SEZG566/SSZG566

Secure Software Engineering

Managing for Security

T V Rao

BITS Pilani

Pilani | Dubai | Goa | Hyderabad

- *The slides presented here are obtained from the authors of the books, product documentations, and from various other contributors. I hereby acknowledge all the contributors for their material and inputs.*
- *I have added and modified slides to suit the requirements of the course.*

BITS Pilani

Pilani | Dubai | Goa | Hyderabad

DARPA IDS Data

DARPA IDS Data

- The intrusion detection learning task is to build a predictive model capable of distinguishing between ``bad'' connections, called intrusions or attacks, and ``good'' normal connections
- The 1998 DARPA Intrusion Detection Evaluation Program was prepared and managed by MIT Lincoln Labs
  - A standard set of data to be audited, which includes a wide variety of intrusions simulated in a military network environment, was provided.
  - The 1999 KDD intrusion detection contest uses a version of this dataset

DARPA IDS Data

http://www.cs.uccs.edu/~jkalita/papers/2015/BhuyanMonowarIJNS2005.pdf

Page 16: List of features in the KDDcup99 intrusion dataset

Challenges in having a good dataset and relevant efforts:

https://www.semanticscholar.org/paper/Toward-Generating-a-New-Intrusion-Detection-Dataset-Sharafaldin-Lashkari/a27089efabc5f4abd5ddf2be2a409bff41f31199

BITS Pilani

Pilani | Dubai | Goa | Hyderabad

Governance for Security

Governance vs. Management

- IT governance is a framework for decision rights and accountability to encourage desirable behavior in the use of IT.
- IT management is the daily decision making and implementation activities around the firm's use of IT.
- Governance identifies who will make key IT decisions and how will they be held accountable.
  - Good governance is enabling action and reduces bureaucracy and dysfunctional politics by formalizing organizational learning and thus avoiding the trap of repeating the same mistakes.

Governance vs. Management

Governance	Management
Oversight	Implementation
Authorizes decision rights	Authorized to make decisions
Enact policy	Enforce policy
Accountability	Responsibility
Strategic planning	Project planning
Resource allocation	Resource utilization

Governance for Security

- According to NIST, IT governance is the process of establishing and maintaining a framework to provide assurance that information security strategies
  - are aligned with and support business objectives,
  - are consistent with applicable laws and regulations through adherence to policies and internal controls, and
  - provide assignment of responsibility,

all in an effort to manage risk

Governance for Security

Characteristics of effective security governance

- It is an institution-wide issue
- Leaders are accountable
- It is viewed as an institutional requirement (cost of doing business)
- It is risk-based
- Roles, responsibilities and segregation of duties are defined
- It is addressed and enforced in policy
- Adequate resources are committed
- Staff are aware and trained
- A development life cycle is required
- It is planned, managed, measureable and measured
- It is reviewed and audited

BITS Pilani

Pilani | Dubai | Goa | Hyderabad

IT Security Controls

IT Security Controls

Control is defined as:

"An action, device, procedure, or other measure that reduces risk by eliminating or preventing a security violation, by minimizing the harm it can cause, or by discovering and reporting it to enable corrective action."

Management controls

- Focus on security policies, planning, guidelines, and standards that influence the selection of operational and technical controls to reduce the risk of loss and to protect the organization's mission
- These controls refer to issues that management needs to address

