Chapter 1

Information System (IS) : A set of software, hardware, data, people, procedures, and networks, that are necessary to use information as a resource in an organization.

Characteristics of Information

1. Availability
2. Accuracy
3. Authenticity
4. Confidentiality
5. Integrity
6. Utility
7. Possession

Security: The quality or state of being secure **or** to be free from danger

Security Layers a successful organization should have

1. Physical security
2. Personal security
3. Operations security
4. Communications security
5. Network security
6. Information security

Information Security: Protection of information and its critical elements, including systems that handle that information

Necessary tools for Information Security

1. Policy

2. Awareness
3. Training
4. Education
5. Technology

Components of Information Security

1. Information Security Management
2. Computer & Data Security
3. Policy
4. Network Security

Securing Components in an Information System

Computer (software and hardware): is the key component in information systems.

They can either be a subject or an object of an attack.

Subject: An active tool to conduct attack.

object: Entity being attacked.

Balancing Information Security and Access

Impossible to obtain perfect security.

There should be a balance between protection and availability.

To do that, level of security must allow reasonable access, yet protect against threats

---

R-609

Information security began with Rand Report R-609

R-609: paper that started the study of computer security

Scope of computer security grew from physical security to include:
1. Safety of data
2. Limiting unauthorized access to data
3. Involvement of personnel from multiple levels of an organization

---

Chapter 2

important functions Information security does for organizations

1. Protecting the organization’s ability to function
2. Enabling the safe operation of applications running on the organization’s IT systems .
3. Protecting the data and information the organization collects and uses.
4. Safeguarding the organization’s technology assets in Organizations.

Business -> Application -> Data -> Technology

Threats

Threat: A thing that represents a constant danger to an asset.

Management must be informed of the different threats facing the organization

By examining each threat category, management effectively protects information through policy, education, training, and technology controls.

CSI and The FBI found in a 2004 survery that:

1. 79% of orgs had cyber security breaches in the last 12 month
2. 54% of them reported financial losses totaling over $141 million

---

Threats to Information Security

1. Acts of Human Error or Failure

Acts performed without malicious intent (examples):
1.Inexperience

2. Improper training
3. Incorrect assumptions

Employees are among the greatest threats to an organization’s data.

Employee mistakes can easily lead to:
1. Revelation(reveal) of classified data
2. Entry of erroneous(wrong) data
3. Accidental data deletion or modification
4. Data storage in unprotected areas
5. Failure to protect information

These threats can be prevented with controls.

Deliberate Acts of Espionage or Trespass

there is a difference between Competitive intelligence (legal) and industrial espionage (illegal)

Shoulder surfing occurs anywhere a person accesses confidential information

Controls let trespassers know they are encroaching on organization’s cyberspace

Hackers uses skill, guile, or fraud to bypass controls protecting others’ information

examples:
1. Unauthorized access or data collection

Deliberate Acts of Theft

Illegal taking of another’s property

Physical theft is controlled relatively easily

Electronic theft is more complex problem (explain why)
as evidence crime not readily apparent

Deliberate Software Attacks

Malicious software (malware) designed to target systems.

examples:

1. viruses
2. worms
3. Trojan horses
4. logic bombs
5. back doors
6. denial-of-services attacks

Forces of Nature

- Among the most dangerous threats
- Disrupt not only lives, but also storage, transmission, and use of information
- Orgs must implement controls to limit damage and prepare plans for continued operations.

Deviations in Quality of Service

- Situations where products or services not delivered as expected.
- Information system depends on many interdependent support systems

Stuff that affect availability of information and systems:

1. Internet service
2. Communications
3. Power irregularities

Internet Service Issues

ISP failures can considerably undermine availability of information

Outsourced Web hosting providers are responsible for all Internet services as well as hardware and Web site operating system software.

Attacks

Accomplished by threat agent which damages or steals organization’s information.

