support and direction. A bottom-up approach is usually less effective, not broad enough, and doomed to fail. A top-down approach makes sure the people actually responsible for protecting the company's assets (senior management) are driving the program.

Security Administration and Supporting Controls

If no security officer role currently exists, one should be established by management. The security officer role is directly responsible for monitoring a majority of the facets of a security program. Depending on the organization, security needs, and size of the environment, the security administration may consist of one person or a group of individuals who work in a central or decentralized manner. Whatever its size, the security administration requires a clear reporting structure, an understanding of responsibilities, and testing and monitoring capabilities to make sure compromises do not slip in because of a lack of communication or comprehension.

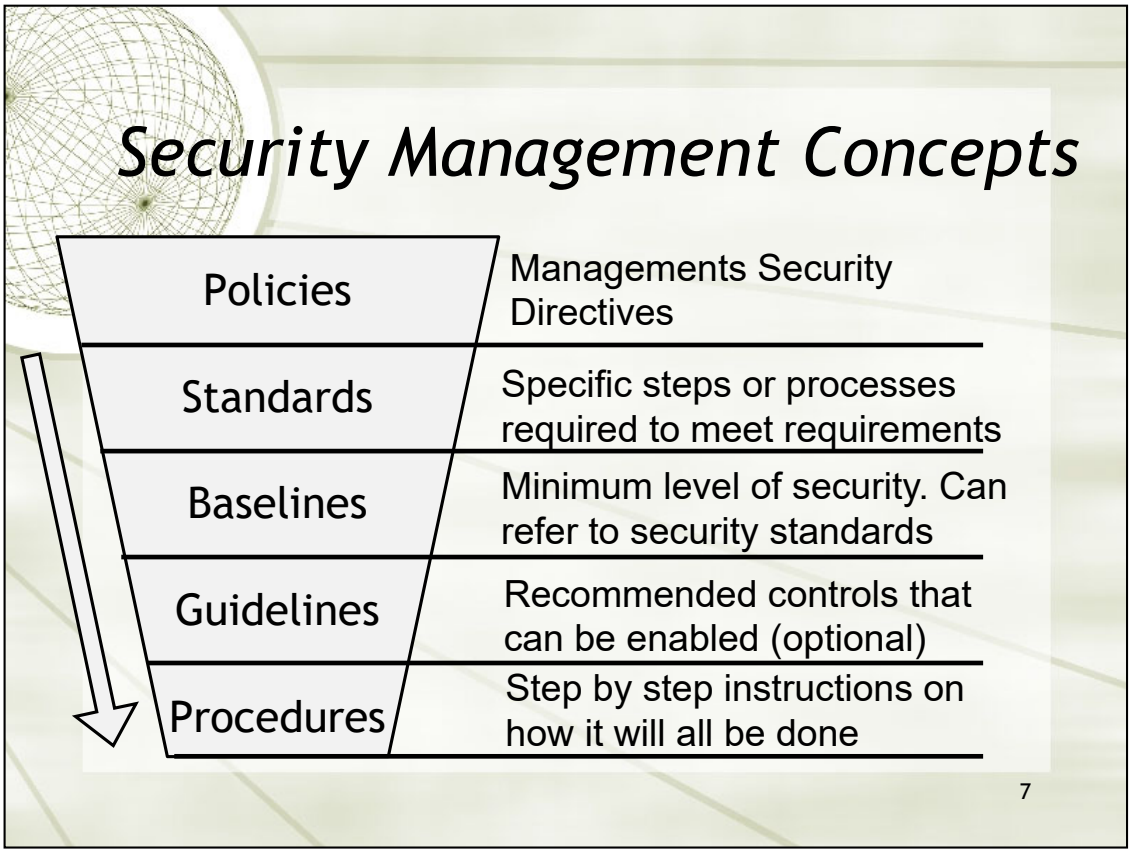
Information owners should dictate which users can access their resources and what those users can do with those resources after they access them. The security administration's job is to make sure these objectives are implemented.