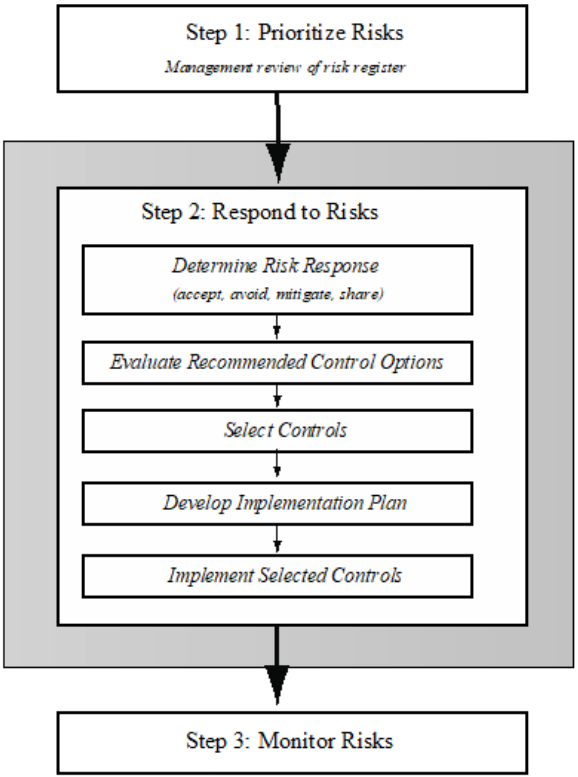
Operational controls

- Address the correct implementation and use of security policies and standards, ensuring consistency in security operations and correcting identified operational deficiencies
- These controls relate to mechanisms and procedures that are primarily implemented by people rather than systems
- They are used to improve the security of a system or group of systems

Technical controls

- Involve the correct use of hardware and software security capabilities in systems
- These range from simple to complex measures that work together to secure critical and sensitive data, information, and IT systems functions

IT Security Controls address Risks

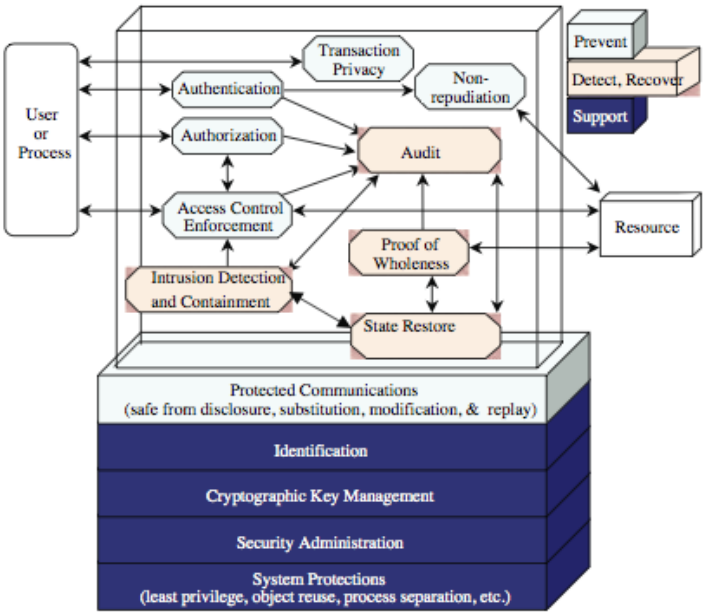


Technical Controls

Supportive: generic, underlying technical IT capabilities

Preventive: focus on preventing security breaches
by warning of violations

Detection/recovery: focus on response to a security breach



Proof of Wholeness : In order to determine that integrity has been compromised, the ability must exist to detect when information or system state is potentially corrupted. The proof of wholeness service provides this ability.

NIST SP800-53 Security Controls

CLASS	CONTROL FAMILY
Management	Planning
Management	Program Management
Management	Risk Assessment
Management	Security Assessment and Authorization
Management	System and Services Acquisition
Operational	Awareness and Training
Operational	Configuration Management
Operational	Contingency Planning
Operational	Incident Response
Operational	Maintenance
Operational	Media Protection
Operational	Personnel Security
Operational	Physical and Environmental Protection
Operational	System and Information Integrity
Technical	Access Control
Technical	Audit and Accountability
Technical	Identification and Authentication
Technical	System and Communications Protection

BITS Pilani

Pilani | Dubai | Goa | Hyderabad

Managing for Security

IT Security Management Overview

Is the formal process of answering the questions:

Ensures that critical assets are sufficiently protected in a cost-effective manner

Security risk assessment is needed for each asset in the organization that requires protection

