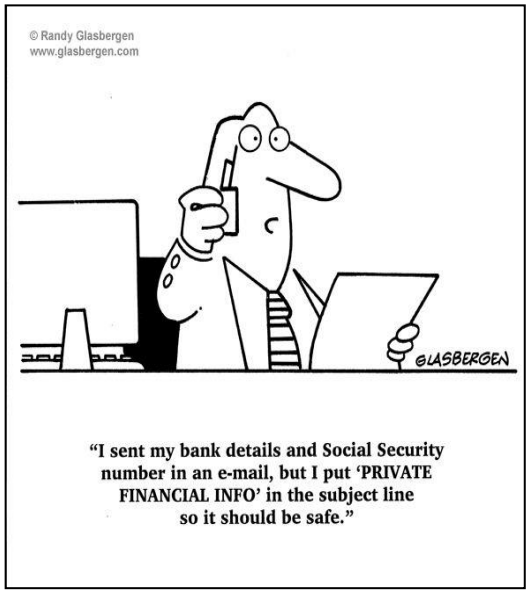
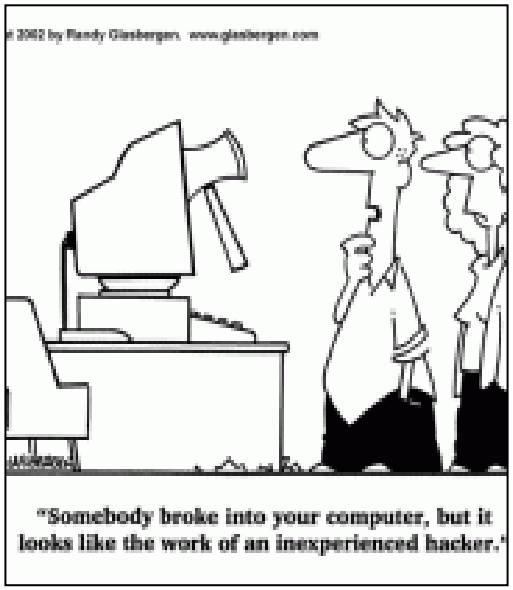
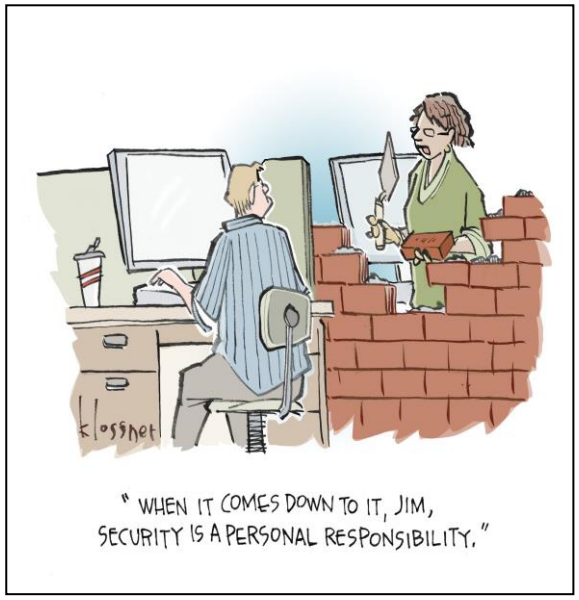
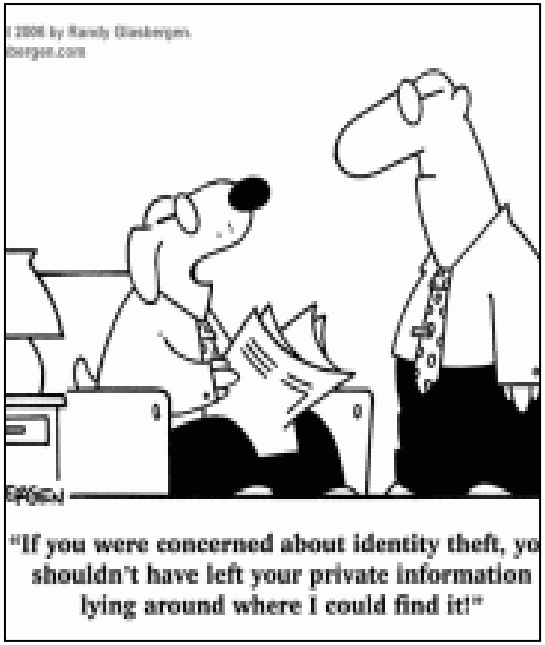
Introduction to Cyber Security

