Risk Mitigation

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

Threat Assessment

> A formal process of examining the seriousness of a potential threat, as well as the likelihood of it being carried out.

- should determine asset value, and relative worth of assets at risk

Types of threats:

- Environmental
- Man-Made
- Internal vs. External

Threat Categories:

- *Strategic* - affects the long-term goals of the enterprise
- *Compliance* - following, or not following, a regulation or standard
- *Financial* - impact of financial decisions, or market factors
- *Operational* - impacts daily business
- *Technical* - affects IT systems / highly skilled fields
- *Managerial* - related to the management

Risk Assessment

Testing

- tech should be tested to identify any vulnerabilities
- intrusive vulnerability scan - attempts to penetrate
- non-intrusive vulnerability scan - only uses available information to hypothesize
- pentest - exploit weaknesses
    - authorization should be obtained for legal protection, indemnification, and limit retaliation

Change management

- methodology for making modifications & keeping track
- proper documentation
- all kinds of changes are recorded for IT systems

Two major changes that need proper documentation:

- System architecture
- file or document classification

Change Management Teams (CMT)

- body for overseeing changes
- composed of representatives from IT, network security, and upper management
- proposals must be approved by CMT
- review proposed changes
- ensure risk and impact of changes are well understood
- recommend approval, disapproval, deferral, or withdrawal
- communicate proposals to coworkers

Privilege management

Subject's access level, and the act of granting or revoking access

- privilege auditing

Incident management

Components required to identify, analyze, and contain incident

- Incident handling - planning, coordination, communications, and planning functions for resolution

Risk calculations

two approaches:

- qualitative risk calculation - educated guess, figurative values
- quantitative risk calculation - divided into likelihood and impact

Risk likelihood:

- Mean Time Between Failure (BTBF)
- Mean Time To Recovery (MTTR)
- Mean Time To Failure (MTTF)
- Failure In Time (FIT)
- Annualized Rate of Occurrence (ARO) - historical data

Risk impact:

- Monetary loss associated with an asset → amount of money lost
- Single Loss Expectancy (SLE) - expected monetary loss every time a risk occurs
- Annualized Loss Expectancy (ALE) - expected monetary loss over one year

Representing risk information

- Risk register - potential threats & associated risks
- Risk matrix - impact and likelihood

Strategies for Reducing Risk

Using Control Types

- Any device or process that's used to reduce risk
- Administrative Controls - ensuring policies and procedures are followed
- Technical Controls - security controls carried out or managed by devices

Subtypes:

- Deterrent controls
- Preventative controls
- Physical controls
- Detective controls
- Compensating controls
- Corrective controls

Distributing Allocation

> "spreading" the risk

- *Transference* - make a 3rd party responsible
- *Risk avoidance* - do not engage in activity
- *Mitigation* - address the risk by making it less serious

Implementing Technology

- Risk is often introduced by human error
- Using tech can minimize these errors

Automation

> That which replaces human activity

- Scalability
- Elasticity (the opposite)
- Continuous monitoring

Images and templates

- Master image - pre-built with proper configurations
- Templates standardize content

Non-persistence tools

- “live” boot media
- revert to known state
- rollback to known configuration
- snapshots

Practices for Reducing Risk

Security Policies

- Consensus of judgement
- appropriate behaviors
- what tools and procedures are needed
- directives for HR
- if necessary to prosecute

  Must balance trust and control

Examples:

- Encryption policy
- Antivirus policy
- Database credentials coding
- Email
- Extranet
- Router security
- Server security
- VPN security
- Wireless comms
- *Acceptable Use Policy*

Agreements

- Service Level Agreement (SLA) - services and responsibilities
- Blanket Purchase Agreement (BPA) - prearranged purchase between a government and contractor
- Memorandum of Understanding (MOU) - agreement between two or more
- Interconnection Security Agreement (ISA) - minimize security risks over network
- Non-Disclosure Agreement (NDA) - confidentiality