Provides the information necessary to decide what management, operational, and technical controls are needed to reduce the risks identified

Security Policy

- Organizations are expected to have a security policy in order to bring all stakeholders together.
- Security Policy may address
  - Scope and purpose including relation of objectives to business, legal, regulatory requirements
  - IT security requirements
  - Assignment of responsibilities
  - Risk management approach

Organizational Context and Security Policy

- Maintained and updated regularly
  - Using periodic security reviews
  - Reflect changing technical/risk environments
- Examine role and importance of IT systems in organization

First examine organization's IT security:

Objectives - wanted IT security outcomes

Strategies - how to meet objectives

Policies - identify what needs to be done

Security Policy

Security Policy is also expected to address

- Security awareness and training
- General personnel issues and any legal sanctions
- Integration of security into systems development
- Information classification scheme
- Contingency and business continuity planning
- Incident detection and handling processes
- How, when policy reviewed, and change control to it

Management Support

- IT security policy must be supported by senior management
- Need IT security officer
  - to provide consistent overall supervision
  - manage process
  - handle incidents
- Large organizations need IT security officers on major projects/teams
  - manage process within their areas

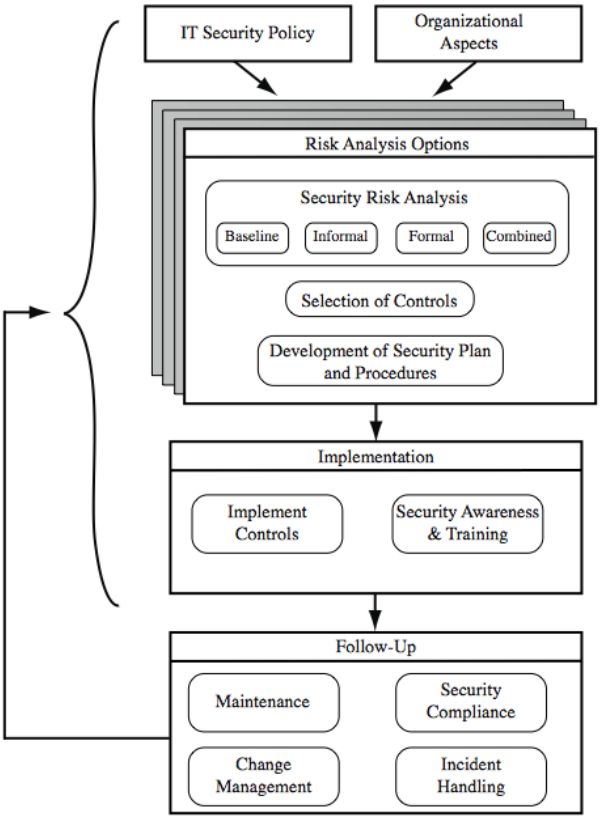
IT Security Management

- **IT Security Management:** a process used to achieve and maintain appropriate levels of
  - Confidentiality,
  - Integrity,
  - Availability,
  - Accountability,
  - Authenticity and
  - Reliability

IT Security Management

- IT security management functions include:
  - Help determine organizational IT security objectives, strategies and policies
  - Help determining organizational IT security requirements
  - Identifying and analyzing security threats to IT assets
  - Identifying and analyzing risks
  - Specifying appropriate safeguards
  - Monitoring the implementation and operation of safeguards
  - Developing and implement a security awareness program
  - Detecting and reacting to incidents

IT Security Management Process



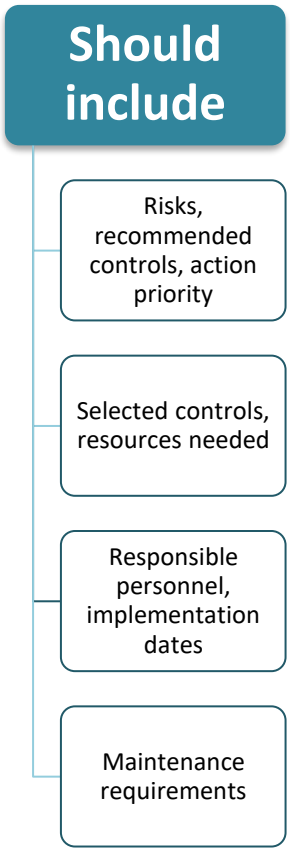
Adapted from ISO 27005 (*Information security risk management,* 2005)