Dr. Srinivas Josyula

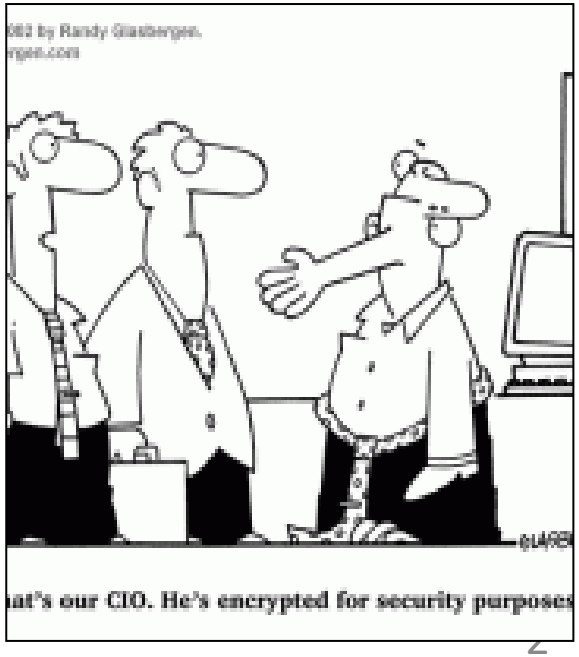

© Randy Glasbergen
www.glasbergen.com
GLASBERGEN
"I sent my bank details and Social Security number in an e-mail, but I put 'PRIVATE FINANCIAL INFO' in the subject line so it should be safe."


"Somebody broke into your computer, but it looks like the work of an inexperienced hacker."


klossner
" 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!"


Copyright 2004 by Randy Glasbergen.
www.glasbergen.com
GLASBERGEN
"For the sake of information security, everything on my résumé is false."


at's our CIO. He's encrypted for security purposes

Therefore, I say:

One who knows the enemy and knows himself will not be in danger in a hundred battles.

One who does not know the enemy but knows himself will sometimes win, sometimes lose

One who does not know the enemy and does not know himself will be in danger in every battle

~ Sun Tzu

"It takes 20 years to build a reputation and a few minutes of cyber-incident to ruin it."

"Cyber-Security is much more than a matter of IT."

~ Stephane Nappo.

Agenda

- **Digital Products**
- **Cyber Security**
- **Ten Commandments and Ethics**
- **Objectives / Principles / Functions of Information Security**
- **CIA**
- **Threats and Vulnerabilities**
- **Risk Management**
- **Controls**
- **Cyber Frauds**

What ‘Digital’ really means

- Is it Technology?
- New ways of doing Business?

Digital should be seen as a thing or way *of doing things*

Three Attributes :

1. ***Creating Value*** *at the New frontiers*
2. ***Creating Value in Core Businesses*** *(Rethinking how to use new capabilities to improve how customers are served)*
3. ***Building foundational capabilities***
   a) ***Mindsets :*** *use data to make better and faster decisions*
   b) ***Systems and Architecture*** *: commitment to building networks that connect devices , objects and people*

Source *: Mc Kinsey & Company (Karel Dorner and David Edelman)*

Product vs Digital Products?

- *"A product is the item offered for sale. A product can be a service or an item. It can be physical or in virtual or cyber form. Every product is made at a cost and each is sold at a price. The price that can be charged depends on the market, the quality, the marketing, and the segment that is targeted. Each product has a useful life after which it needs replacement, and a lifecycle after which it has to be re-invented."*

Digital Product

- *A service, physical item, or digital item that provides an agreed and specific outcome for a consumer; that incorporates and requires software to realize that outcome; that is expected to require active management of the software and its required resources over its lifecycle, in a manner prescribed by the provider; and that is described by a formal offer of the outcome to be provided in exchange for an explicit price."*

~ *The Open Group*

What are Digital Products

- **e Commerce Websites :** *A website that provides functionality for shoppers and vendors to reach a commercial agreement is a typical Digital Product. The consumer of this Digital Product would be the vendor's Sales Department(s), not the shopper.*
- **Mobile Applications :** *Mobile applications are Digital Products. Most are provided through a store managed by the digital platform provider. They may also be linked to other products, physical and digital. Fitness mobile applications typically require a separate physical device to track motion and location. Other mobile applications act as channels to Digital Products, such as a newspaper subscription or online banking.*
- **Operational Technology :** *Digital Products can also automate manufacturing, warehouses, or other activities outside of typical back-office applications. This more industrial and embedded use of automation technology is commonly known as Operational Technology (OT).*
- **Smart Devices with Digital Interfaces :** *This is a rapidly growing category of internet-connected products ranging from smart watches to automobiles that combine a traditional physical product format with software to create Digital Products. These smart products do not contain only the physical device and its embedded software; the core product definition may also include cloud-based software and software running on other platforms, such as smartphones*

