Security Planning Risk Analysis, Organizational Security Policy

By

Prof. Muhammad Iqbal Bhat

Department of Higher Education

Government Degree College Beerwah

Topics:

1. What are Security Planning
2. Risk Analysis
3. Organizational Security Policy
4. Physical Security

Security Planning

What is Security Planning?

Security planning is the process of developing strategies to protect information and information systems from potential security threats.

It involves identifying the risks that an organization faces and developing a plan to address those risks.

Effective security planning should ensure that the confidentiality, integrity, and availability of information and information systems are maintained.

The Steps of Security Planning:

Identify and classify	Identify and classify information assets - Identify the information assets that need protection and classify them based on their importance and sensitivity.
Identify	Identify potential threats - Identify potential threats that may affect the organization's information and information systems.
Assess	Assess vulnerabilities - Assess vulnerabilities in the organization's information systems that could be exploited by attackers.
Determine	Determine the likelihood and impact of potential risks - Determine the likelihood of the identified threats and their potential impact on the organization.
Develop	Develop a risk management plan - Develop a risk management plan that outlines strategies for mitigating the identified risks.
Implement	Implement security measures - Implement security measures to mitigate the identified risks. This may include policies, procedures, and technical controls.
Monitor and review	Monitor and review - Monitor the effectiveness of the security measures and review the security plan regularly to ensure it remains effective.

Types of Security Plans

Information Security Plan - This plan outlines the organization's overall approach to security and provides guidance on how to protect information and information systems. It includes policies and procedures for access control, data protection, incident response, and other aspects of security.

Disaster Recovery Plan - This plan outlines procedures for recovering from a disaster, such as a natural disaster or cyber attack. It includes procedures for backing up and restoring data, restoring system functionality, and communicating with employees, customers, and other stakeholders.

Business Continuity Plan - This plan outlines procedures for maintaining business operations in the event of a disruption. It includes procedures for maintaining critical business functions, communicating with employees and stakeholders, and resuming normal operations.

Examples of Security Planning

Developing	Developing an incident response plan in case of a security breach.
Creating	Creating a security awareness program to educate employees on security best practices.
Conducting	Conducting a vulnerability assessment to identify potential security weaknesses in an organization's network or information systems.
Developing	Developing a disaster recovery plan in case of a natural disaster or cyber attack.

Risk Analysis

What is Risk Analysis?

1. Risk analysis is the process of identifying, assessing, and prioritizing risks to an organization.

2. It involves analyzing potential threats, determining the likelihood and impact of those threats, and developing strategies to manage or mitigate those risks.

The Steps of Risk Analysis

Identify

Identify risks - Identify potential risks to the organization, such as natural disasters, cyber attacks, or human error.

Assess

Assess risks - Assess the likelihood and potential impact of each risk. This can be done using techniques such as risk scoring or qualitative analysis.

Prioritize

Prioritize risks - Prioritize risks based on their likelihood and potential impact. This helps to identify the risks that require the most attention and resources.

Develop

Develop risk management strategies - Develop strategies to manage or mitigate the identified risks. This may include implementing security controls, transferring risk to an insurance provider, or accepting the risk.

Implement

Implement risk management strategies - Implement the identified risk management strategies and monitor their effectiveness.

Types of Risk Analysis

Qualitative Risk Analysis - This method involves identifying and assessing risks based on their qualitative characteristics such as severity, likelihood, and impact. It is subjective and does not involve numerical calculations.

Quantitative Risk Analysis - This method involves assigning numerical values to risks based on their likelihood and impact. It provides a more objective assessment of risks and helps to prioritize them based on their level of severity.

Delphi Technique - This is a group-based approach to risk analysis where experts are asked to anonymously provide their opinions on risks and potential mitigation strategies. The results are then compiled and analyzed to identify common themes and trends.

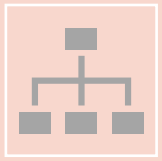
Examples of Risk Analysis

Conducting	Conducting a risk analysis to identify potential security threats to an organization's network.
Assessing	Assessing the risks associated with a new product or service before it is launched.
Conducting	Conducting a risk analysis to identify potential hazards in the workplace and develop strategies to mitigate those risks.
Assessing	Assessing the risks associated with outsourcing a critical business function to a third-party provider.