Types of Attacks

Type	Explanation
Malicious code	Execution of viruses and such with intent to destroy or steal information
Back door	Gaining access to system or network using known or previously unknown/newly discovered access mechanism
Password crack	Attempting to reverse calculate a password
Brute force	Trying every possible combination of options of a password
Dictionary	Selects specific accounts to attack and uses commonly used passwords to guide guesses
Spoofing	Intruder assumes a trusted IP address, to gain unauthorized access
Man-in-the-middle	Attacker monitors network packets, modifies them, and inserts them back into network
Spam	Unsolicited commercial e-mail (more annoyance than attack)
Mail bombing	Attacker routes large quantities of e-mail to target (DoS)
Sniffers	program or device that monitors data traveling over network (can be used for legit purposes)
Social engineering	Using social skills to convince people to reveal valuable info to attacker
Buffer overflow	Error occurring when more data is sent to a buffer than can be handled
Timing attack	Exploring contents of a Web browser’s cache to create malicious cookie (new)
Denial-of-service (DoS)	Sending a large number of connection or information requests to a target system, which can overwhelm it alongside legit request, causing crashes or preventing it from handling legitimate service requests effectively.
Distributed denial-of-service (DDoS):	Coordinated stream of requests is launched against target from many locations simultaneously

What Makes DDoS Attacks Possible?

1. Internet was designed with functionality & not security in mind
2. Internet security is highly interdependent
3. Internet resources are limited
4. Power of many is greater than power of a few

Chapter 3

Cryptography: Using codes to secure transmission of information.

Encryption: Converting messages into a form unreadable by unauthorized individuals.

Cipher Methods

1. Bit stream: Each plaintext bit transformed into cipher bit one bit at a time.

2. Block cipher: message divided into blocks (e.g., sets of 8- or 16-bit blocks (most common)), each block is transformed into encrypted block of cipher bits (how)
    - using algorithm and key.

Substitution Cipher

Substitution cipher: substitute one value for another

types:
1. Monoalphabetic substitution: One alphabet
2. Polyalphabetic substitution: Two or more alphabets (more advanced)

example:

`plain text= HELLO`

`Alphabet: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z`

`Substitution: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C`

`**Ciphertext**: KHOOR`

Transposition Cipher

Transposition cipher: Rearranging values within a block to create ciphertext

example:

Plaintext: `HELLO WORLD`

Key: `4312`

Grid:

```
H E L L
O W O R
L D X X
```

Numbered Columns:

```
3 4 1 2
L L H E
O R O W
X X L D
```

Ciphertext: `LOXLRXHOLEWD`

Exclusive OR

Exclusive OR (XOR): function of Boolean algebra; two bits are compared

Same = 0
Different = 1

num1	num2	sign
0	0	0
0	1	1
1	0	1
1	1	0

Cryptographic Algorithms

Today’s popular cryptosystems use hybrid combination of symmetric and asymmetric algorithms.

The categories are distinguished by types of keys used for encryption and decryption operations

---

Symmetric Encryption

Symmetric encryption: Uses same secret key to encipher and decipher message

Traits:

- Encryption methods can be extremely efficient, requiring minimal processing
- Both sender and receiver must possess encryption key
- If either copy of key is compromised, an intermediate can decrypt and read messages

Symmetric-key encryption:

- Encryption key k = decryption key k* (same key is used to both encrypt and decrypt the data)
- Dec(k, Enc(k,m)) = m (a formula that says if you decrypt message m that was encrypted with k, you should get m)
- Deck(Enck (m)) = m (another example formula)

Types:
a) Data Encryption Standard (DES): one of most popular ,64-bit block size; 56-bit key, Adopted by NIST in 1976 as standard for encrypting non-classified information.

b)Triple DES (3DES): created to provide better security than DES

c)Advanced Encryption Standard (AES): developed to replace both DES and 3DES

Asymmetric Encryption

Two different but related keys; either key can encrypt or decrypt message

If Key A encrypts message, only Key B can decrypt

Highest value when one key serves as private key and the other serves as public key

Asymmetric Encryption (public key encryption)

Public key pk = (N, e)

Secret key sk = (N, d)

Encryption: Enc_{pk} (m) = [me mod N] (encrypt using the Public key)

Decryption: Dec_{sk} (c) = [cd mod N] (decrypt using the private key)

Cryptography Tools

Public Key Infrastructure (PKI): integrated system that enables users to communicate securely

PKI cryptosystems examples:

1. digital certificates
2. certificate authorities (CAs)

Digital Signatures

Digital Signatures: Encrypted messages that can be mathematically proven to be authentic

Created in response to rising need to verify information transferred using electronic systems

Uses asymmetric encryption processes

uses Public Key to ensure data integrity and non-repudiation

s = $Sign_{sk}$ (m)

$Verify_{pk}$ (m,*s*) = true or false

Hash-then-sign: s = $Sign_{sk}$(h(m)), where h is a cryptographic hash function

---

Key Distribution

Asymmetric key system can help distribute symmetric key

example:

Ahmad key pair = (K_{bp},K_{bs}) (p = public, s = secret)

Mohammed key pair = (K_{ap},K_{as}) (p = public, s = secret)

How can Ahmad send a symmetric key K* to Mohammed through Internet
using their asymmetric keys?

