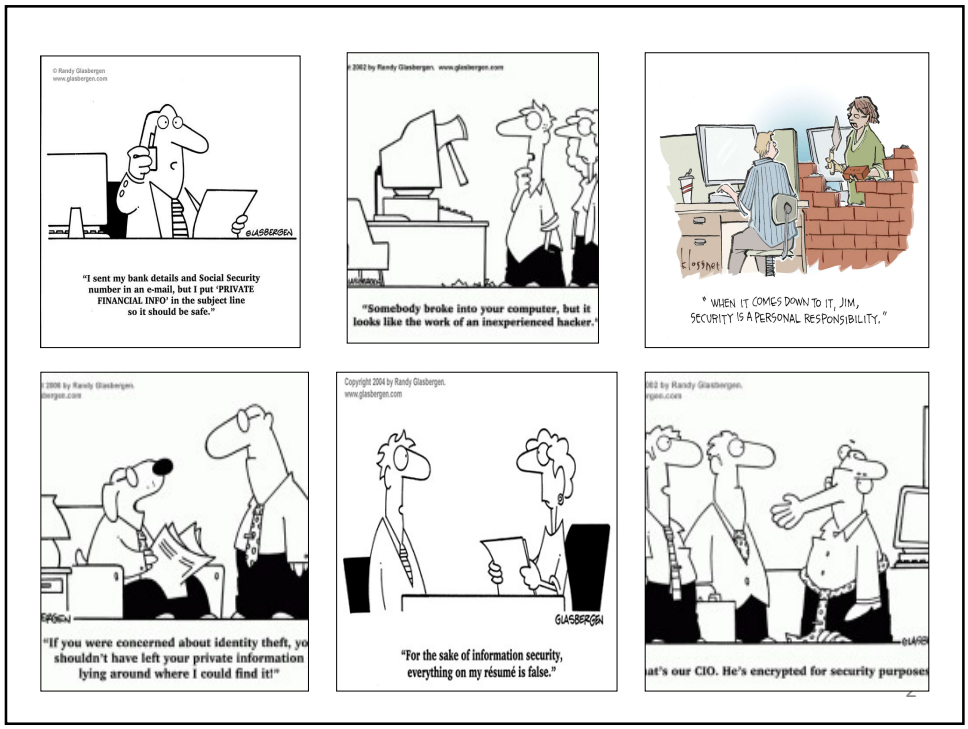

Management of
Information Security
1

1


"I sent my bank details and Social Security number in an e-mail, but I put 'PRIVATE FINANCIAL INFO' in the subject line so it should be safe."
"Somebody broke into your computer, but it looks like the work of an inexperienced hacker."
" WHEN IT COMES DOWN TO IT, JIM, SECURITY IS A PERSONAL RESPONSIBILITY."
"If you were concerned about identity theft, yo shouldn't have left your private information lying around where I could find it!"
"For the sake of information security, everything on my résumé is false."
at's our CIO. He's encrypted for security purposes

2

Agenda

- **Information Security and Cyber Security**
- **Ten Commandments and Ethics**
- **Objectives / Principles / Functions of Information Security**
- **CIA**
- **Threats and Vulnerabilities**
- **Risk Management**
- **Controls**
- **Cyber Frauds**
- **Incident Management/ DR/ BC/ Crisis Management**

3

3

What Is Security?

- In general, security means being free from danger. To be secure is to be protected from the risk of loss, damage, unwanted modification, or other hazards
- Achieving an appropriate level of security for an organization also depends on the implementation of a multilayered system
- Security is often achieved by means of several strategies undertaken simultaneously or used in combination with one another
- It is the role of management to ensure that each strategy is properly planned, organized, staffed, directed, and controlled

4

Cyber space

"A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."

- NIST

5

Defining Cyber Security / Information Security

- **Cyber security** is the ability to protect or defend the use of cyberspace from cyber attacks.
- **Cyber security** is all about the security of anything in the cyber realm.
- C**yber Security** is protecting our cyberspace from attack, damage, misuse, and economic espionage.

- An Information System (IS) can be any ***organized combination of people, hardware, software, communications networks, data resources, and policies and procedures that stores, retrieves, transforms, and disseminates information in an organization***
- **Information security** is all about the security of information regardless of the realm.

6

Areas of Information Security

- Specialized areas of security include:
  - Physical security
  - Operations security
  - Communications security
  - Cyber (or computer) security
  - Network security

7

Information Security

- Information security (InfoSec) focuses on the protection of information and the characteristics that give it value, such as **confidentiality**, **integrity**, and **availability**, and includes the technology that houses and transfers that information through a variety of protection mechanisms such as **policy**, **training and awareness** programs, and **technology**

8

Elements of Information Security

1. Information security supports the mission of the organization.
2. Information security is an integral element of sound management.
3. Information security protections are implemented so as to commensurate with risk.
4. Information security roles and responsibilities are made explicit.
5. Information security responsibilities for system owners go beyond their own organization.
6. Information security requires a comprehensive and integrated approach.
7. Information security is assessed and monitored regularly.
8. Information security is constrained by societal and cultural factors.

Source: NIST SP 800-12 REV. 1

9

9

The Ten Commandments of Computer Ethics (Computer Ethics Institute)

1. Thou shalt not use a computer to harm other people
2. Thou shalt not interfere with other people's computer work
3. Thou shalt not snoop around in other people's computer files
4. Thou shalt not use a computer to steal
5. Thou shalt not use a computer to bear false witness
6. Thou shalt not copy or use proprietary software for which you have not paid
7. Thou shalt not use other people's computer resources without authorization or proper compensation
8. Thou shalt not appropriate other people's intellectual output
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing
10. Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans

(Source: Computer Professionals for Social Responsibility)

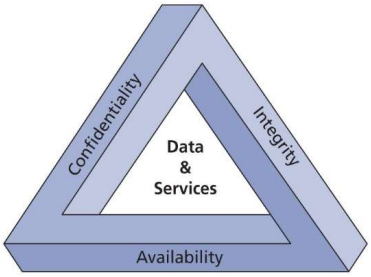
10

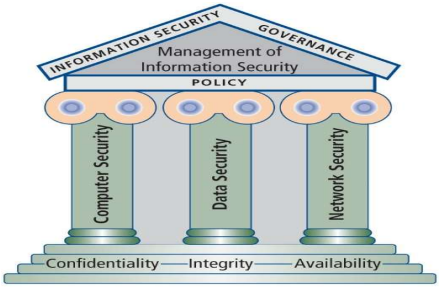
Components of an Information System

Information System (IS) is entire set of Software, Hardware, Data, People, Policies/Procedures, and networks necessary to use information as a resource in the organization

The value of information comes from the characteristics it possesses:

- Confidentiality
- Integrity
- Availability





11

Information Security - Objectives

The objective of information security is protecting the interests of those relying on information and the systems and communications that deliver the information from harm resulting from failures of availability, confidentiality and integrity.