IT Security Plan

Provides details of:

- What will be done
- What resources are needed
- Who is responsible

Goal is to detail the actions needed to improve the identified deficiencies in the risk profile

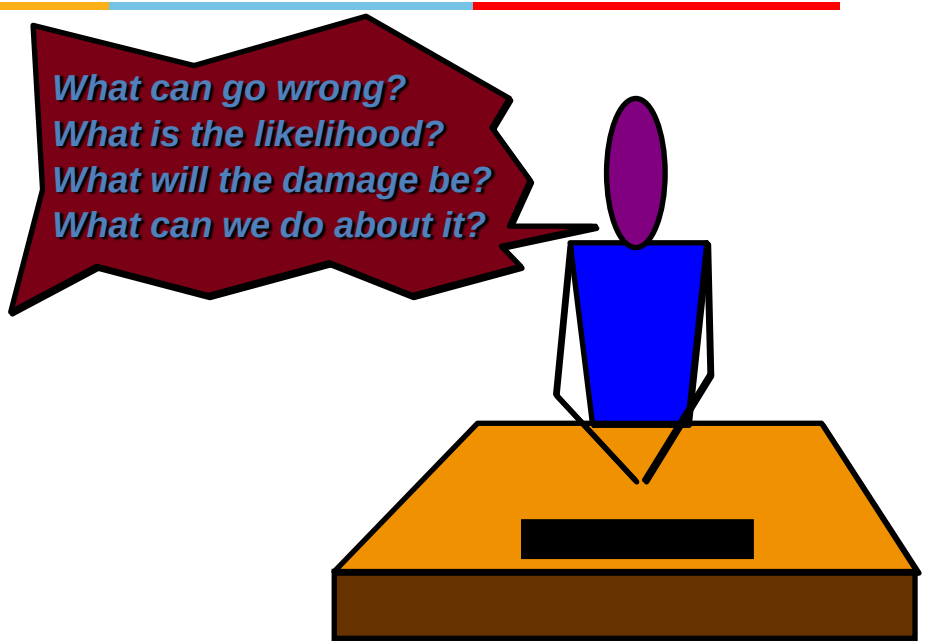


BITS Pilani

Pilani | Dubai | Goa | Hyderabad

Risk Management

Risk Management



The time to repair the roof is when the sun is shining.

John F. Kennedy

Definition of Risk

- A risk is a potential problem – it might happen and it might not
- Conceptual definition of risk
  - Risk concerns future happenings
  - Risk involves change in mind, opinion, event, action, place, etc.
  - Risk involves choice and the uncertainty that choice entails
- Two characteristics of risk
  - Uncertainty – the risk may or may not happen, that is, there are no 100% risks (those, instead, are called constraints)
  - Loss – the risk becomes a reality and unwanted consequences or losses occur