Ans:

Ahmad first uses his secret key to encrypt the message, then uses Mohammed's public key to further encrypt the message, then sends it

$M=K_{ap}(K_{bs}(K^*))$

Mohammed uses his secret key to decrypt the message, then uses Ahmad's public key to further decrypt the message

$K_{bp}(K_{as}(M))=K^*$

Full Procedure

$M=K_{ap}(K_{bs}(K))$ --> $K_{bp}(K_{as}(M))=K$

OR Ahmad can also use Mohammed's public key to encrypt then send it,

$K_{ap}(K^*)$

Mohammed can then use his secret key to decrypt it

$K_{as}(K_{ap}(K^*))$

full procedure

$K_{ap}(K)$ --> $K_{as}(K_{ap}(K))$

Protocols for Secure Communications

Secure Socket Layer (SSL) protocol: uses public key encryption to secure channel over public Internet

Secure Hypertext Transfer Protocol (S-HTTP): Extended version of HTTP; provides for encryption of individual messages between client and server across Internet

S-HTTP is the application of SSL over HTTP; allows encryption of information passing between computers through protected and secure virtual connection

---

E-mail Securing

Secure Multipurpose Internet Mail Extensions (S/MIME): builds on normal MIME encoding format by adding encryption and authentication.

Privacy Enhanced Mail (PEM): proposed as standard to function with public key cryptosystems; uses 3DES symmetric key encryption.

Pretty Good Privacy (PGP): uses IDEA Cipher for message encoding

---

Web transactions Securing

Secure Electronic Transactions (SET): developed by MasterCard and VISA in 1997 to provide protection from electronic payment fraud

- Uses DES to encrypt credit card information transfers
- Provides security for both Internet-based credit card transactions and credit card swipe systems in retail stores

---

Chapter 4

Risk management: Identifying and controlling risks facing an organization

Risk identification: Examining an organization’s current information technology security situation

Risk control: Applying controls to reduce risks to an organization's data and info systems

---

An Overview of Risk Management

Know yourself: identify, examine, and understand the information and systems currently in place

Know the enemy: identify, examine, and understand threats facing the organization

---

Risk Identification

Assets are targets of various threats and threat agents

Risk management involves
1. identifying organization's assets
2. identifying threats/vulnerabilities

Risk identification begins with
1. identifying organization's assets
2. assessing their value

Asset Identification and Valuation

Iterative process begins with identification of assets, including all elements of an organization's system, Assets are then classified and categorized.

Categorizing the Components of an Information System

Traditional system	**SecSDLC and risk management**	**SecSDLC and risk management Example**
People	Employees	Trusted employees/ Other staff
	NonEmployees	People at trusted/ organizations Strangers
Procedures	Procedures	IT and business standard procedures IT and business sensitive procedures
Data	Information	Transmission Processing Storage
Software	Software	Applications Operating systems

Traditional system	SecSDLC and risk management	SecSDLC and risk management Example
		Security components
Hardware	System devices and peripherals	Systems and peripherals Security devices
	Networking components	Intranet components Internet or DMZ components

---

People, Procedures, and Data Asset Identification

Human resources, documentation, and data information assets are more difficult to identify

People with knowledge, experience, and good judgment should be assigned this task

These assets should be recorded using reliable data-handling process

Asset attributes for people:

1. position name/number/ID; supervisor
2. security clearance level
3. special skills

Asset attributes for procedures:

1. description
2. intended purpose; what elements is it tied to;
3. storage location for reference; storage location for update

Asset attributes for data:

1. classification
2. owner/creator/ manager
3. data structure size
4. data structure used; online/ offline
5. location
6. backup procedures employed

Hardware, Software, and Network Asset Identification

What information attributes to track depends on:

1. Needs of organization/risk management efforts
2. Management needs of information security/information technology communities

Asset attributes to be considered are:

1. name
2. IP address
3. MAC address
4. element type
5. serial number
6. manufacturer name
7. model/part number
8. software version
9. physical or logical location
10. controlling entity

Information Asset Classification

Many organizations have data classification schemes (e.g., confidential, internal, public data)

Classification of components must be specific to allow determination of priority levels

Categories must be comprehensive and mutually exclusive

Information Asset Valuation

Questions help develop criteria for asset valuation: which information asset

1. is most critical to organization’s success?
2. generates the most revenue/profitability?
3. would be most expensive to replace or protect?
4. would be the most embarrassing or cause greatest liability if revealed?