The information owner (also called the data owner) is usually a senior executive within the management group of the company, or the head of a specific department. The information owner has the corporate responsibility for data protection and would be the one held liable for any negligence when it comes to protecting the company's information assets. The person who holds this role is responsible for assigning classifications

to information and for dictating how the data should be protected. If the information owner does not lay out the foundation of data protection and ensure the directives are being enforced, she would be violating the due care concept.

By having a security administration group, a company ensures it does not lose focus on security and that it has a hierarchical structure of responsibility in place. The security officer's job is to ensure that management's security directives are fulfilled, not to construct those directives in the first place. There should be a clear communication path between the security administration group and senior management to make certain the security program receives the proper support and to ensure management makes the decisions. Too often, senior management is extremely disconnected from security issues, despite the fact that when a serious security breach takes place, senior management must explain the reasons to business partners, shareholders, and the public. After this humbling experience, the opposite problem tends to arise—senior management becomes too involved. A healthy relationship between the security administration group and senior management should be developed from the beginning, and communication should easily flow in both directions.

Inadequate management can undermine the entire security effort in a company. Among the possible reasons for inadequate management are that management does not fully understand the necessity of security; security is in competition with other management goals; management views security as expensive and unnecessary; or management applies lip service instead of real support to security. Powerful and useful technologies, devices, software packages, procedures, and methodologies are available to provide the exact level of security required, but without proper security management and management support, none of this really matters.



Imagine the day-to-day operation of an organization without any policies. Individuals would have to make decisions about what is right or wrong for the company based upon their personal values or their own past experience. This could potentially consist of as many values as there are people in the organization. Management would also be failing to demonstrate due diligence by not putting practices in place to protect the investors and manage the employees of the organization. Policies establish the glue that ensures everyone has a common set of expectations and communicates management's goals and objectives.

Procedures, standards, guidelines, and baselines are different components that support the implementation of the security policy. A policy without mechanisms for its implementation is analogous to an organization having a business strategy without action plans to execute the strategy. In this situation, there would be limited chance of success, as expectations to achieve the higher-level business strategy would not be clear to the workforce. Similarly, policies communicate management's expectations, which are fulfilled through the execution of procedures and adherence to standards, baselines, and guidelines.

Security policies may consist of **different types**, depending upon the specific need for the policy.

- Organizational or program policy: This policy is issued by a senior management individual, who creates the authority and scope for the security program. The purpose of the program is described, and the assigned responsibility is defined for carrying out the information security mission. The goals of confidentiality, integrity, and availability are addressed in the policy.
- Functional, issue-specific policies: While the organizational security policies are broad in scope, the functional or issue-specific policies address areas of particular security concern requiring clarification.
- System-specific policies: Areas where it is desired to have clearer direction or greater control for a specific technical or operational area may have more detailed policies.

The more detailed and issue specific the written policy is, the higher the likelihood is that the policy will require more frequent changes.

Standards.

Whereas policies define what an organization needs, standards take this a step further and define the requirements. Standards provide the agreements that provide interoperability within the organization through the use of common protocols. Standards simplify the operation of the security controls within the company and increase efficiency.

Procedures.

Procedures are step-by-step instructions in support of the policies, standards, guidelines, and baselines. The procedure indicates how the policy will be implemented and who does what to accomplish the tasks. The procedure provides clarity and a common understanding to the operation required to effectively support the policy on a consistent basis.