For most computer users, the **security objective** is met when:

1. Information systems are available and usable when required, and can appropriately resist attacks and recover from failures (**Availability**)
2. Information is observed by or disclosed to only those who have a right to know (**Confidentiality)**
3. Information is protected against unauthorized modification or error so that accuracy, completeness and validity are maintained (**Integrity)**
4. Business transactions and information exchanges between enterprises, customers, suppliers, partners and regulators can be trusted (**Authenticity and Non-Repudiation)**
5. **Non-Repudiation** Protection against an individual falsely denying having performed a particular action. Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message.

12

12

Confidentiality

- Confidentiality is "**an attribute of information that describes how data is protected from disclosure or exposure to unauthorized individuals or systems**"
- ***Confidentiality means limiting access to information only to those who need it, and preventing access by those who do not***
- To protect the confidentiality of information, a number of measures are used:
  - Information classification
  - Secure document (and data) storage
  - Application of general security policies
  - Education of information custodians and end users
  - Cryptography (encryption)

13

Integrity

- Integrity is "**an attribute of information that describes how data is whole, complete, and uncorrupted**"
- The integrity of information is threatened when it is exposed to corruption, damage, destruction, or other disruption of its authentic state
- ***Corruption can occur while information is being entered, stored, processed or transmitted***

14

Availability

- Availability is "**an attribute of information that describes how data is accessible and correctly formatted for use without interference or obstruction**"
- Availability of information means that users, either people or other systems, have access to it in a usable format.
- Availability does not imply that the information is accessible to any user; **rather, it means it can be accessed when needed by *authorized* users**

15

Privacy

- Privacy is, "**in the context of information security, the right of individuals or groups to protect themselves and their information from unauthorized access, providing confidentiality**"
- Information that is collected, used, and stored by an organization is to be used only for the purposes stated by the data owner at the time it was collected
- In this context, ***privacy does not mean freedom from observation; it means that the information will be used only in ways approved by the person who provided it***

16

Identification

- Identification is ***"the access control mechanism whereby unverified entities who seek access to a resource provide a label by which they are known to the system***"
- An information system possesses the characteristic of identification when it is able to recognize individual users
- Identification and authentication are essential to establishing the level of access or authorization that an individual is granted
- Identification is typically performed by means of a user name or other ID

17

Authentication

- Authentication is **"the access control mechanism that requires the validation and verification of an unauthenticated entity's purported identity**"
- It is the process by which a control establishes whether a user (or system) has the identity it claims to have
- Individual users may disclose a personal identification number (PIN), a password, or a passphrase to authenticate their identities to a computer system

18

Authorization

- Authorization is **"the access control mechanism that represents the matching of an authenticated entity to a list of information assets and corresponding access levels**"
- After the identity of a user is authenticated, authorization defines what the user (whether a person or a computer) has been specifically and explicitly permitted by the proper authority to do, such as access, modify, or delete the contents of an information asset

19

Accountability

- Accountability is "**the access control mechanism that ensures all actions on a system—authorized or unauthorized—can be attributed to an authenticated identity. Also known as auditability"**
- Accountability of information occurs when a control provides assurance that every activity undertaken can be attributed to a named person or automated process.
- Accountability is most commonly associated with system audit logs

20

Principles of Information Security Management

21

Principles of Information Security Management

- The unique functions of information security management are known as the **six P**s:

1. Planning
2. Policy
3. Programs
4. Protection
5. People
6. Project management

22

InfoSec Planning

- Planning as part of InfoSec management and includes activities necessary to support the design, creation, and implementation of information security strategies.
- Because the InfoSec strategic plans must support not only the IT use and protection of information assets, but those of the entire organization, it is imperative that the CISO work closely with all senior managers in developing InfoSec strategy

23

InfoSec Planning (Continued)

- Several types of InfoSec plans exist:
  - Incident response planning
  - Business continuity planning
  - Disaster recovery planning
  - Policy planning
  - Personnel planning
  - Technology rollout planning
  - Risk management planning
  - Security program planning including education, training and awareness

24

Policy

- Policy is “a set of organizational guidelines that dictate certain behavior within the organization”.
- In InfoSec, there are three general categories of policy:
  - Enterprise information security policy (EISP)
  - Issue-specific security policy (ISSP)
  - System-specific policies (SysSPs)

25

Programs

- InfoSec operations are specifically managed as separate entities
- A security education training and awareness (SETA) program is one such entity
- Other programs that may emerge include a **physical security program, complete with fire, physical access, gates, guards,** and so on

26

Protection

- The protection function is executed **via a set of risk management activities, including risk assessment and control, as well as protection mechanisms, technologies, and tools**.

27

People

- People are the most critical link in the information security program.
- This area of InfoSec includes security personnel and the security of personnel, as well as aspects of the SETA program mentioned earlier

28

Projects

- The final component is the application of thorough project management discipline to all elements of the information security program.
- Project management involves identifying and controlling the resources applied to the project, as well as measuring progress and adjusting the process as progress is made toward the goal

29

Project Management

- Information security is a process, not a project, however, each element of an information security program must be managed as a project, even if the overall program is perpetually ongoing.
- Information security is both a process and a project. It is, in fact, a continuous series, or chain, of projects.