Data Classification and Management

Data Classification and Management: Variety of classification schemes used by corporate and military organizations

Information owners are responsible for classifying their information assets

Information classifications must be reviewed periodically

Most organizations do not need detailed level of classification used by military or federal agencies; however, organizations may need to classify data to provide protection

---

Threat Identification

Realistic threats need investigation; unimportant threats are set aside

Threat assessment:

1. Which threats present danger to assets?
2. Which threats represent the most danger to information?
3. How much would it cost to recover from attack?
4. Which threat requires greatest expenditure to prevent?

Vulnerability Identification

Vulnerabilities: Specific avenues threat agents can exploit to attack an information asset

Examine how each threat could be perpetrated and list organization’s assets and vulnerabilities

Process works best when people with diverse backgrounds within organization work iteratively in a series of brainstorming sessions

At end of risk identification process, list of assets and their vulnerabilities is achieved

---

Risk Assessment

Risk assessment: evaluates the relative risk for each vulnerability and assigns a risk rating or score to each information asset

Documenting the Results of Risk Assessment

Final summary comprised in ranked vulnerability risk worksheet

Worksheet details asset, asset impact, vulnerability, vulnerability likelihood, and risk-rating factor

Ranked vulnerability risk worksheet: initial working document for next step in risk management

process: assessing and controlling risk

Risk Control

Strategies to control each risk:

1. Apply safeguards (avoidance)
2. Transfer the risk (transference)
3. Reduce impact (mitigation)
4. Understand consequences and accept risk (acceptance)

Avoidance

Attempts to prevent exploitation of the vulnerability

Preferred approach: countering threats, removing asset vulnerabilities, limiting asset access, and adding protective safeguards

Three common methods of risk avoidance:

1. Application of policy
2. Training and education
3. Applying technology

Transference

If lacking, organization should hire individuals/firms that provide security expertise

Organization may then transfer risk associated with management of complex systems to another organization experienced in dealing with them.

Mitigation

Attempts to reduce impact of vulnerability exploitation through planning and preparation

Approach includes three types of plans:

1. Incident response plan (IRP): The actions to take while incident is in progress is defined
2. Disaster recovery plan (DRP) (most common)
3. Business continuity plan (BCP): encompasses continuation of business activities if catastrophic event occurs

---

Acceptance

Doing nothing to protect a vulnerability and accepting the outcome of its exploitation

Valid only when the particular function, service, information, or asset does not justify cost of protection

Risk appetite describes the degree to which organization is willing to accept risk as trade-off to the expense of applying controls