What are Digital Products

- **Digital Platforms :** *An important category of Digital Product is the digital platform. This product is designed to enable the creation or hosting of other Digital Products which can be sold or shared with consumers. Common examples of how this works in practice include the app stores available to Apple® and Android™ customers, or the Azure® and Amazon Web Services.*

- **Interplay Among Digital Products :** *The digital oven example in Smart Devices with Digital Interfaces illustrates an accelerating trend in which collaboration between interacting Digital Products adds greater value than when they function independently.*

- *This interplay creates opportunities and data for all parties. The data and ongoing consumer feedback received helps the Digital Product Manager to make decisions such as adding features, improving performance, adjusting pricing models, and updating market strategies.*

Criteria for Digital Product ?

The criteria of a Digital Product:

- A Digital Product must include one or more Service Offers which define Service Contract options for consumers
- A Digital Product may be delivered as a Digital Product Instance (defined below) as described in the Service Offer
- The Digital Product Instance may include a system containing IT, non-IT resources, and software
- A Digital Product may be consumed within an organization or externally
- A Digital Product may have dependencies on other Digital Products
- A Digital Product may be comprised of other Digital Products
- A Digital Product may be a resource for other Digital Products
- A Digital Product must provide interactions via machine and/or human interfaces

Cyber attacks in India

- *“More and more aspects of our lives are becoming dependent on technology and connectivity to internet. As a result, we present a much wider attack surface than ever before. It’s likely, therefore, that we will see more disruptive attacks in the future,"*

  ~ Kaspersky, Cyber security research organization, 2021

- *India witnessed a surge in cyberattacks amid rapid adoption of digital services across the country following the lockdown imposed in the wake of covid.*

  ~ Mint ,23 March 2021

- *“As per the information reported to and tracked by the Indian Computer Emergency Response Team (CERT-In), 3,94,499 and 11,58,208 cyber security incidents have been observed during 2019 and 2020, respectively," the home ministry informed Parliament in a reply.*

  ~ Mint ,23 March 2021

Zero Trust Framework

- *Zero Trust is a security framework requiring all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data*

- *Zero Trust is a go to framework for securing infrastructure and data for today's modern digitally transforming Banks .*

- *Zero Trust is a significant departure from traditional security which followed the "trust but verify" method."*

India ranks among top 10 in ITU's Global Cybersecurity Index-2020, Released on 29 June 2021

- The Global Cybersecurity Index (GCI) is a trusted reference that measures the commitment of countries to cybersecurity at a global level – to raise awareness of the importance and different dimensions of the issue.

- As cybersecurity has a broad field of application, cutting across many industries and various sectors, each country's level of development or engagement is assessed along five pillars –
- (i) Legal Measures,
- (ii) Technical Measures,
- (iii) Organizational Measures,
- (iv) Capacity Development, and
- (v) Cooperation – and then aggregated into an overall score.

https://cybersecureindia.in/india-ranks-among-top-10-itus-global-cybersecurity-index-2020/

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

Defining Cyber 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.
- **Information security** is all about the security of information regardless of the realm.
- C**yber Security** is protecting our cyberspace (critical infrastructure) from attack, damage, misuse, and economic espionage.
- **Cyber Intrusions and Attacks** have increased dramatically over the last decade, exposing sensitive personal and business information, disrupting critical operations, and imposing high costs on the economy.

Information Systems / Security?

- 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***

- 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.***

Critical Infrastructure

Information Infrastructure is the term used to describe the totality of interconnected computers and networks, and information flowing through them.

Critical Information Infrastructure is defined as: ***"The computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety."***

~ Section 70 of IT Act 2000,

CII Protection

- The Information Technology Act, 2000 defines Critical Information Infrastructure (CII) as “… that computer resource, the incapacitation or destruction of which, shall have a debilitating impact on national security, economy, public health or safety".