30

ITGI Approach to Information Security Governance

- According to ISACA's Information Technology Governance Institute (ITGI), InfoSec governance includes the accountabilities and methods undertaken by the board of directors and executive management to provide:
  - strategic direction,
  - establishment of objectives,
  - measurement of progress toward those objectives,
  - verification that risk management practices are appropriate, and
  - validation that the organization's assets are used properly

31

ITGI Approach to Information Security Governance

ITGI recommends that boards of directors supervise strategic InfoSec objectives by:

1. Creating and promoting a culture that recognizes the criticality of information and InfoSec to the organization
2. Verifying that management's investment in InfoSec is properly aligned with organizational strategies and the organization's risk environment
3. Mandating and assuring that a comprehensive InfoSec program is developed and implemented
4. Requiring reports from the various layers of management on the InfoSec program's effectiveness and adequacy

32

Information Security Governance - Desired Outcomes

- **Strategic alignment** of InfoSec with business strategy to support organizational objectives
- **Risk management** by executing appropriate measures to manage and mitigate threats to information resources
- **Resource management** by utilizing InfoSec knowledge and infrastructure efficiently and effectively
- **Performance measurement** by measuring, monitoring, and reporting InfoSec governance metrics to ensure that organizational objectives are achieved
- **Value delivery** by optimizing InfoSec investments in support of organizational objectives

33

NCSP Framework for Information Security Governance

- According to the Corporate Governance Task Force (CGTF), the organization should engage in a core set of activities suited to its needs to guide the development and implementation of the InfoSec governance program:
  - *Conduct an annual InfoSec evaluation, the results of which the CEO should review with staff and then report to the board of directors*
  - *Conduct periodic risk assessments of information assets as part of a risk management program*
  - *Implement policies and procedures based on risk assessments to secure information assets*
  - *Establish a security management structure to assign explicit individual roles, responsibilities, authority, and accountability*

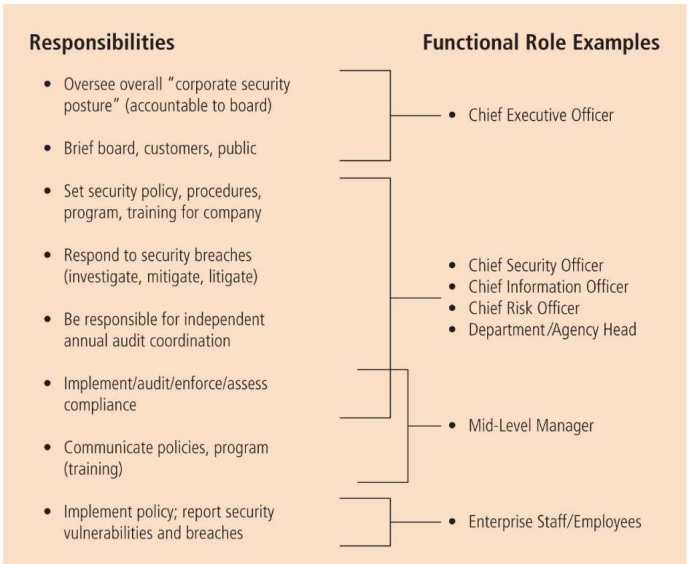
34

NCSP Framework for Information Security Governance

- Develop plans and initiate actions to provide adequate InfoSec for networks, facilities, systems, and information
- Treat InfoSec as an integral part of the system life cycle
- Provide InfoSec awareness, training, and education to personnel
- Conduct periodic testing and evaluation of the effectiveness of InfoSec policies and procedures
- Create and execute a plan for remedial action to address any InfoSec deficiencies
- Develop and implement incident response procedures
- Establish plans, procedures, and tests to provide continuity of operations
- Use security best practices guidance, such as the ISO 27000 series, to measure InfoSec performance

35

Information Security Responsibilities



36

Info Sec Policy

- Policy is the essential foundation of an effective information security program:
  - *The* ***success of an information resources protection program depends on the policy generated, and on the attitude of management toward securing information on automated systems***
  - *You,* ***the policy maker, set the tone and the emphasis on how important a role information security will have within your agency***
  - *Your primary responsibility is to* ***set the information resource security policy for the organization with the objectives of reduced risk, compliance with laws and regulations and assurance of operational continuity, information integrity, and confidentiality***

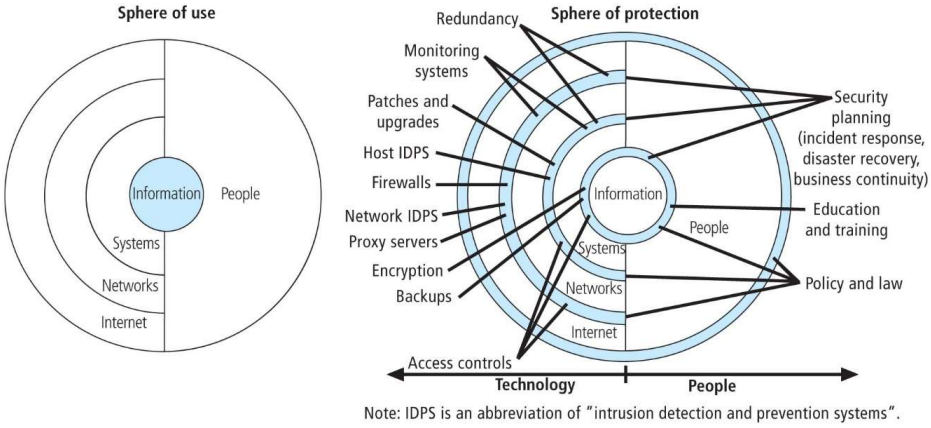
~ (NIST, 1989)

37

Why Policy?