---

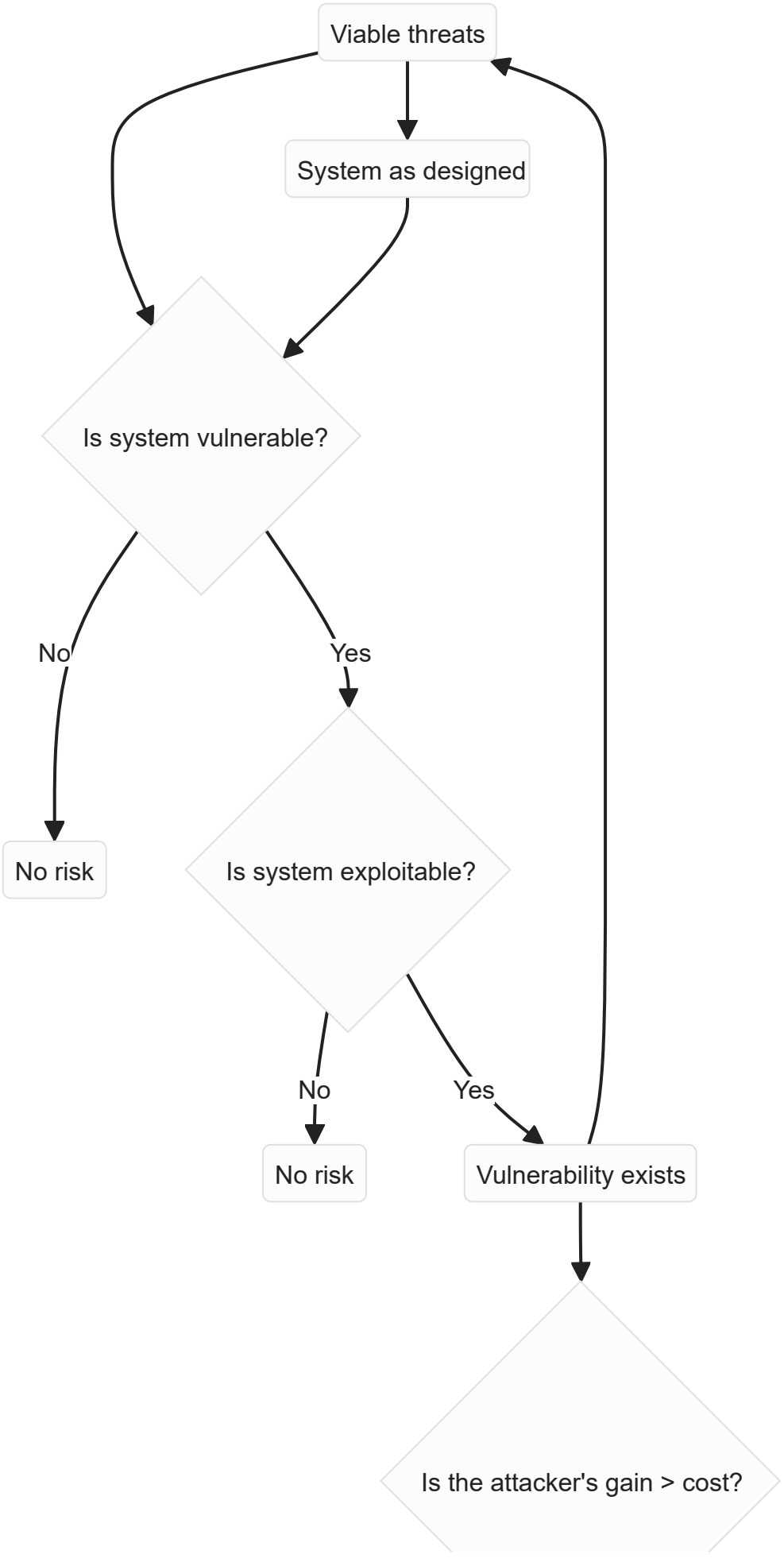
Selecting a Risk Control Strategy

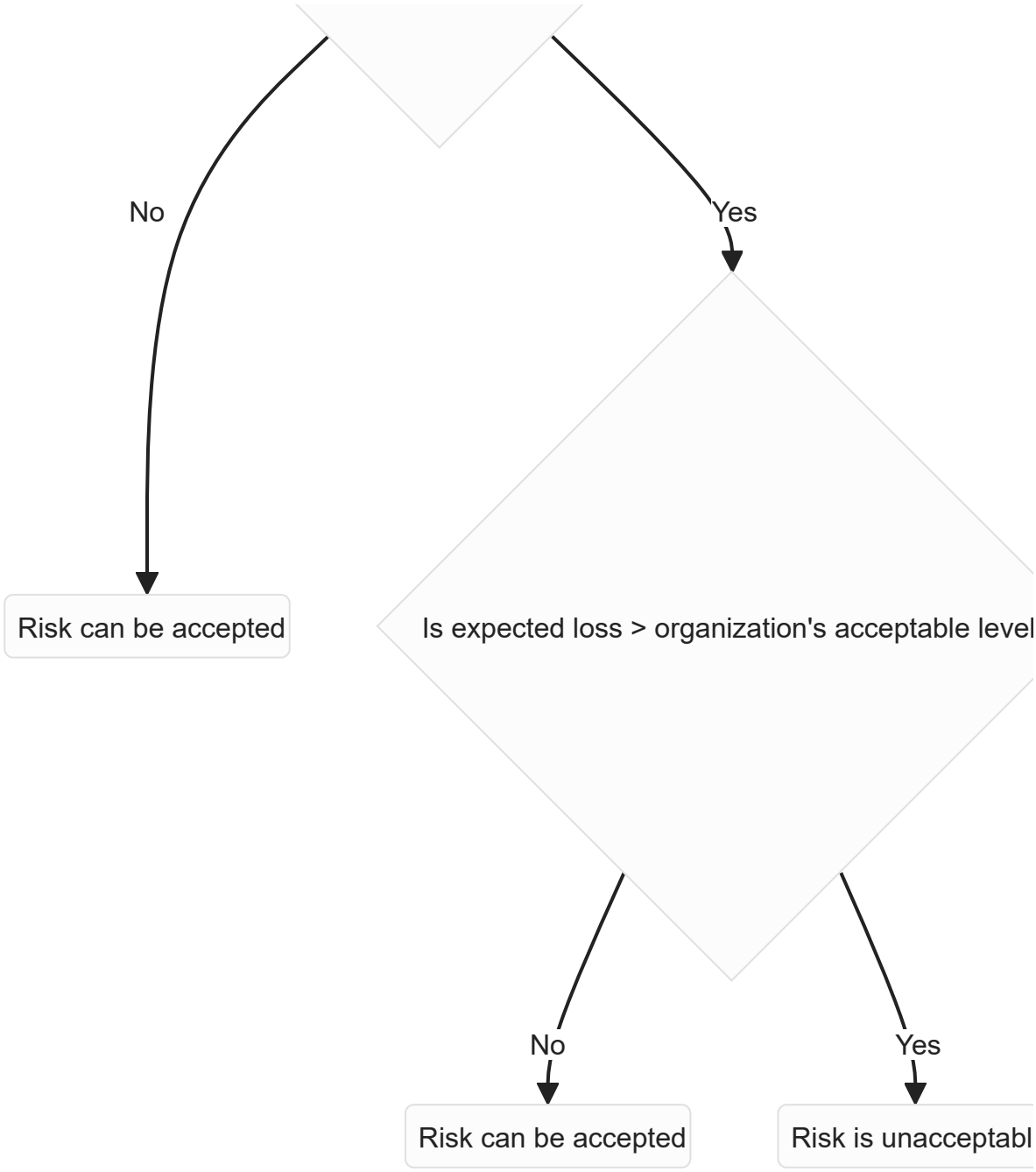
Level of threat and value of asset play major role in selection of strategy