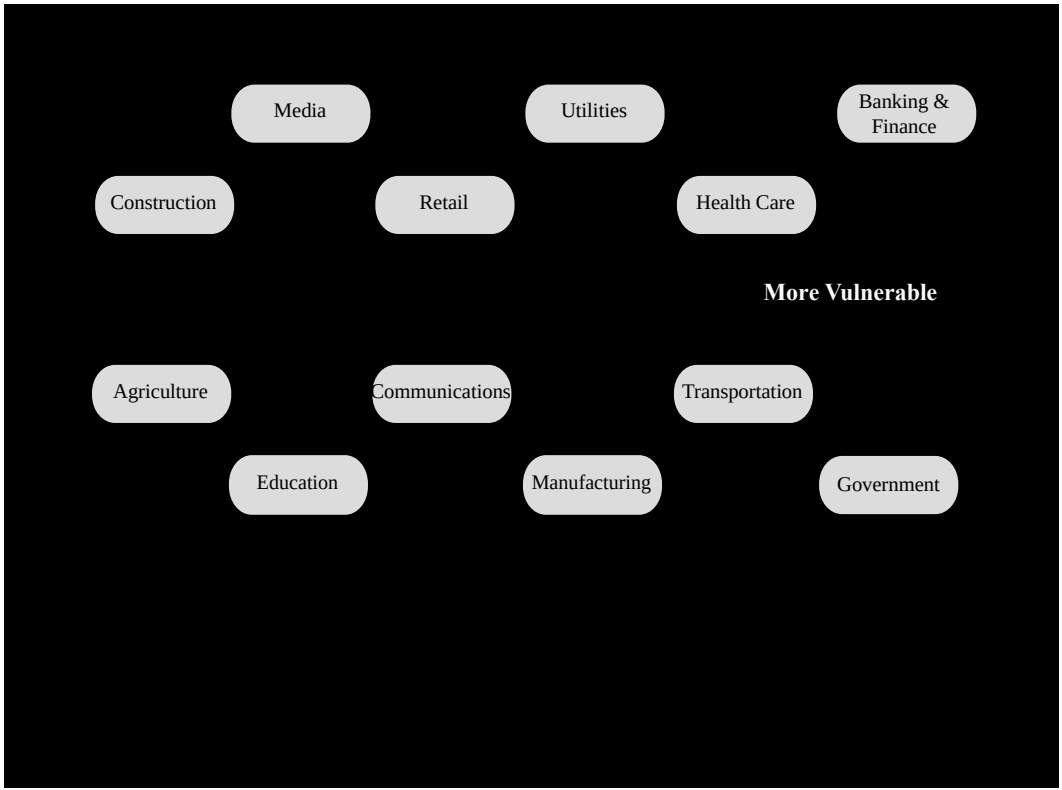
Security Risk Assessment

- Critical component of process
  - else may have vulnerabilities or waste money
- Ideally examine every asset vs risk
  - not feasible in practice
- Choose one of possible alternatives based on organization's resources and risk profile
  - Baseline - use "industry best practice", implement safeguards against most common threats
  - Informal - informal, pragmatic risk analysis with knowledge and expertise of analyst
  - Formal - most comprehensive, costly and slow
  - Combined – formal assessment for critical assets, risks

Detailed Risk Analysis Process

1. System Characterization
2. Threat Identification
3. Vulnerability Identification
4. Control Analysis
5. Likelihood Determination
6. Impact Analysis
7. Risk Determination
8. Control Recommendations
9. Result Documentation

Generic Organizational Risk Context



Adapted from an IDC 2000 report. Landscape might have evolved since then.

Risk Terminology (Stallings)

Asset:	A system resource or capability of value to its owner that requires protection
Threat:	A potential for a threat source to exploit a vulnerability in some asset, which if it occurs may compromise the security of the asset and cause harm to the asset's owner
Vulnerability:	A flaw or weakness in an asset's design, implementation, or operation and management that could be exploited by some threat
Risk:	The potential for loss computed as the combination of the likelihood that a given threat exploits some vulnerability to an asset, and the magnitude of harmful consequence that results to the asset's owner

Threats/Vulnerabilities identification

Threats may be

- Natural “acts of God”
- Man-made
- Accidental or Deliberate

For a deliberate attacker, consider

- Motivation
- Capability
- Resources
- Probability of Attack
- Deterrence

Past experience can be a guide

- Identify exploitable flaws or weaknesses in organization’s IT systems or processes
- Determines applicability and significance of threat to organization
- Need combination of threat and vulnerability to create a risk to an asset
- Outcome should be a list of threats and vulnerabilities with brief descriptions of how and why they might occur

Analyze Risks

- Specify likelihood of occurrence of each identified threat to asset given existing controls
- Specify consequence should threat occur
- Derive overall risk rating for each threat
  - Risk = probability threat occurs x cost to organization
- Hard to determine accurate probabilities and realistic cost consequences
- Use qualitative, not quantitative ratings

