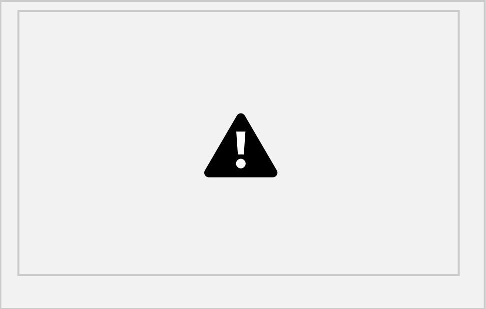
Chapter 14

IT Security Management

IT Security

Overview

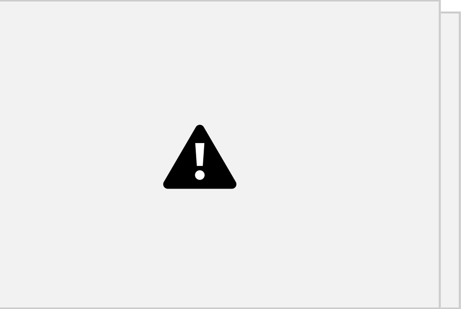
Management Overview



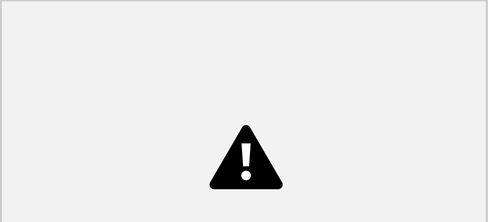
what

those assets threatened

threats



assets need to be protected



howwhat can be done to

are counter those

effective manner

ensures that critical assets are sufficiently protected in a cost

-

security risk assessment is needed for each asset in the

IT SECURITY MANAGEMENT: A process used to achieve and maintain appropriate levels of confidentiality, integrity, availability, accountability, authenticity, and reliability. IT security

manage unctions include:

determining organizational IT security objectives, strategies, and policies

determining organizational IT security requirements

identifying and analyzing security threats to IT assets within the organization

specifying

implementation and operation of safeguards that are necessary in order to cost effectively protect the information and services

monitoring the within the

organization

developing and implementing a security awareness program

detecting and reacting to incidents

Organizational Context and Security Policy

first examine

organization’s IT security:

objectives - wanted IT security

outcomes

strategies - how to meet objectives

policies - identify what needs to be done

Management Support.

Security Risk Assessment

Baseline

Approach

Informal Approach

most

comprehensive
approach

structured
process

- number of stages
- identify threats
and vulnerabilities

significant cost
in time,
resources,

may be a legal
requirement to
use

suitable for
large
organizations
with IT
systems critical

to their business objectives

Combined Approach

provides the most accurate evaluation of an organization's IT system’s security risks highest cost initially focused on addressing defense security concerns

often mandated by government

organizations and associated businesses

Step 1 -Establishing the Context

Step 2: Asset Identification

.

- “anything that needs to be protected”
  - has value to organization to meet its objectives
  - tangible or intangible
  - whose compromise or loss would seriously impact the operation of the organization

Step 3: Threat

Identification

integrity

availability

reliability

prevent an asset
from providing
appropriate levels
of the key security
services

confidentiality

accountability

anything that
might hinder or

authenticity

Step 4:

Vulnerability Identification

Step 5: Analyze Risks

Step 6: Analyze Existing Controls

Risk Likelihood

Table 14.3

Risk Consequences

Risk Treatment Alternatives

risk

acceptance

risk

avoidance

transfer

reduce consequence

reduce likelihood

choosing to accept a risk level greater than normal for business reasons

not proceeding with the activity or system that creates this risk

sharing responsibility for the risk with a third party

modifying the structure or use of the assets at risk to reduce the impact on the organization should the risk occur

risk

implement suitable controls to

lower the chance of the vulnerability being exploited

Case Study: Silver Star Mines

Assets