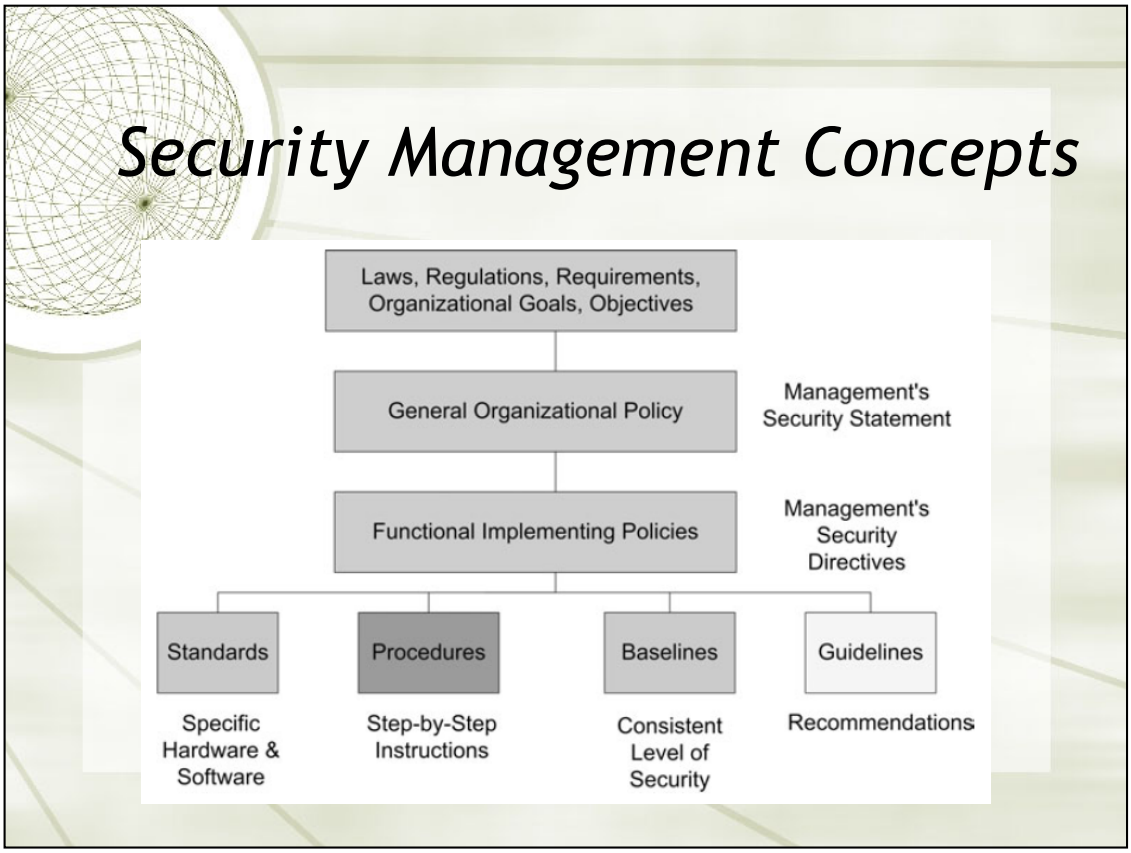
Baselines.

Baselines provide descriptions of how to implement security packages to ensure that these implementations are consistent throughout the organization. Different software packages, hardware platforms, and networks have different methods of ensuring security. There are many different options and settings that must be determined to provide the desired protection. An analysis of the available configuration settings and subsequent settings desired, forms the basis for future, consistent implementation of the standard.

Guidelines.

Guidelines are discretionary or optional controls used to enable individuals to make judgments with respect to security actions. A good exercise is to replace the word *guideline* with the word *optional.* Guidelines are also those recommendations, best practices, and templates provided by other organizations

such as the Control Objectives for Information and related Technology (COBIT), the Capability Maturity Model (CMM), ISO 17799, and British Standard 7799, security configuration recommendations such as those from the National Institute of Standards and Technology (NIST) or the National Security Agency (NSA), organizational guidelines, or other governmental guidelines.