- A quality information security program begins and ends with policy
- In general, **a policy is simply a manager's or other governing body's statement of intent; as such, a policy (document) actually contains multiple policies (statements)**
- Some basic rules must be followed when shaping a policy:
  - Policy should never conflict with law
  - Policy must be able to stand up in court if challenged
  - Policy must be properly supported and administered

38

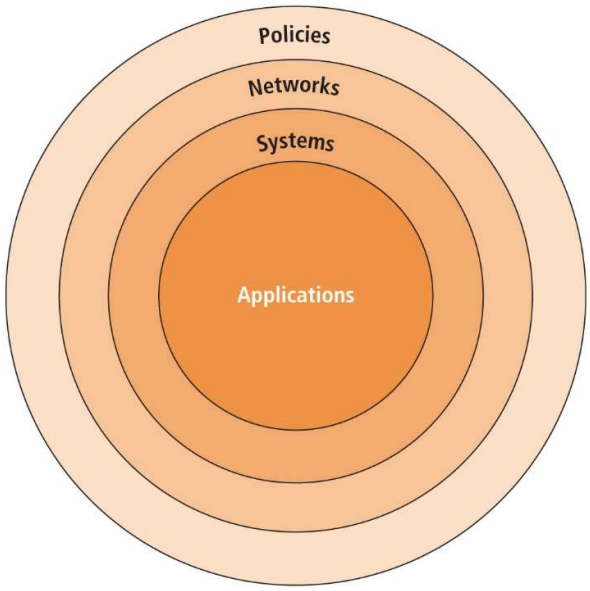


Note: IDPS is an abbreviation of "intrusion detection and prevention systems".

Figure 4-1 Spheres of security

39

Bulls Eye Model



40

Policy-Centric Decision Making

- Bull's-eye model layers:
  - Policies—first layer of defense
  - Networks—threats first meet the organization's network
  - Systems—computers and manufacturing systems
  - Applications—all applications systems

- *Policies are important reference documents for internal audits and for the resolution of legal disputes about management's due diligence [and] policy documents can act as a clear statement of management's intent.*

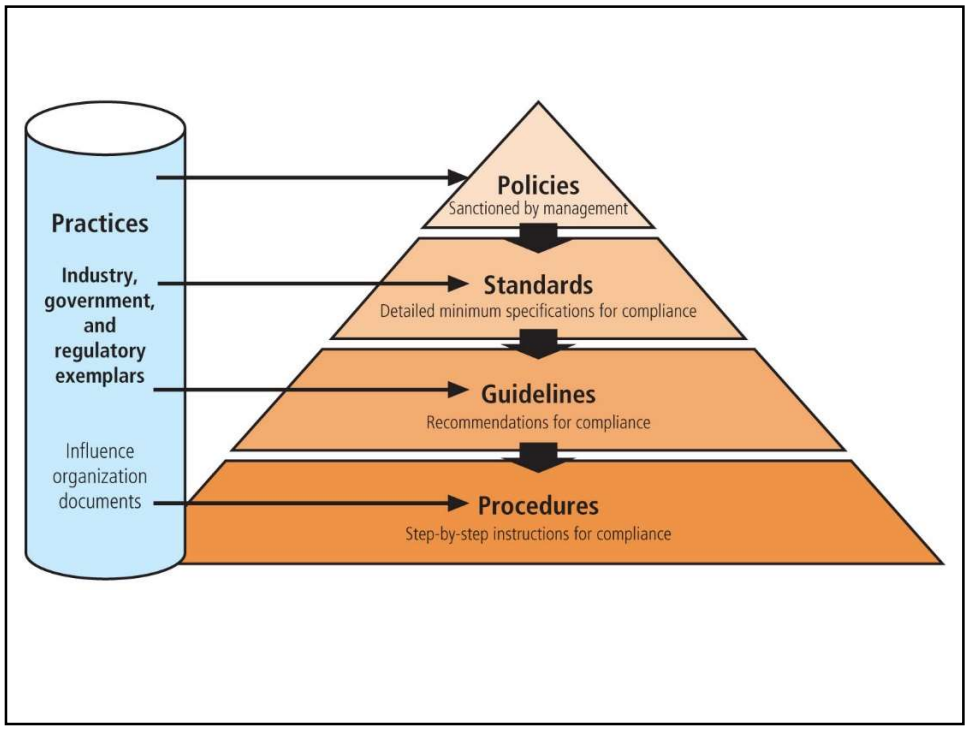
  (Wood, 2012)

41

Policy, Standards, and Practices

- **Policy** is a set of "organizational guidelines that dictate certain behavior within the organization"
- A **standard** is "a detailed statement of what must be done to comply with policy, sometimes viewed as the rules governing policy compliance"
- **Guidelines** are "nonmandatory recommendations the employee may use as a reference in complying with a policy"
- **Procedures** are "step-by-step instructions designed to assist employees in following policies, standards, and guidelines"
- **Practices** are "examples of actions that illustrate compliance with policies"
- **Policies define *what* you can do and not do, whereas the other documents focus on the *how***

42



43

Ethics and Education

- ***Employees must be trained and kept up-to-date on InfoSec topics, including the expected behaviors of an ethical employee.***
- Proper ***ethical and legal education, training and awareness are vital to creating an informed, well-prepared, and low-risk system user***.

44

Implementing SETA Programs

- The SETA program is designed to reduce accidental security breaches by members of the organization
- SETA programs offer three major benefits:
  - ***They can improve employee behavior***
  - ***They can inform members of the organization about where to report violations of policy***
  - ***They enable the organization to hold employees accountable for their actions***
- The purpose of SETA is to enhance security:
  - By building in-depth knowledge, as needed, to design, implement, or operate security programs for organizations and systems
  - By developing skills and knowledge so that computer users can perform their jobs while using IT systems more securely
  - By improving awareness of the need to protect system resources