- NCIIPC has broadly identified the following as ‘Critical Sectors’ :-
  - Power & Energy
  - **Banking, Financial Services & Insurance**
  - Telecom
  - Transport
  - Government
  - Strategic & Public Enterprises

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.

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 be 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

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**)

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***.

Deter Unethical and Illegal Behaviour

- It is the responsibility of InfoSec personnel to deter unethical and illegal acts, ***using policy, education and training, and technology as controls or safeguards, in order to protect the organization's information and systems.***

- There are three general categories of unethical behavior that organizations and society should seek to eliminate:

  1. Ignorance
  2. Accident
  3. Intent

Deter Unethical and Illegal Behaviour

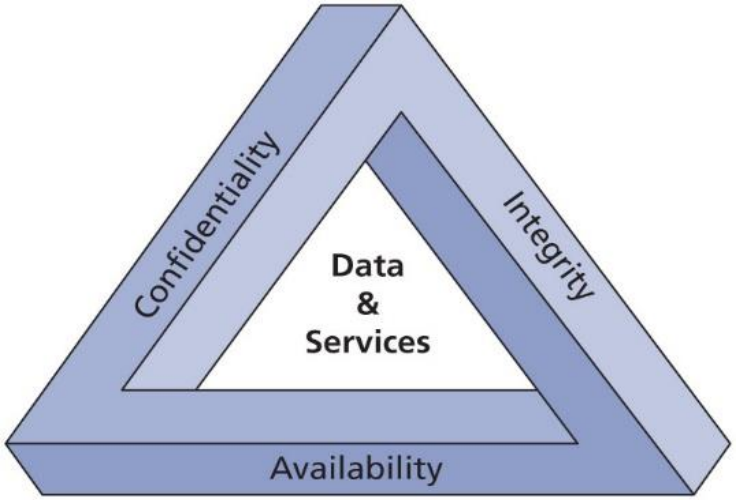
- Deterrence is the best method for preventing illegal or unethical activity.
- Laws, policies, and technical controls are all examples of deterrents.
- However, laws and policies and their associated penalties only deter if three conditions are present:
  - ***Fear of penalty***
  - ***Probability of being caught***
  - ***Probability of penalty being administered***

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



Information Security

There is continuous debate about extending this classic CIA triad.

Other principles include:

- Authenticity,
- Non-repudiation and
- Accountability

Which are also now becoming key considerations for practical security installations

Confidentiality

- Confidentiality is "**an attribute of information that describes how data is protected from disclosure or exposure to unauthorized individuals or systems**"
- Confidentiality supports the principle of "least privilege" by providing that only **authorized individuals, processes, or systems should have access to information on a need-to-know basis**. The level of access that authorized individuals should have is at the level necessary for them to do their job.
- 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)

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

- Integrity is the principle that information should be protected from intentional, unauthorized, or accidental changes. *Information stored in files, databases, systems, and networks must be relied upon to accurately process transactions and provide accurate information for business decision making.*

Availability

- Availability is "**an attribute of information that describes how data is accessible and correctly formatted for use without interference or obstruction**"

- Availability is the principle that ensures that information is available and accessible to users when needed.
- The two primary areas affecting the availability of systems are
  - Denial-of-Service attacks (DoS attack)
  - Loss of service due to a disaster, which could be man-made (e.g., poor capacity planning resulting in a system crash, outdated hardware, and poor testing resulting in system crash after upgrade) or natural (e.g., earthquake, tornado, blackout, hurricane, fire, and flood).

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.

Information Aggregation

- Many organizations collect, swap, and sell personal information as a commodity

- Today, it is possible to collect and combine personal information from several different sources (known as information aggregation) that have resulted in databases that could be used in ways the original data owner has not agreed to or even knows about