Risk Determination

	Consequences					
Likelihood	**Doomsday**	**Catastrophic**	**Major**	**Moderate**	**Minor**	**Insignificant**
Almost Certain	E	E	E	E	H	H
Likely	E	E	E	H	H	M
Possible	E	E	E	H	M	L
Unlikely	E	E	H	M	L	L
Rare	E	H	H	M	L	L

Risk Level	Description
Extreme (E)	Will require detailed research and management planning at an executive/director level. Ongoing planning and monitoring will be required with regular reviews. Substantial adjustment of controls to manage the risk are expected, with costs possibly exceeding original forecasts.
High (H)	Requires management attention, but management and planning can be left to senior project or team leaders. Ongoing planning and monitoring with regular reviews are likely, though adjustment of controls are likely to be met from within existing resources
Medium (M)	Can be managed by existing specific monitoring and response procedures. Management by employees is suitable with appropriate monitoring and reviews.
Low (L)	Can be managed through routine procedures.

Risk Handling/Treatment Alternatives

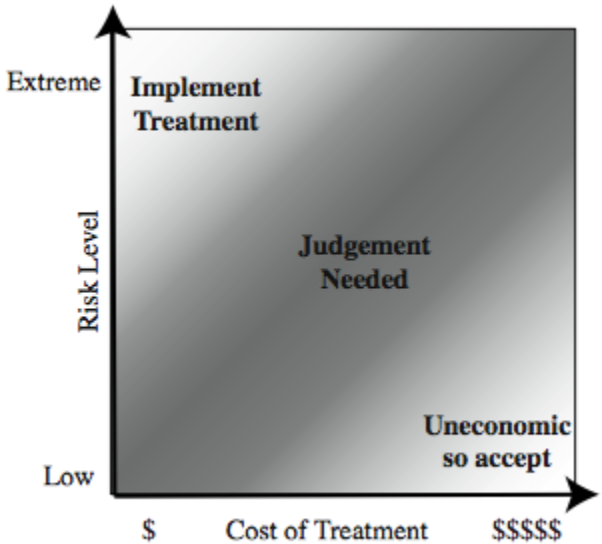
risk acceptance: *accept risk (perhaps because of excessive cost of risk treatment)*

risk avoidance: *do not proceed with the activity that causes the risk (loss of convenience)*

risk transfer: buy insurance; outsource

reduce consequence: *modify the uses of an asset to reduce risk impact (e.g., offsite backup)*

reduce likelihood: *implement suitable controls*



BITS Pilani

Pilani | Dubai | Goa | Hyderabad

Case Study: Silver Star Mines
(Stallings)

Establishing the Context

- Initial step
  - Determine the basic parameters of the risk assessment
  - Identify the assets to be examined
- Explores political and social environment in which the organization operates
  - Legal and regulatory constraints
  - Provide baseline for organization's risk exposure
- Risk appetite
  - The level of risk the organization views as acceptable

Case Study: Silver Star Mines

- Fictional operation of global mining company
- Large IT infrastructure
  - both common and specific software
  - some directly relates to health & safety
  - formerly isolated systems now networked
- Decided on combined approach
- Mining industry less risky end of spectrum
- Management accepts moderate or low risk

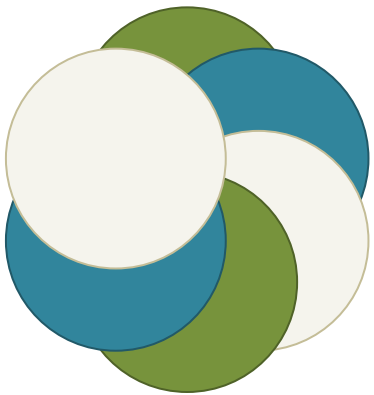
Asset Identification

- Draw on expertise of people in relevant areas of organization to identify key assets
  - Identify and interview such personnel