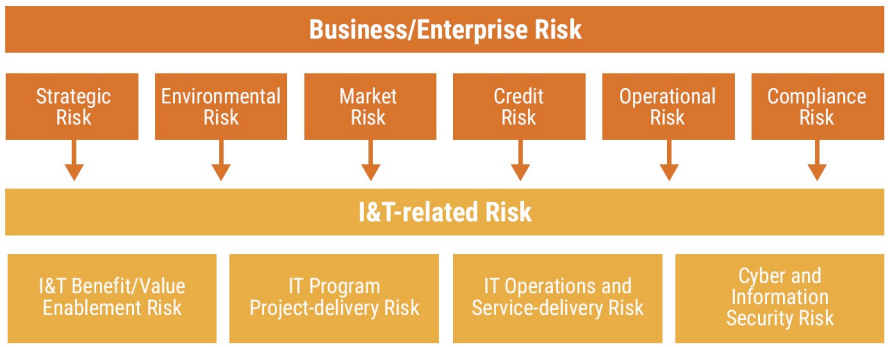
45

Knowing Yourself and Knowing the Enemy

- When operating any kind of organization, a certain amount of risk is always involved.
- For an organization *to* ***manage risk properly, managers should understand how information is collected, processed, stored, and transmitted*** **.**
- Knowing yourself in this context requires ***identifying which information assets are valuable to the organization, categorizing and classifying those assets, and understanding how they are currently being protected.***
- Knowing the enemy means ***identifying, examining, and understanding the threats facing the organization's information assets***

46

I&T Related Risk Relative to Other Major Categories of Risk



47

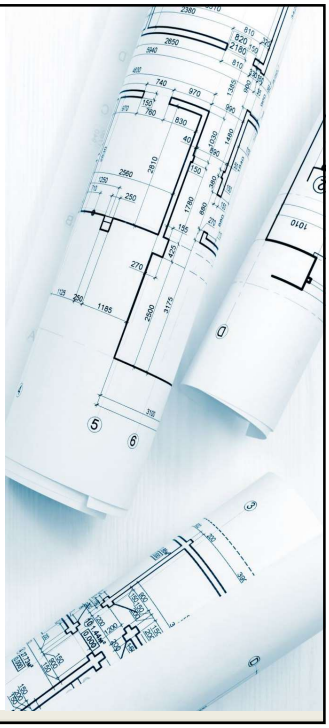
47

Risk Management Process

During the implementation phase of the RM framework, the RM plan guides the implementation of the RM process, in which risk evaluation and remediation of key assets are conducted

The RM process uses the specific knowledge and perspective of the team to complete the following tasks:

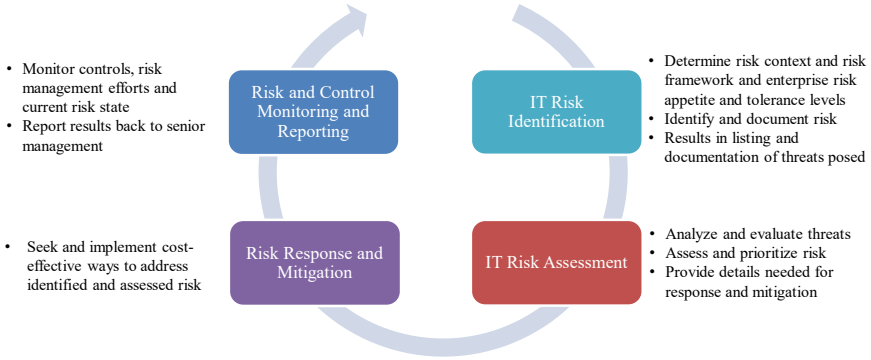
- Establishing the context
- Identifying risk
- Analyzing risk
- Evaluating the risk
- Treating the unacceptable risk
- Summarizing the findings



48

48

IT Risk Management Life Cycle



- Monitor controls, risk management efforts and current risk state
- Report results back to senior management

- Determine risk context and risk framework and enterprise risk appetite and tolerance levels
- Identify and document risk
- Results in listing and documentation of threats posed

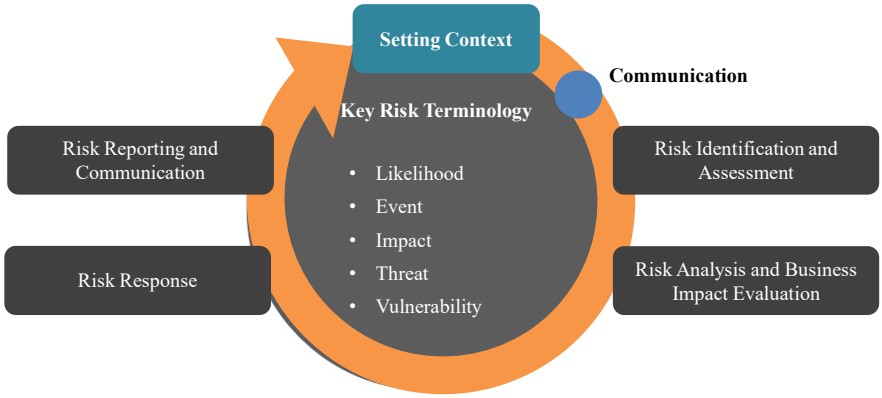
- Seek and implement cost-effective ways to address identified and assessed risk

- Analyze and evaluate threats
- Assess and prioritize risk
- Provide details needed for response and mitigation

49

49

Setting Context for Risk in the Enterprise



50

Key Concepts of Information Security: Threats and Attacks

- A threat represents - a *potential* risk to an information asset, whereas an attack (or threat event) represents an ongoing act against the asset that could result in a loss.
- Threat agents damage or steal an organization's information or physical assets by using exploits to take advantage of a vulnerability where controls are not present or no longer effective
- **Attack:** "an intentional or unintentional act that can damage or otherwise compromise information and the systems that support it"
- **Exploit:** "a technique used to compromise a system… Threat agents may attempt to exploit a system or other information asset by using it illegally for their personal gain"
- **Vulnerability:** "a potential weakness in an asset or its defensive control system(s)"

51

IT-related Business Risk

52

52

Assets Inventory and Documentation

Update to reflect items currently in use when implementing changes or updates

Common requirement in regulations, standards and agreements relating to privacy

Data/information assets

- System(s)
- Source
- Acquisition method
- Business use
- Business criticality
- Availability
- Completeness
- Processing
- Storage
- Transmission
- Sensitivity
- Classification
- Business owner