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

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

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

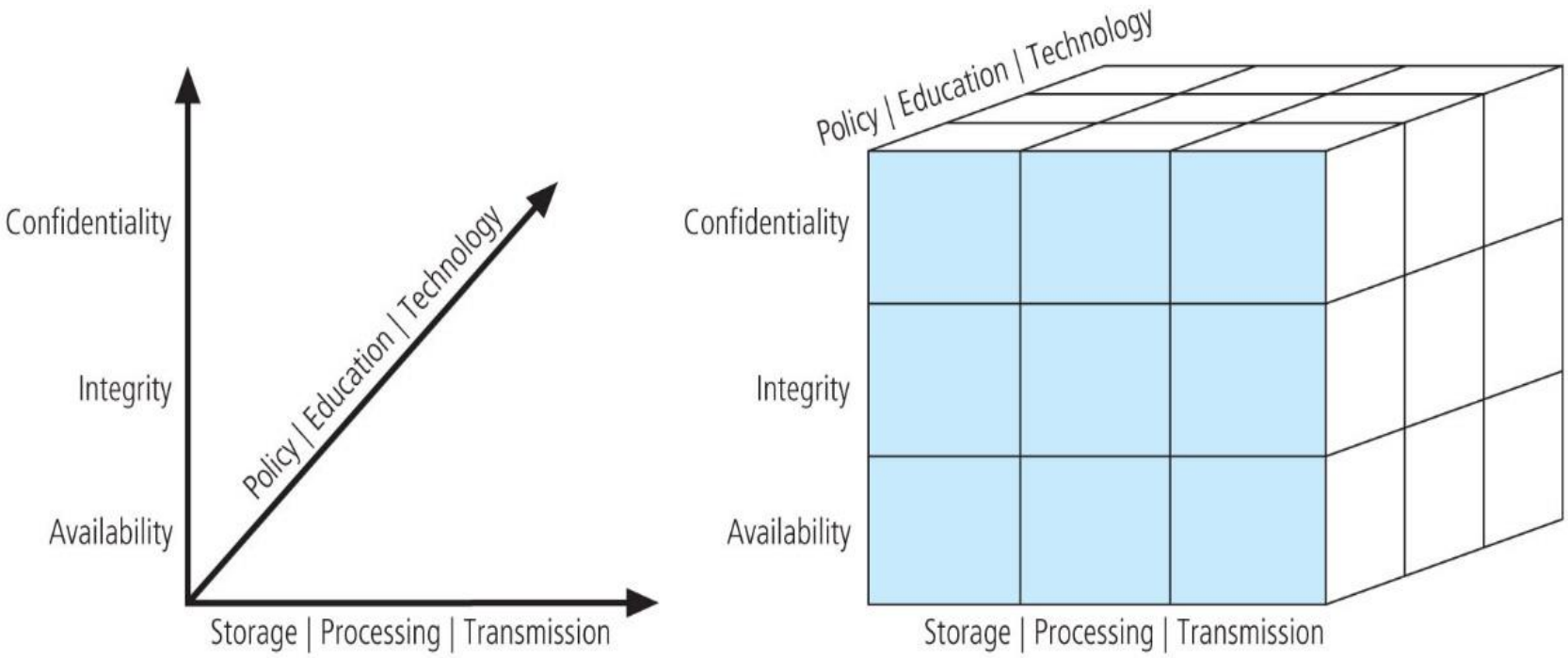
Accountability

- 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

CNSS Security Model



Source:
Management of Information Security: (6th Edition) by Michael E Whitman and Herbert J Mattord, Cengage Learning, USA , 2018

