CIT 270: SYSTEMS SECURITY I

CHAPTER 15: RISK MITIGATION

BYU IDAHO

INTRODUCTION

Remember this presentation does not replace your reading and only covers at best 70% of the chapter material.

Note

Keep any eye out for boxes like this one in your chapter readings. These are note boxes that highlight important information. Your chapter quiz will often have questions that refer directly to one of these.

In this presentation pay special attention to yellow words. These highlighted words denote a topic that will almost always be on your chapter quiz.

MANAGING RISK

Threat Assessment: a formal process of examining the seriousness of a potential threat as well as the likelihood that it will be carried out.

There are many threats an organization can face. Despite the multitude of threats most fall into three broad categories:

- Environmental
- Man-made
- Internal or External

MANAGING RISK: THREAT CLASSIFICATIONS

Threat Category	Description	Example
Strategic	Action that affects the long-term goals of the organization	Theft of intellectual property, not pursuing a new opportunity, loss of major account, competitor entering market
Compliance	Following (or not following) a regulation or standard	Breach of contact, not responding to the introduction of news laws
Financial	Impact of financial decisions or market factors.	Increase in interest rates, global financial crisis
Operational	Events that impact the daily business of the organization	Fire, hazardous chemical spill, power blackout
Technical	Events that affect information technology systems	DoS attack, SQL injection attacks, virus
Managerial	Actions related to the management of the organization	Long-term illness of company president, key employee resigning

MANAGING RISK

A Supply Chain Assessment may be an additional assessment your organization may want to conduct. It looks at threats in your supply chain especially such threats as:

- device driver manipulation
- shimming; call interrupting code (code refactoring)

MANAGING RISK: RISK ASSESSMENT

Penetration testing authorization and vulnerability testing authorization should be obtained before any test begin. These protect you and limit your responsibility. At a base minimum they should cover:

- legal authorization
- indemnification
- limit retaliation

Change Management: a methodology for making changes to a system and keeping track of those changes; this can also be a review (check up):

- privilege management; access rights
- incident management

MANAGING RISK: RISK CALCULATION

Qualitative Risk Calculation: an *educated guess* based on observation; customer database given a higher asset value. (1-10 or High, Medium, Low)

Quantitative Risk Calculation: attempts to create a *hard* number associated with the risk of an element in a system by using historical data; can be grouped by likelihood and impact of risk.

Annualized Rate of Occurrence (ARO): the likelihood of a risk occurring within any given year based on historical data.

MANAGING RISK: RISK CALCULATION

Single Loss Expectancy (SLE): expected monetary loss every time a risk occurs

Annualized Loss Expectancy (ALE): expected monetary loss that can be expected for an asset due to risk over a one-year period.

Risk Register: a list of potential threats and associated risks.

STRATEGIES FOR REDUCING RISK

Security Control: any device or process that is used to reduce risk.

Administrative Controls: the process for developing and ensuring that policies and procedures are carried out; user actions of may do, must do, cannot do.

Technical Controls: security controls carried out or managed by devices.

Activity Phase Controls: subtypes of the two main levels of controls types; can be administrative or technical.

STRATEGIES FOR REDUCING RISK: ACTIVITY PHASE CONTROLS

Control Name	Description	When it occurs	Example
Deterrent	Discourage attack	Before attack	Signs indicating that the area is under video surveillance
Preventative	Prevent attack	Before attack	Security awareness training for all users
Physical	Prevent attack	Before attack	Fences that surround the perimeter
Detective	Identify attack	During attack	Installing motion detection sensors
Compensating	Alt. to normal control	During attack	An infected computer isolated on a different network
Corrective	Lesson attack damage	After attack	A virus is cleaned from an infected server

STRATEGIES FOR REDUCING RISK

Distributive Allocation is distributing risk as your organization might face.

- Transference; 3rd party
- Avoidance; avoid the activity
- Mitigation; make it less serious

Automated Course of Action is turing to automation (robots) which comes with added benefits:

- scalability
- elasticity
- continuous monitoring
- configuration validation

STRATEGIES FOR REDUCING RISK

Non-persistence Tools: used to ensure that unwanted data is not carried forward.

Tool name	Description	How its used
Live boot media	A *lightweight* bootable image on a USB flash drive or optical media	Temporarily creates a secure, non-persistent client for use on a public computer for accessing a secure remote network
Revert to known state	Restore device to a previous secure condition	Used to reset a device to a stable and secure setting
Rollback to known configuration	Undo recent changes that cause errors or weaken security	Can restore a device to a previous configuration
Snapshot	An instance (image) of a virtual machine	Used to replace a corrupted or infected virtual machine

PRACTICES FOR REDUCING RISK

Security Policy: a written document that states how an organization plans to protect the company's information technology assets; see page 671 for types.

Acceptable Use Policy (AUP): a policy that defines the actions users may perform while accessing systems and networking equipment.

Personal Email Policy: a policy that determines how employees can and should use email; business use only, business access only, forwarding emails, etc.

Social Media Policy: a policy that determines how employees can and should use social media for the business.

PRACTICES FOR REDUCING RISK: AGREEMENTS

Service Level Agreement (SLA): a service contract between a vendor and a client that specifies what services will be provided, responsibilities of each party, and any guarantees of service.

Blanket Purchase Agreement (BPA): a prearranged purchase or sale agreement between a government agency and a business; used for repetitive needs.

Memorandum of Understanding: describes an agreement between two or more parties; a *convergence of will* but usually not legally enforceable.

Non-disclosure Agreement (NDA): a legal contract between parties that specify how confidential material will be shared between parties but restricted to others.