Hardware Assets

- Equipment
- Supplier
- Acquisition date
- Original cost
- Actual cost
- Location
- Equipment owner
- Maintenance details
- Insurance and warranty data

53

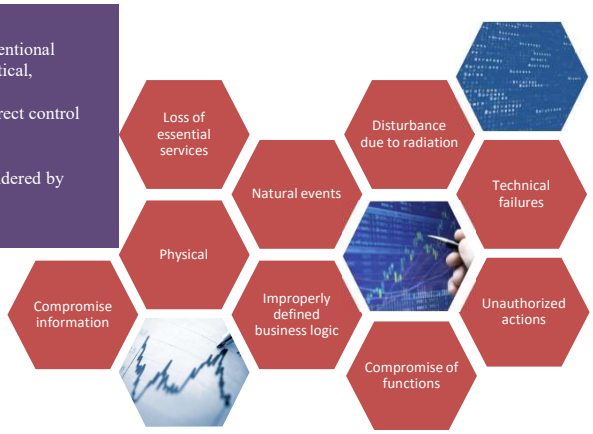
53

Threat Sources

Threats may be divided into multiple categories, including:

Threats are:
- External or internal, intentional or unintentional
- May be caused by natural events or political, economic or competitive factors
- Existing and are typically beyond the direct control of the risk practitioner or asset owner

Not all conceivable threats need to be considered by every enterprise.



54

54

Threats Assessment

- Armed with a properly classified inventory, *you can assess potential weaknesses in each information asset - a process known as threat assessment.*
- Any organization typically faces a wide variety of threats; if you assume that every threat can and will attack every information asset, then the project scope becomes too complex.

55

55

Vulnerability Analysis

Vulnerabilities are weaknesses, gaps in an enterprise's people, processes or technologies that provide an opportunity for a threat actor to exploit, creating consequences that may impact the enterprise.

Many vulnerabilities are system conditions that must be identified to be addressed. The purpose of vulnerability identification is to find problems before an adversary finds and exploits them. An enterprise should conduct regular vulnerability assessments and penetration tests to identify, validate and classify its vulnerabilities. Where vulnerabilities exist, there is a potential for risk.

NIST Special Publication 800-30 Revision 1: Guide to Conducting Risk Assessments provides a list of vulnerabilities to consider with predisposing conditions that may lead to the rapid or unpredictable emergence of new vulnerabilities.

56

56

Sources of Vulnerabilities

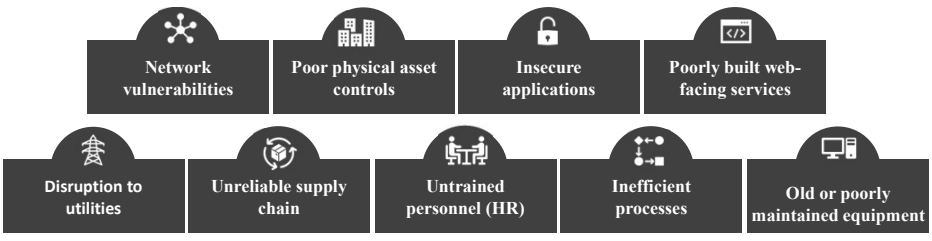
Network:	Misconfiguration of equipment, poor architecture or traffic interception protocols
Physical Access	Allows attackers to potentially bypass other types of controls
Apps/Web Services	Supports business function without due regard to security requirements
Utilities	Power failure or environmental conditions leading to system failure
Supply Chain	Reliance on products, raw materials and supplies from other locations
Equipment	Expectations, goals and objectives of programs and projects
Cloud Computing	Limited view on outsourced enterprise Data centers are large, visible targets
Big Data	Analyze structured and unstructured data for better business decisions

57

57

Vulnerabilities Assessment

- A process of identifying and classifying vulnerabilities
- Provides a careful examination of a target environment to discover any potential points of compromise or weakness



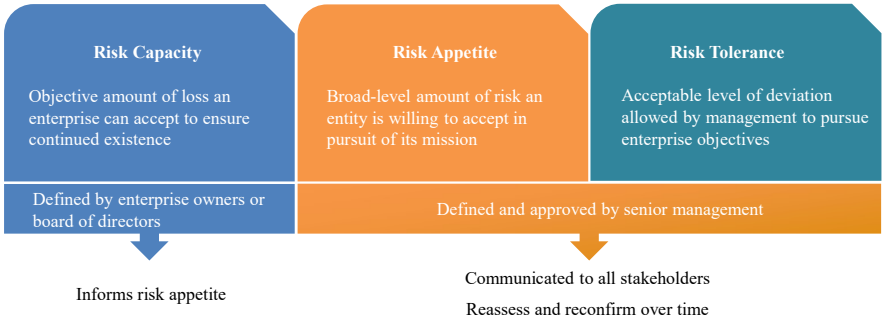
58

TVA

- At the end of the risk identification process, an organization should have
  - a prioritized list of assets and
  - a prioritized list of threats facing those assets
- The prioritized lists of assets and threats can be combined into a Threats-Vulnerabilities-Assets (TVA) worksheet, in preparation for the addition of vulnerability and control information during risk assessment
- This provides a starting point for a risk assessment, along with the other documents and forms

59

Risk Capacity, Appetite and Tolerance



60

Common Types of Fraud

- **Social engineering :**

Fraudsters will use a range of techniques to trick you into sharing banking information or transferring money – usually over the phone, by text message or email. Often criminals use more than one approach to build a level of trust. These tactics are known as social engineering.

E.g., Resist pressure, Beware of emotion, Check who you're talking to, Be suspicious of saviors, Don't divulge information

- **Invoice fraud :**

CEO frauds, Mandate frauds,

https://www.cafonline.org/about-us/security-centre/be-aware---current-threats

https://www.ncsc.gov.uk/guidance/WannaCry-guidance-for-home-users-and-small-businesses

61

Common Types of Fraud

- **Malware and spyware :**

Malicious software, or malware, is software code or virus designed to disrupt the normal working of computer systems or mobile devices. Any exchange of data, such as opening an infected email attachment, visiting a malware-hosting website, or importing the content of a USB stick, carries the risk of transferring malware into an organization's systems and services.