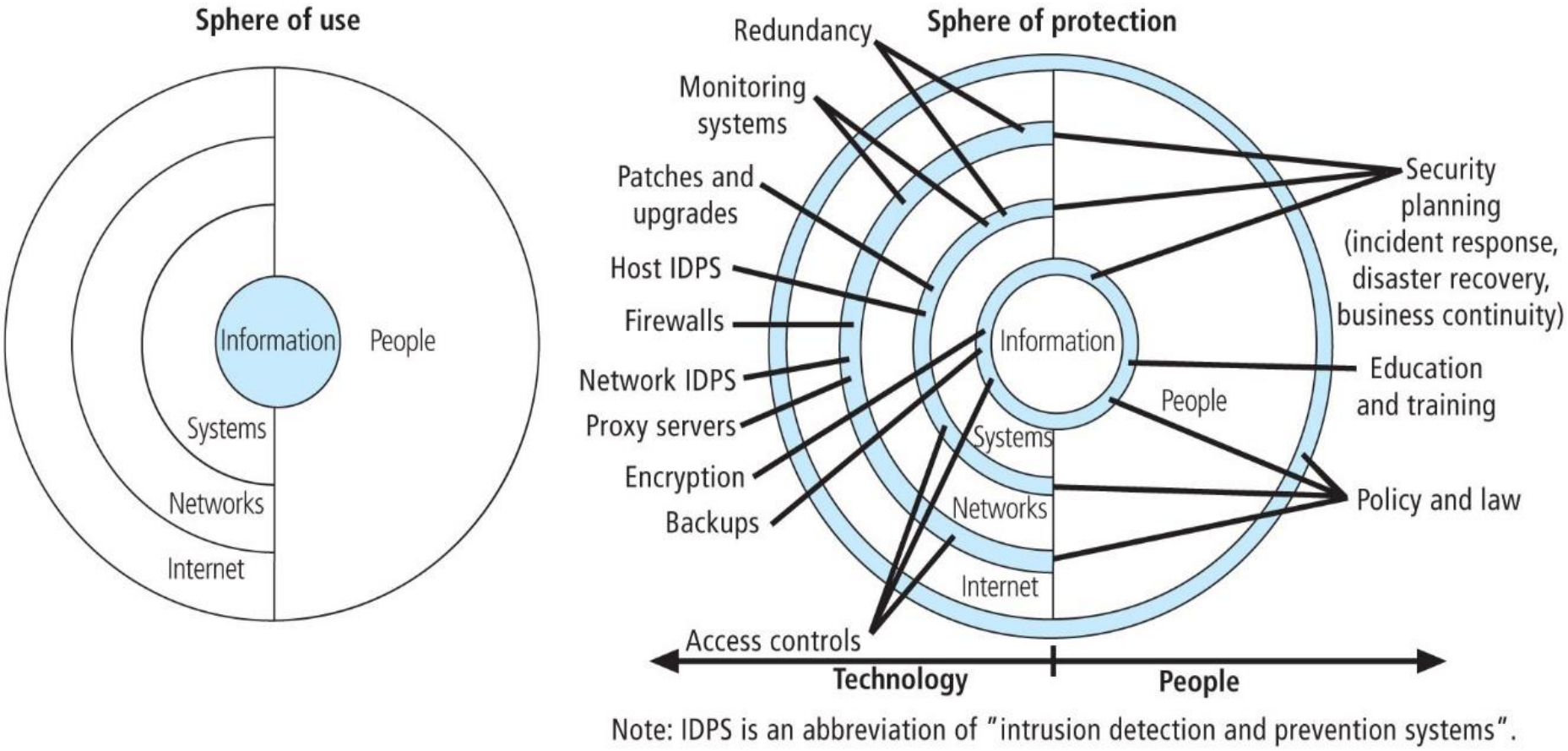


Figure 4-1 Spheres of security

Source:
Management of Information Security: (6th Edition) by Michael E Whitman and Herbert J Mattord, Cengage Learning, USA , 2018

Areas of Security

Specialized areas of security include:

1. **Physical security:** protection of physical items, objects, or areas from unauthorized access and misuse
2. **Operations security:** protection of details of an organization's operations and activities
3. **Communications security:** protection of all communications media, technology, and content
4. **Cyber (or computer) security**: protection of information processing systems and the data they contain and process
5. **Network security**: a subset of communications and cyber security, the protection of voice and data networking components and connections.

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***

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)"

IT-related Business Risk

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

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.

Threat Sources

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.

Threats may be divided into multiple categories, including:

Internal Threats

Threat	• Inadequate training • Not enough time to perform job	• Key personnel moves to another enterprise	• Compromise system • Release data • Coerced to share trade secrets
Risk	Causes business impacts, intentional or unintentional	Leaves gaps in knowledge and skills	Exposes the enterprise to legal and reputational risk

External Threats

Espionage	Theft	Sabotage	Terrorism	Criminal Acts
Software Errors	Hardware Flaws	Mechanical Failures	Lost Assets	Data Corruption
Facility Flaws	Fire	Supply Chain Interruption	Industrial Accidents	Disease (Epidemic)
Seismic Activity	Flooding	Utility Failure	Severe Storms	Natural Disasters

External Threat Actors

- Criminals
- Hacktivists
- Corporate spies
- Thieves
- Advanced persistent threats (APT)

Nation-State

- Sponsored by governments, organized crime or competitors
- Break into systems for military or economic purposes

Hacktivists

- Varied skill set and motivations
- Break into systems to publicly shame or humiliate enterprises

APTs

- Highly skilled attackers persistent in their attempts to exploit systems and networks
- Possess effective tools

Emerging Threats

Examples

- Unusual activity on a system
- Repeated alarms
- Degraded system or network performance
- New or excessive activity in logs

Common Issue

- Compromised organizations have evidence of emergent threats prior to the actual breach

Lack of Monitoring and Response

+ Threat = Breach

Role of Risk Practitioner

- Be alert to the emergence of new technologies
- Prepare for introducing new technologies
- Internet of things (IoT)
  - Example of a revolution in how enterprises view technology assets
  - Risk is self-evident
  - May tempt the enterprise by promising to greatly reduce cost and refresh rate

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.