Rules of thumb:

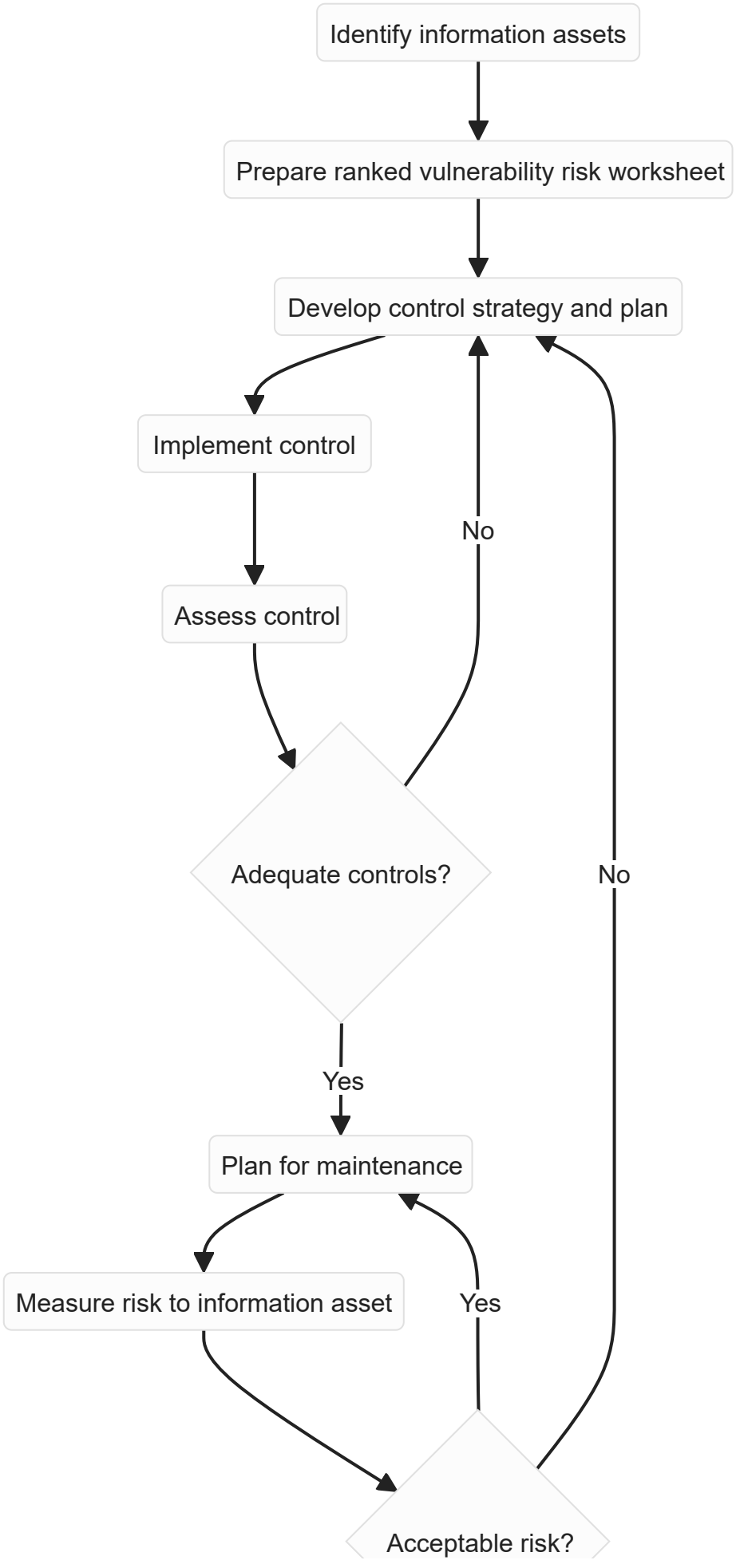
1. When a vulnerability exists
2. When a vulnerability can be exploited
3. When attacker’s cost is less than potential gain
4. When potential loss is substantial