Malware can be used by fraudsters to capture information from systems, PCs, laptops or portable devices, or to read data entered onto them such as passwords and log-on details.

Other names for malware include *viruses, worms, trojan horses, spyware and ransomware.*

Ransomware refers to a particular use of malware, in which a fraudster threatens to make public the victim's seized data or block access to it, unless a ransom is paid.

https://www.cafonline.org/about-us/security-centre/be-aware---current-threats
https://www.ncsc.gov.uk/guidance/WannaCry-guidance-for-home-users-and-small-businesses

62

Common Types of Fraud

Phishing :

Phishing is a technique of fraudulently obtaining private information like login ID and Password, Debit / Credit Card details, PIN, Date of Birth, and Mobile Number etc. This is one of the most common type of social engineering attack. Most Phishing scams endeavour to:

- Obtain personal information such as names, bank account details (User ID, Password, OTP), PAN, Aadhaar etc. by using the shortened or misleading link.
- Incorporate threats, fear, and a sense of urgency with phishing message/ email to manipulate the user into responding quickly.

Vishing

Vishing is the voice form of Phishing where frauds take place over phone calls. It is an act of using the telephone to trick the user into surrendering private information that will be used for fraudulent purposes. The scammer usually pretends to be from a legitimate entity and tries to befool the victim by luring or threatening him.

Smishing

Smishing uses cell phone text messages to lure users in a similar fashion like Phishing. They take the form of text messages that claim to be from legitimate entities and are often used in combination with other techniques to bypass inbuilt protections. They might also direct victims to malicious websites on their phones.

63

Espionage / Trespass

- Password attacks fall under the category of espionage or trespass.
- Attempting to guess or reverse-calculate a password is often called cracking.
- There are alternative approaches to password cracking:
  - Brute force attack :
  - Dictionary password attack
  - Social engineering password attack etc

64

Forces of Nature

Some typical force of nature attacks include the following:

- Fire
- Flood
- Earthquake
- Lightning
- Landslide or mudslide
- Tornados or severe windstorms
- Hurricanes, typhoons, and tropical depressions
- Tsunami
- Electrostatic discharge (ESD)
- Dust contamination
- Epidemics/ Pandemics

65

Software Attacks

- Deliberate software attacks occur when an individual or a group designs and deploys software to attack a system.
- This software can be used to overwhelm the processing capabilities of online systems or to gain access to protected systems by hidden means
  - ***Malware—viruses, worms, Trojan horses, polymorphic threats and hoaxes***
  - ***Back doors, and maintenance hooks***
  - ***Denial-of-service (DoS) and distributed denial-of-service attacks (DDoS)***
  - ***E-mail attacks- spam,***
  - ***Communications interception attacks***

66

Technical Software Failures

- The Open Web Application Security Project (OWASP) list of "The Ten Most Critical Web Application Security Risks" for 2021:

1. **Broken Access Control**
2. **Cryptographic Failures**
3. **Injection**
4. **Insecure Design**
5. **Security Misconfiguration**
6. **Vulnerable and Outdated Components**
7. **Identification and Authentication Failures**
8. **Software and Data Integrity Failures**
9. **Security Logging and Monitoring Failures**
10. **Server-Side Request Forgery (SSRF)**

https://owasp.org/www-project-top-ten/
https://www.appsealing.com/owasp-top-10-vulnerabilities/

67

Introduction to Contingency Planning

- Incident Response Plan
- Disaster Recovery plan
- Business Resumption
- Crisis Management

68

Fundamentals of Contingency Planning

- The overall ***planning for unexpected adverse events is called contingency planning*** (CP).
- It is how organizational units ***prepare for, detect, react to, and recover*** from events that threaten the security of information resources and assets.
- The main goal of CP is to ***restore normal modes of operation with minimum cost and disruption to normal business activities*** after an unexpected adverse event

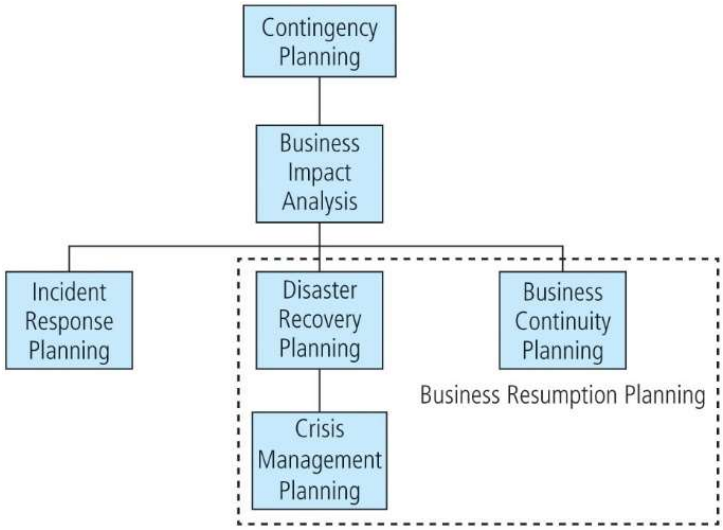
69

Fundamentals of Contingency Planning

- CP consists of four major components:
  1. Business impact analysis (BIA)
  2. Incident response plan (IR plan)
  3. Disaster recovery plan (DR plan)
  4. Business continuity plan (BC plan)
- Depending on the organization's size and business philosophy, IT and InfoSec managers can either
  - create and develop these four CP components as one unified plan or
  - create the four separately in conjunction with a set of interlocking procedures that enable continuity

70

Contingency Planning



71

Incident Response

72

Incident Response

- When those *events represent the potential for loss, they are referred to as adverse events or incident candidates*.
- When an ***adverse event begins to manifest as a real threat to information, it becomes an incident***.
- The incident response plan (IR plan) is usually activated when the organization detects an incident that affects it, regardless of how minor the effect is