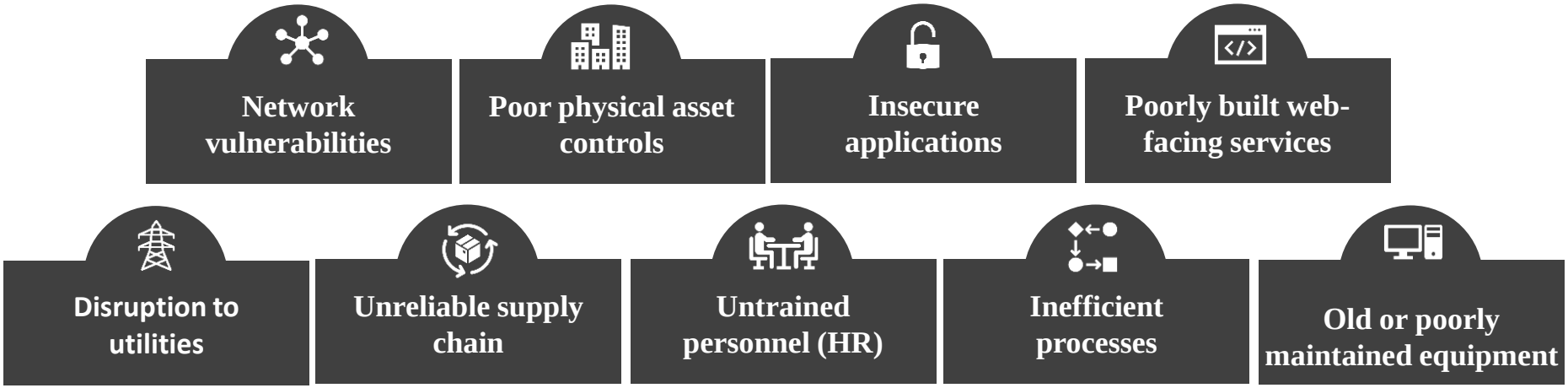
NIST Special Publication 800-30 Revision 1: Guide to Conducting Risk Assessments provides a list of vulnerabilities to consider with predisposing conditions that may lead to the rapid or unpredictable emergence of new vulnerabilities.

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

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



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

Policies, Standards, Guidelines, Procedures, 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***