Imagine the day-to-day operation of an organization without any policies. Individuals would have to make decisions about what is right or wrong for the company based upon their personal values or their own past experience. This could potentially consist of as many values as there are people in the organization. Management would also be failing to demonstrate due diligence by not putting practices in place to protect the investors and manage the employees of the organization. Policies establish the glue that ensures everyone has a common set of expectations and communicates management's goals and objectives.

Procedures, standards, guidelines, and baselines are different components that support the implementation of the security policy. A policy without mechanisms for its implementation is analogous to an organization having a business strategy without action plans to execute the strategy. In this situation, there would be limited chance of success, as expectations to achieve the higher-level business strategy would not be clear to the workforce. Similarly, policies communicate management's expectations, which are fulfilled through the execution of procedures and adherence to standards, baselines, and guidelines.

Security policies may consist of **different types**, depending upon the specific need for the policy.

- Organizational or program policy: This policy is issued by a senior management individual, who creates the authority and scope for the security program. The purpose of the program is described, and the assigned responsibility is defined for carrying out the information security mission. The goals of confidentiality, integrity, and availability are addressed in the policy.
- Functional, issue-specific policies: While the organizational security policies are broad in scope, the functional or issue-specific policies address areas of particular security concern requiring clarification.
- System-specific policies: Areas where it is desired to have clearer direction or greater control for a specific technical or operational area may have more detailed policies.

The more detailed and issue specific the written policy is, the higher the likelihood is that the policy will require more frequent changes.

Standards.

Whereas policies define what an organization needs, standards take this a step further and define the requirements. Standards provide the agreements that provide interoperability within the organization through the use of common protocols. Standards simplify the operation of the security controls within the company and increase efficiency.

Procedures.

Procedures are step-by-step instructions in support of the policies, standards, guidelines, and baselines. The procedure indicates how the policy will be implemented and who does what to accomplish the tasks. The procedure provides clarity and a common understanding to the operation required to effectively support the policy on a consistent basis.

Baselines.

Baselines provide descriptions of how to implement security packages to ensure that these implementations are consistent throughout the organization. Different software packages, hardware platforms, and networks have different methods of ensuring security. There are many different options and settings that must be determined to provide the desired protection. An analysis of the available configuration settings and subsequent settings desired, forms the basis for future, consistent implementation of the standard.

Guidelines.

Guidelines are discretionary or optional controls used to enable individuals to make judgments with respect to security actions. A good exercise is to replace the word *guideline* with the word *optional.* Guidelines are also those recommendations, best practices, and templates provided by other organizations

such as the Control Objectives for Information and related Technology (COBIT), the Capability Maturity Model (CMM), ISO 17799, and British Standard 7799, security configuration recommendations such as those from the National Institute of Standards and Technology (NIST) or the National Security Agency (NSA), organizational guidelines, or other governmental guidelines.

SECURITY DEFINITIONS

The words “vulnerability,” “threat,” “risk,” and “exposure” often are used to represent the same thing, even though they have different meanings and relationships to each other. It is important to understand each word’s definition, but it is more important to understand each concept’s relationship to the other concepts.

A vulnerability is a software, hardware, procedural, or human weakness that may provide an attacker the open door he is looking for to enter a computer or network and have unauthorized access to resources within the environment. A vulnerability characterizes the absence or weakness of a safeguard that could be exploited. This vulnerability may be a service running on a server, unpatched applications or operating system software, unrestricted modem dial-in access, an open port on a firewall, lax physical security that allows anyone to enter a server room, or unenforced password management on servers and workstations.

A threat is any potential danger to information or systems. The threat is that someone, or something, will identify a specific vulnerability and use it against the company or individual. The entity that takes advantage of a vulnerability is referred to as a threat agent. A threat agent could be an

intruder accessing the network through a port on the firewall, a process accessing data in a way that violates the security policy, a tornado wiping out a facility, or an employee making an unintentional mistake that could ex- pose confidential information or destroy a file's integrity.