What is an Asset

- "anything that needs to be protected" because it has value to the organization and contributes to the successful attainment of the organization's objectives

Assets



Reliability and integrity of SCADA nodes and net

Availability, integrity and confidentiality of mail services

Integrity of stored file and database information

Availability, integrity of maintenance/producti on system

Availability, integrity of financial system

Availability, integrity of procurement system

Supervisory control and data acquisition (**SCADA**) is a system for remote monitoring and control for distributed industrial processes

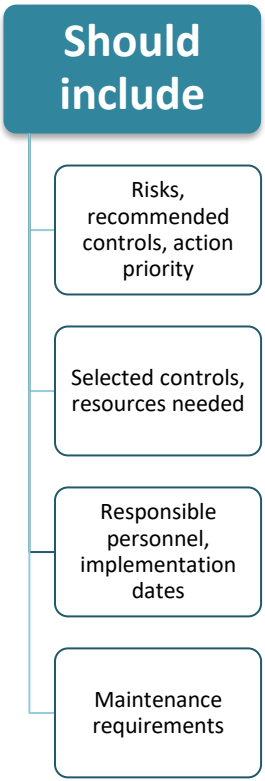
Risk Register

Asset	Threat/ Vulnerability	Existing Controls	Likelihood	Consequence	Level of Risk	Risk Priority
Reliability and integrity of the SCADA nodes and network	Unauthorized modification of control system	Layered firewalls and servers	Rare	Major	High	1
Internet Router	Outside hacker attack	Admin password only	Possible	Moderate	High	2
Availability and integrity of financial system	Attacks/errors affecting system	Firewall, policies	Possible	Moderate	High	3
Availability and integrity of procurement system	Attacks/errors affecting system	Firewall, policies	Possible	Moderate	High	4
Availability and integrity of maintenance/ production system	Attacks/errors affecting system	Firewall, policies	Possible	Minor	Medium	5
Availability, integrity and confidentiality of mail services	Attacks/errors affecting system	Firewall, ext mail gateway	Almost Certain	Minor	High	6

IT Security Plan

Provides details of:

- What will be done
- What resources are needed
- Who is responsible
- Goal is to detail the actions needed to improve the identified deficiencies in the risk profile



Implementation Plan

Risk (Asset/Threat)	Hacker attack on Internet router
Level of Risk	High
Recommended Controls	•Disable external telnet access •Use detailed auditing of privileged command use •Set policy for strong admin passwords •Set backup strategy for router configuration file •Set change control policy for the router configuration
Priority	High
Selected Controls	•Implement all recommended controls •Update related procedures with training for affected staff
Required Resources	•3 days IT net admin time to change & verify router configuration, write policies; •1 day of training for network administration staff
Responsible Persons	John Doe, Lead Network System Administrator, Corporate IT Support Team
Start – End Date	February 6, 2017 to February 9, 2017
Other Comments	•Need periodic test and review of configuration and policy use

BITS Pilani

Pilani | Dubai | Goa | Hyderabad

Cognitive Bias

You have a Choice!

- Given a choice what do you prefer?

  a) A cash of Rs 10000/-

  b) A coin flip – you will get Rs 20000/- if you win.

You have a Choice!

- Given a choice what do you prefer?

  a) Pay a fine of Rs 10000/-

  b) A coin flip – you will pay nothing if you win, but Rs 20000/- if you lose.

Prospect theory

- Prospect theory (proposed by Noble laureate Daniel Kahneman et al.) is a behavioral economic theory that describes the way people choose between probabilistic alternatives that involve risk, where the probabilities of outcomes are known.
- Prospect theory shows that a loss is more significant than the equivalent gain, that a sure gain is favored over a probabilistic gain, and that a probabilistic loss is preferred to a definite loss.
- This is considered Framing effect or cognitive bias

Prospect theory/Cognitive Bias

Amos Tversky and Daniel Kahneman explored how different phrasing affected participants' responses to a choice in a hypothetical life and death situation in 1981.