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

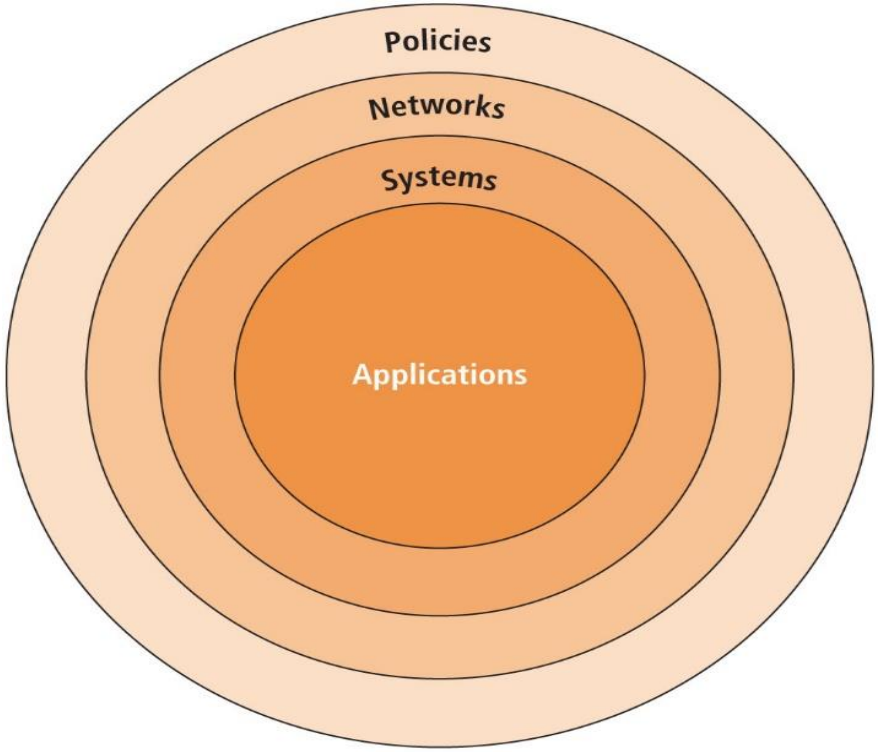
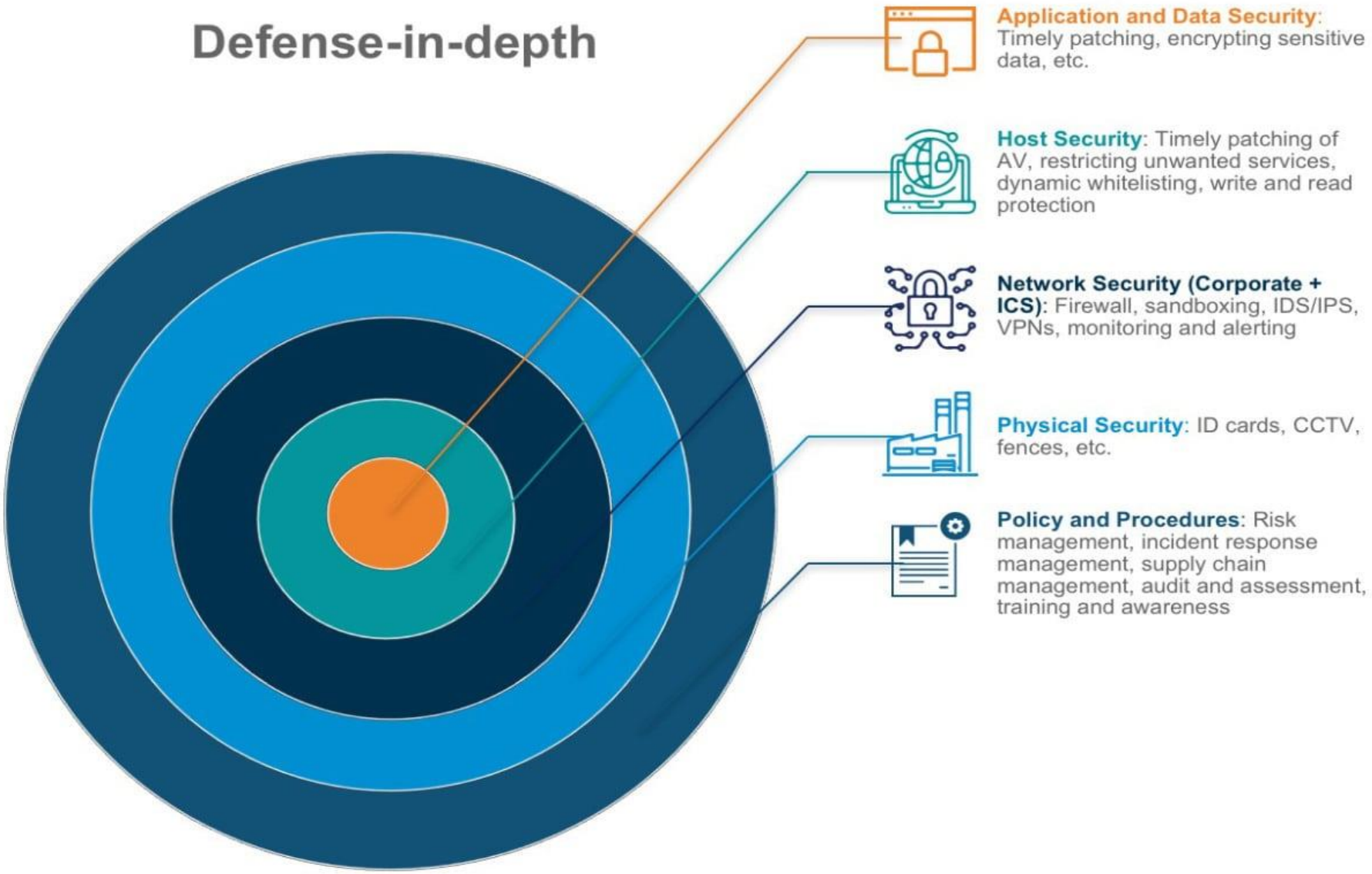


Figure 4-2 Bull's-eye model

Source:
Management of Information Security: (6th Edition) by Michael E Whitman and Herbert J Mattord, Cengage Learning, USA , 2018

Defense in Depth



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, SIM Swap 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

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

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.

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
  - Rainbow tables
  - Social engineering password attack

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

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***

Technical Software Failures

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

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/

Q&A