A risk is the likelihood of a threat agent taking advantage of a vulnerability and the corresponding business impact. If a firewall has several ports open, there is a higher likelihood that an intruder will use one to access the network in an unauthorized method. If users are not educated on processes and procedures, there is a higher likelihood that an employee will make an intentional or unintentional mistake that may destroy data. If an intrusion detection system (IDS) is not implemented on a network, there is a higher likelihood an attack will go unnoticed until it is too late. Risk ties the vulnerability, threat, and likelihood of exploitation to the resulting business impact.

An exposure (incident) is an instance of being exposed to losses from a threat agent. A vulnerability exposes an organization to possible damages. If password management is lax and password rules are not enforced, the company is exposed to the possibility of having users' passwords captured and used in an unauthorized manner. If a company does not have its wiring inspected and does not put proactive fire prevention steps into place, it exposes itself to potentially devastating fires.

A countermeasure (safeguard), is put into place to mitigate the potential risk. A countermeasure may be a software configuration, a hardware device, or a procedure that eliminates a vulnerability or that reduces the likelihood a threat agent will be able to exploit a vulnerability. Examples of countermeasures include strong password management, a security guard, access control mechanisms within an operating system, the implementation of basic input/output system (BIOS) passwords, and security-awareness training.

If a company has antivirus software but does not keep the virus signatures up-to-date, this is a vulnerability. The company is vulnerable to virus attacks. The threat is that a virus will show up in the environment and disrupt productivity. The likelihood of a virus showing up in the environment and causing damage is the risk. If a virus infiltrates the company's environment, then a vulnerability has been exploited and the company is exposed to loss. The countermeasures in this situation are to update the signatures and install the antivirus software on all computers.

Applying the right countermeasure can eliminate the vulnerability and exposure, and thus reduce the risk. The company cannot eliminate the threat agent, but it can protect itself and prevent this threat agent from exploiting

vulnerabilities within the environment.

Example: SQL injection

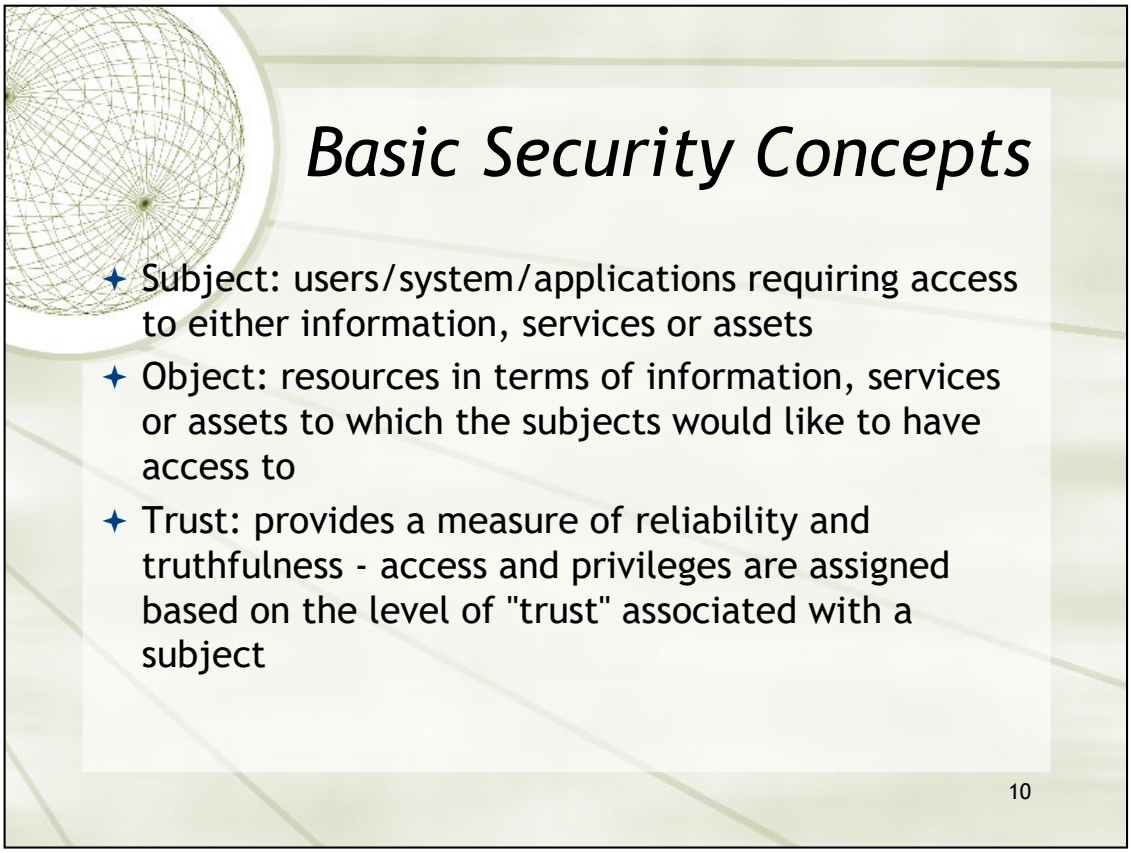
Vulnerability: a database server software does not correctly parse special characters in SQL requests