Organizational Security Policy

What is an Organizational Security Policy?

An organizational security policy is a formal document that outlines an organization's security objectives, standards, and procedures.



It provides guidance and direction to employees, contractors, and other stakeholders on how to protect the organization's assets and information.

Elements of an Organizational Security Policy

Scope	• The policy should clearly define the scope of the policy, including which assets and information are covered and who is responsible for enforcing the policy.
Objectives	• The policy should outline the organization's security objectives, such as protecting the confidentiality, integrity, and availability of information.
Standards	• The policy should establish minimum standards for security controls, such as access control, encryption, and incident response.
Procedures	• The policy should provide specific procedures for implementing and enforcing the security controls.
Roles and Responsibilities	• The policy should clearly define the roles and responsibilities of individuals and departments within the organization for implementing and enforcing the security policy.
Monitoring and Review	• The policy should establish procedures for monitoring and reviewing the effectiveness of the security controls and the policy itself.

Benefits of an Organizational Security Policy:

Provides Guidance –	• An organizational security policy provides guidance to employees and other stakeholders on how to protect the organization's assets and information.
Reduces Risk –	• An effective security policy can reduce the risk of security incidents, such as data breaches or cyber attacks.
Promotes Compliance –	• A security policy can help organizations comply with legal and regulatory requirements, such as the General Data Protection Regulation (GDPR) or the Health Insurance Portability and Accountability Act (HIPAA).
Enhances Reputation –	• Effective security policies can enhance an organization's reputation by demonstrating its commitment to protecting its assets and information.

Examples of Organizational Security Policies:

Information Security Policy	• This policy outlines an organization's approach to protecting information assets, such as data, documents, and intellectual property.
Acceptable Use Policy	• This policy defines acceptable use of organizational assets, such as computers, networks, and other technology resources.
Physical Security Policy	• This policy outlines procedures for protecting physical assets, such as buildings, facilities, and equipment.
Incident Response Policy	• This policy defines procedures for responding to security incidents, such as data breaches or cyber attacks.

Physical Security

What is Physical Security?

Physical security refers to the measures taken to protect physical assets, people, and property from unauthorized access, theft, damage, or destruction.

It includes a variety of security measures such as access control, surveillance, and environmental controls.

Elements of Physical Security:

Access Control

- Access control refers to the measures taken to control who has access to a physical space. This can include physical barriers, such as fences or walls, as well as electronic access controls, such as key cards or biometric scanners.

Surveillance

- Surveillance includes the use of cameras, alarms, and other monitoring systems to detect and deter unauthorized access or activity.

Environmental Controls

- Environmental controls include measures such as fire suppression systems, temperature and humidity control, and backup power systems to protect against natural disasters or other disruptions.

Importance of Physical Security

Protects Assets

- Physical security measures help protect physical assets, such as property, equipment, and inventory, from theft or damage.

Protects People

- Physical security measures also help protect employees, customers, and other people who may be present in a facility from harm.

Deters Criminal Activity

- Visible physical security measures, such as cameras and alarms, can deter criminal activity by making it more difficult for criminals to gain access to a facility or property.

Improves Regulatory Compliance

- Physical security measures can help organizations comply with regulations, such as the Sarbanes-Oxley Act, which require certain security measures to protect against financial fraud.

Examples of Physical Security Measures:

Perimeter Security

- This can include fences, walls, or other physical barriers to prevent unauthorized access to a facility or property.

Access Control Systems

- Electronic access control systems, such as key cards or biometric scanners, can be used to control access to secure areas within a facility.

Video Surveillance

- Video cameras can be used to monitor activity in and around a facility, and can help deter criminal activity.

Security Lighting

- Lighting can be used to improve visibility and deter criminal activity.

Alarm Systems

- Alarms can be used to alert security personnel or law enforcement in the event of an unauthorized entry or other security breach.

Questions?