Risk Handling Decision Point Diagram


Viable threats
System as designed
Is system vulnerable?
No
Yes
No risk
Is system exploitable?
No
Yes
No risk
Vulnerability exists
Is the attacker's gain > cost?



Risk control cycle


Identify information assets
Prepare ranked vulnerability risk worksheet
Develop control strategy and plan
Implement control
Assess control
Adequate controls?
No
No
Yes
Plan for maintenance
Measure risk to information asset
Yes
Acceptable risk?

Cost Benefit Analysis (CBA)

Most common approach for information security controls is economic feasibility of implementation

Cost Benefit Analysis: The formal process of evaluating worth of assets to be protected and the loss in value if those assets are compromised

Items that impact cost of a control or safeguard include:

1. cost of development
2. training fees
3. implementation cost
4. service costs
5. cost of maintenance

Benefit: The value an organization realizes by using controls to prevent losses associated with a vulnerability

Asset valuation: Assigning financial value or worth to each information asset; with many components to it

---

Benchmarking

An alternative approach to risk management, involves studying and copying successful practices from other organizations.

One of two measures typically used to compare practices:

1. Metrics-based measures
2. Process-based measures

Standard of Due Care:
This means the organization has taken reasonable steps to protect its security, similar to what other responsible organizations would do, when adopting levels of security.

Due Diligence:
This shows that the organization continuously checks and updates its security measures to ensure they still work.

Failure to support standard of due care or due diligence can leave organization open to legal liability

Best business practices: security efforts that provide a superior level protection of information

When considering best practices for adoption in an organization, consider:

1. Does organization resemble identified target with best practice?
2. Are resources at hand similar?
3. Is organization in a similar threat environment?

Problems with Applying Benchmarking and Best Practices

Organizations don’t talk to each other (biggest problem)

No two organizations are identical

Best practices are a moving target (always changing)

Knowing what was going on in information security industry in recent years through benchmarking doesn’t necessarily prepare for what’s next (benchmarking doesn't necessarily prepare for the future)

Chapter 5

Law and Ethics in Information Security

Laws: Rules that mandate or prohibit certain behavior

Ethics: Socially acceptable behavior, based on Cultural mores

Cultural mores: fixed moral attitudes or customs of a particular group;

Laws carry sanctions of a governing authority; ethics do not

Types of Laws

Relevant U.S. Laws (General)

1. Computer Fraud and Abuse Act of 1986 (CFA Act)
2. National Information Infrastructure Protection Act of 1996
3. USA Patriot Act of 2001
4. Telecommunications Deregulation and Competition Act of 1996
5. Communications Decency Act of 1996 (CDA)
6. Computer Security Act of 1987

U.S. Copyright Law

Intellectual property recognized as protected asset in the U.S

copyright law extends to electronic formats

With proper acknowledgement, permissible to include portions of others' work as reference

U.S. Copyright Office Web site: www.copyright.gov

State and Local Regulations

Restrictions on organizational computer technology

They exist at international, national, state, local levels

Information security professional's responsible for understanding state regulations and ensuring organization is compliant with them

---

International Laws and Legal Bodies

European Council Cyber-Crime Convention:

1. Establishes international task force overseeing Internet security functions for standardized international technology laws
2. Attempts to improve effectiveness of international investigations into breaches of technology law
3. Well received by intellectual property rights advocates due to emphasis on copyright infringement prosecution
4. Lacks realistic provisions for enforcement

United Nations Charter

Makes provisions, to a degree, for information security during information warfare (IW)