Threat: a hacker may exploit the above database server software's vulnerability by issuing specially crafted requests to steal confidential information

Risk: high rating of the likelihood and impact of the above threat event

Incident: an SQL injection attack has happened and hacker managed to steal all users' information from a vulnerable database system

Countermeasure: patching of database serversoftware to prevent SQL injection attacks



Subjects and Objects

The first basic concept focuses on things to be protected and the entities who want access to those things. The things are what are formally called objects and the entities are formally called subjects. Objects (which are generally organizational assets) can be, for example, computers, terminals, applications, databases, user agents, buildings, rooms, communications equipment, power facilities, documentation, or I/O devices (printers, terminals, etc.). Subjects (also commonly referred to as “principals,” “actors,” or “users”) can be, for example, any networked elements (computers, routers, servers, workstations), application servers and clients, DBMSs, user agents, or human beings.

Because computers can interact, let alone programs executing within these computers, there are times when they have to be viewed as subjects. However, this is an abstraction that should only serve as a basic model. A subject in one context may be viewed as an object in a different context, for example, a computer program can be considered a subject when it interacts with stored information (data), yet the same program can be considered an object when a human uses the program or the program is being manipulated by another software component (e.g., by a compiler or a program virus). The critical point here is to be specific as to what subjects are being considered.

What is the definition of trust in the context of security in a computing environment?

The word “trust” is used quite frequently in everyday speech and even used during information security conversations. However, to be used in an engineering context, we need a clear definition of trust. Two typical definitions are:

Confidence in the integrity, ability, character, and truth of a person or thing (The American Heritage Dictionary, Houghton Mifflin, 1983)

and assumed reliance on the character, ability, strength, or truth of someone or something, b: one in which confidence is placed, 3a: a property interest held by one person for the benefit of another. (Webster’s New Collegiate Dictionary, 2nd ed., 1960)

We routinely establish a qualitative measure of trust with those we associate/interact with regarding their honesty and reliability, with the expectation that they will behave in certain ways. Unfortunately, we have yet to identify a quantitative measure of confidence so the best we can achieve is some measure of assurance that a person or thing cannot abuse the degree of “trust” we have that they will act as expected.

Where do we start with measuring assurance? It begins with understanding what needs protection so we need to inventory:

. objects (i.e., assets, tangible/intangible property), and
. subjects (i.e., actors, users).

We also need to identify what and how each subject is allowed to interact with which objects. Subjects can also be grouped according to some common set of attributes, such as all members of the finance, sales, or engineering departments. These organizational groupings are frequently called classes or groups. These subject – object – allowed access relationships represent the level of “trust” we grant to subjects within an organization.