Participants were asked to choose between two treatments for 600 people affected by a deadly disease. Treatment A was predicted to result in 400 deaths, whereas treatment B had a 33% chance that no one would die but a 66% chance that everyone would die. This choice was then presented to participants either with positive framing, i.e. how many people would live, or with negative framing, i.e. how many people would die.

Framing	Treatment A	Treatment B
Positive	"Saves 200 lives"	"A 33% chance of saving all 600 people, 66% possibility of saving no one."
Negative	"400 people will die"	"A 33% chance that no people will die, 66% probability that all 600 will die."

Treatment A was chosen by 72% of participants when it was presented with positive framing ("saves 200 lives") dropping to only 22% when the same choice was presented with negative framing ("400 people will die").

Prospect theory/Information Security

- How does Prospect theory/Cognitive bias (due to framing effect) impact information security
  - Last month, we managed our assets without security investments
  - Do we need expensive protection mechanism now?
  - Can we do with a low-cost solution?

Bruce Schneier cryptographer, computer security and privacy specialist, and writer

BITS Pilani

Pilani | Dubai | Goa | Hyderabad

Security Incident Handling

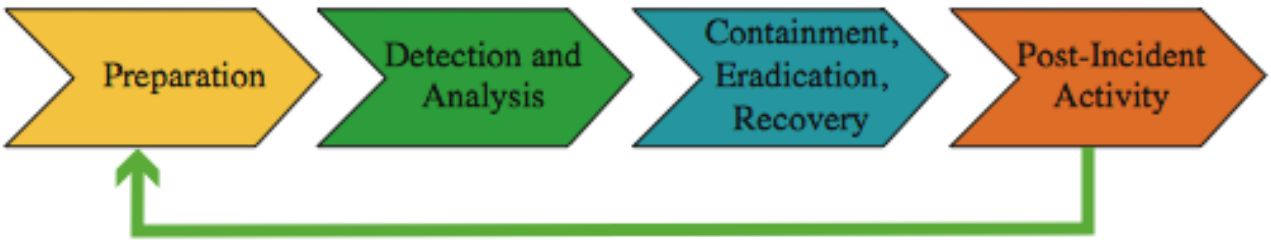
Incident Handling: Essential Control

- Need procedures specifying how to respond to a security incident
  - given it will most likely occur sometime
- Codify action to avoid panic e.g. mass email worm
  - exploiting vulnerabilities in common apps
  - propagating via email in high volumes
  - should disconnect from Internet or not?
    - responsible individual should make a decision (the policy should indicate how to contact the individual)

Types of Security Incidents

- Any action threatening classic security services
- Unauthorized access to a system
  - unauthorized viewing by self/other of information
  - bypassing access controls
  - using another user's access
  - denying access to another user
- Unauthorized modification of info on a system
  - corrupting information
  - changing information without authorization
  - unauthorized processing of information

Managing Security Incidents



Managing Security Incidents

innovate achieve lead

Detecting Incidents

- Reports from users or admin staff
  - train and encourage such reporting
- Detected by automated tools
  - e.g. system integrity verification tools, log analysis tools, network and host intrusion detection systems, intrusion prevention systems
  - updated to reflect new attacks or vulnerabilities
- Admins must monitor vulnerability reports

Responding to Incidents

- Need documented response procedures
- Procedures should
  - identify typical categories of incidents and approach taken to respond
  - identify management personnel responsible for making critical decisions and their contacts
  - whether to report incident to police/CERT etc

Documenting Incidents

Need to identify vulnerability used

- how to prevent it occurring in future

Recorded details for future reference

Consider impact on org and risk profile

- may simply be unlucky
- more likely risk profile has changed
- hence risk assessment needs reviewing
- followed by reviewing controls in use

Computer Security: Principles and Practice by William Stallings, and Lawrie Brown Pearson, 2020.
Software Security Engineering, Julia H. Allen, et al, Pearson, 2008
sei.cmu.edu/cert
www.owasp.com

Thank You!