73

NIST – Incident response cycle

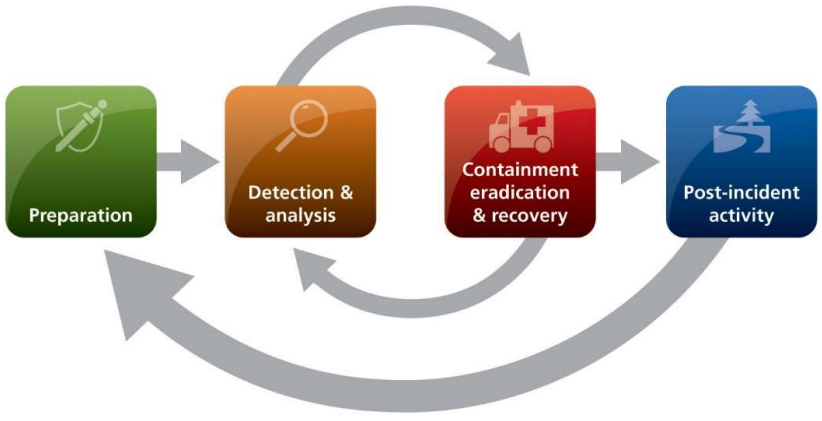
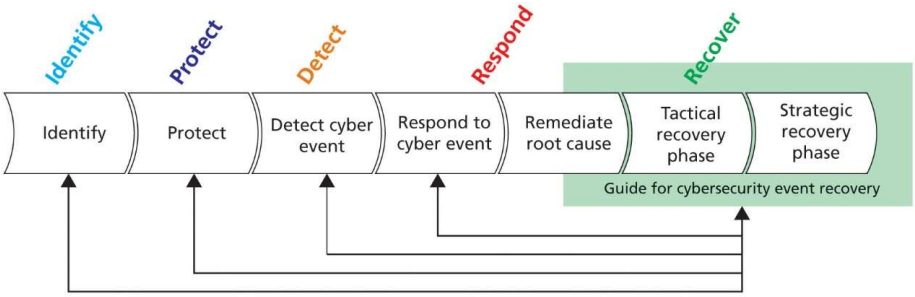


Figure 10-6 NIST incident response life cycle

Source: NIST Special Publication 800-61, Rev. 2: The Computer Security Incident Handling Guide.

74

NIST – Cyber security framework



75

Documenting an Incident

- As soon as an incident has been confirmed and the notification process is underway, ***the team should begin to document it.***
- The documentation should ***record the who, what, when, where, why, and how of each action taken while the incident is occurring.***
- It serves as a case study after the fact to determine if the right actions were taken and if they were effective.
- It can also prove the ***organization did everything possible to deter the spread of the incident***

76

Incident Containment Strategies

- The essential task of IR is to stop the incident and contain its scope or impact.
- **Incident containment strategies focus on two tasks:**
  - Stopping the incident
  - Recovering control of the affected systems
- **Typical containment strategies include:**
  - Disabling compromised user accounts
  - Reconfiguring a firewall to block the problem traffic
  - Temporarily disabling the compromised process or service
  - Taking down the conduit application or server
  - Disconnecting the affected network or network segment
  - Stopping all computers and network devices

77

Incident Escalation

- An ***incident may increase in scope or severity to the point that the IRP cannot adequately contain the incident.***
- Each ***organization will have to determine, during the business impact analysis, the point at which the incident becomes a disaster.***
- The organization must also document when to involve outside responders

78

Recovering from Incidents

- Once the ***incident has been contained, and system control regained, incident recovery can begin.***
- As in the incident reaction phase, ***the first task is to inform the appropriate human resources.***
- Almost simultaneously, the ***CSIRT must assess the full extent of the damage so as to determine what must be done to restore the systems.***
- The immediate determination of the ***scope of the breach of confidentiality, integrity, and availability of information and information assets is called incident damage assessment.***
- Those who document the damage must be ***trained to collect and preserve evidence, in case the incident is part of a crime or results in a civil action***

79

Business Continuity Planning (BCP)

- Sometimes, disasters have such a profound effect on the organization that it cannot continue operations at its primary site until it fully completes all DR efforts, which requires business continuity (BC) strategies
- BC planning (BCP) ensures critical business functions can continue in a disaster, and is most likely managed by the CEO or COO of the organization
- BCP is activated and executed concurrently with the DRP when needed
- While BCP reestablishes critical functions at an alternate site, DRP focuses on reestablishment at the primary site

80

Crisis Management

- Another process that many organizations plan for is crisis management (CM), ***which focuses more on the effects that a disaster has on people than its effects on information assets.***
- While some organizations include crisis management as a subset of the DR plan, the protection of human life and the organization's image is such a high priority that it may deserve its own committee, policy, and plan

81

Crisis Management

- According to Gartner Research, the crisis management team is responsible for managing the event from an enterprise perspective and performs the following roles:
  - Supporting personnel and their loved ones during the crisis
  - Keeping the public informed about the event and the actions being taken to ensure the recovery of personnel and the enterprise
  - Communicating with major customers, suppliers, partners, regulatory agencies, industry organizations, the media, and other interested parties

82

Crisis Management

- The crisis management planning team (CMPT) should establish a base of operations or command center near the site of the disaster as soon as possible.
- The CMPT should include individuals from all functional areas of the organization in order to facilitate communications and cooperation.
- The CMPT is charged with three primary responsibilities:
  1. Verifying personnel status
  2. Activating the alert roster
  3. Coordinating with emergency services

83

Encryption and Public Key Infrastructure

- Encryption
  - Transforming text or data into cipher text that cannot be read by unintended recipients
  - Two methods for encryption on networks
    - Secure Sockets Layer (SSL) and successor Transport Layer Security (TLS)
    - Secure Hypertext Transfer Protocol (S-HTTP)

84

Achieving Digital Resiliency

- Deals with how to maintain and increase resilience of organization and its business processes
- Calls attention to managerial and organizational issues in addition to IT infrastructure
- Single weak link can cause an outage if resiliency has not been explicitly designed in, measured, and tested

85

Q&A

86

86