IW: use of information technology to conduct organized and lawful military operations

IW is relatively new type of warfare,

Military has been conducting IW operations for decades

Policy Versus Law

policy: a body of expectations developed and formalized by Most organizations

Policies serve as organizational laws

To be enforceable, policy must be

1. distributed
2. readily available,
3. easily understood
4. acknowledged by employees

The Ten Commandments of Computer Ethics

Thou shalt

1. Not use a computer to harm other people.
2. Not interfere with other people's computer work.

3. Not snoop around in other people's computer files.
4. Not use a computer to steal.
5. Not use a computer to bear false witness.
6. Not copy or use proprietary software for which you have not paid.
7. Not Use other people's computer resources without authorization or proper compensation.
8. Not Appropriate other people's intellectual output.
9. Think about the social consequences of the program you are writing or the system you are designing.
10. Always use a computer in ways that ensure consideration and respect for your fellow humans.

Ethical Differences Across Cultures

Cultural differences create difficulty in determining what is and is not ethical

Q. When does difficulties arise

- Ans: when one nationality’s ethical behavior conflicts with ethics of another national group

Example: many of ways in which Asian cultures use computer technology is software piracy

---

Ethics and Education

Education: Overriding factor in leveling ethical perceptions within a small population

Employees must be trained in expected behaviors of an ethical employee, especially in areas of information security

Proper ethical training vital to creating informed, well prepared, and low-risk system user

---

Association of Computing Machinery (ACM)

Established in 1947 as “the world's first educational and scientific computing society”

Code of ethics contains references to

1. protecting information confidentiality

2. causing no harm, protecting others' privacy
3. respecting others' intellectual property

Computer Security Institute (CSI)

Provides information and training to support computer, networking, and information security professionals

has argued for adoption of ethical behavior among information security professionals, but without a code of ethics

---

Key U.S. Federal Agencies

1. Department of Homeland Security (DHS)
2. Federal Bureau of Investigation's (FBI's) National Infrastructure Protection Center (NIPC)
3. National Security Agency (NSA)
4. U.S. Secret Service

Information Security Policy, Standards and Practices

Communities of interest must consider policies as basis for all information security efforts

Policies direct how issues should be addressed and technologies used

Security policies are least expensive controls to execute

But security policies are most difficult to implement

Shaping policy is difficult

Definitions

Policy: Actions used by organization to convey instructions from management to employees

Policies are organizational laws

Standards: Detailed statements of what must be done to comply with policy

how to effectively explain complying with policy

1. Practices
2. procedures
3. guidelines

For a policy to be effective, must be properly disseminated, read, understood and agreed to by all members of organization

---

Policy Management

Policies must be managed (why)

- as they constantly change

remain viable, security policies must have:

1. Individual responsible for reviews
2. A schedule of reviews
3. Method for making recommendations for reviews
4. Specific policy issuance and revision date

Information Classification

- Classification of information is an important aspect of policy
- Policies are classified
- A clean desk policy stipulates that at end of business day
- Classified information must be properly stored and secured
- In today’s open office environments, may be beneficial to implement a clean desk policy

---

Security Education, Training, and Awareness Program

As soon as general security policy exist, policies to implement security education, training and awareness (SETA) program should follow

SETA: a control measure designed to reduce accidental security breaches

SETA builds on the general knowledge the employees must possess to do their jobs, familiarizing them with the way to do their jobs securely

The SETA program consists of three elements:

1. security education
2. security training
3. security awareness

Security Education

Everyone in an organization needs to be trained and aware of information security

Not every member needs formal degree or certificate in information security

When education in security is needed, an employee can identify curriculum available from institutions of higher learning or continuing education

A number of universities have formal coursework in information security

---

Security Training

Providing organization members with detailed information and hands-on instruction designed to prepare them to perform their duties securely

Management of information security can develop customized in-house training or outsource the training program

---

Design of Security Architecture

A) Defense in depth

Implementation of security in layers

Establishing sufficient security controls and safeguards so that an intruder faces multiple layers of controls by organizations.

B) Security perimeter

Point at which an organization’s security protection ends and outside world begins

Doesn't apply to internal attacks from employee threats or on-site physical threats

---

Key Technology Components

Firewall: device that selectively discriminates against info flowing in or out of organization

Demilitarized zone (DMZ): no-man’s land between inside and outside networks where some organizations place Web servers

Intrusion Detection Systems (IDSs) (when to implement):

- in effort to detect unauthorized activity within inner network, or on individual machines