



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

ACCA7028

Data Security, Governance and Compliance

Week 1 :Introduction to Information Security

Trawsnewid Addysg; Trawsnewid Bywydau
Transforming Education; Transforming Lives



www.uwtsd.ac.uk

Learning Objective(s) and Key Concepts

Learning Objective(s)

- Explain information systems security and its effect on people and businesses.

Key Concepts

- Information systems security concepts
- Confidentiality, integrity, and availability (C-I-A)
- The seven domains of an IT infrastructure
- The weakest link in the security of an IT infrastructure
- IT security policy framework and data classification standard
- IT Security principles

Introduction

- Best security specialists combine practical knowledge and technical skills with understanding of human nature
 - No two systems or situations are identical, and there are no cookbooks to consult on how to solve security problems

Cyberspace: The New Frontier



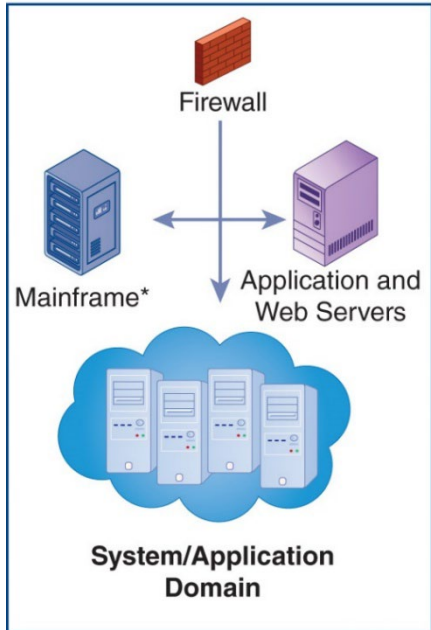
Risks, Threats, and Vulnerabilities

- Risk
 - The level of exposure to some event that has an effect on an asset
- Threat
 - Any action, either natural or human induced, that could damage an asset
- Vulnerability
 - A weakness that allows a threat to be realized or to have an effect on an asset

What Is Information Systems Security?

- Information system
 - Hardware, operating system, and application software that work together to collect, process, and store data for individuals and organisations
- Security
 - Being free from danger or risk
- Information systems security
 - The collection of activities that protect the information system and the data stored in it

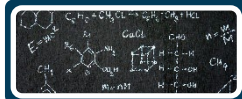
What Are We Securing?



*Note: Used for bulk data processing requiring massive throughput

- Privacy Data of Individuals
 - Name, address, date of birth
 - Social Security number
 - Bank name, account number
 - Credit card account number
 - Utility account number
 - Mortgage account number
 - Insurance policy number
 - Securities and brokerage account numbers
- Corporate Intellectual Property
 - Trade secrets
 - Product development
 - Sales and marketing strategies
 - Financial records
- Copyrights, patents, etc.
- Online B2C and B2B Transactions
 - Online banking
 - Online health care and insurance claims
 - E-commerce, e-government, services
 - Online education and transcripts
- Government Intellectual Property
 - National security
 - Military strategies

Compliance Laws and Regulations Drive the Need for Information Systems Security



Education

- UK Education Regulations (Prevent Duty / Online Safety Requirements)
- US CIPA (Children's Internet Protection Act)



Education

- UK Data Protection Act 2018 (for educational institutions)
- US FERPA (Family Educational Rights and Privacy Act)



Government

- UK NIS Regulations (Network and Information Systems)
- US FISMA (Federal Information Security Management Act)



Corporation

- UK Corporate Governance Code
- US SOX (Sarbanes-Oxley Act)



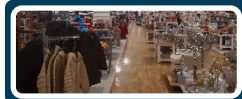
Health care

- UK Data Protection Act 2018 / GDPR
- US- HIPAA (Health Insurance Portability and Accountability Act)



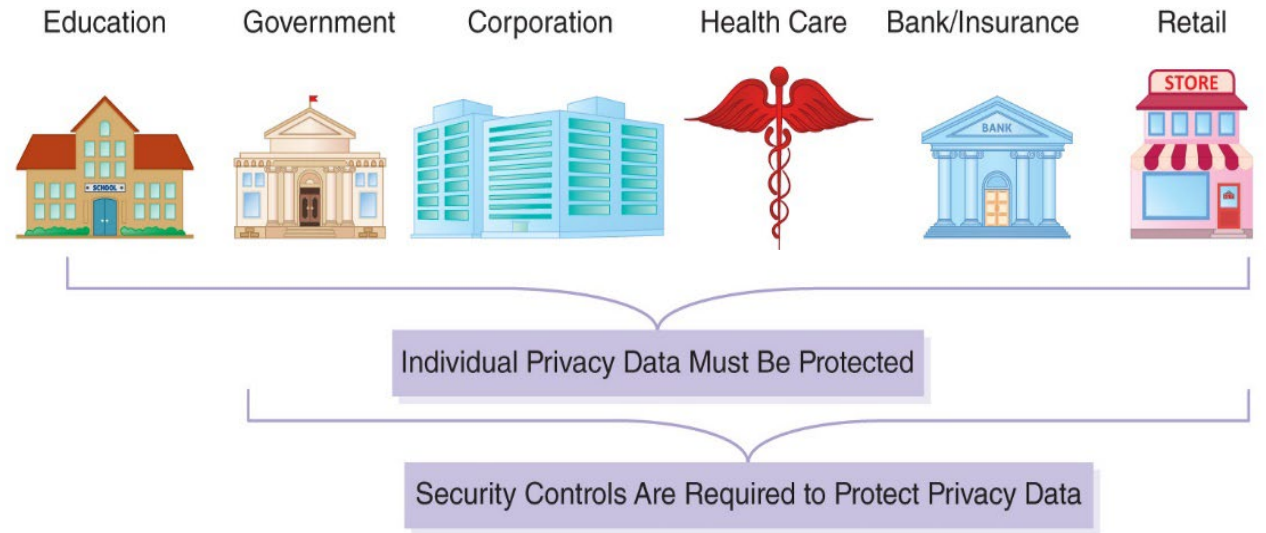
Bank/Insurance

- UK Data Protection Act 2018 / GDPR
- US GLBA (Gramm-Leach-Bliley Act)

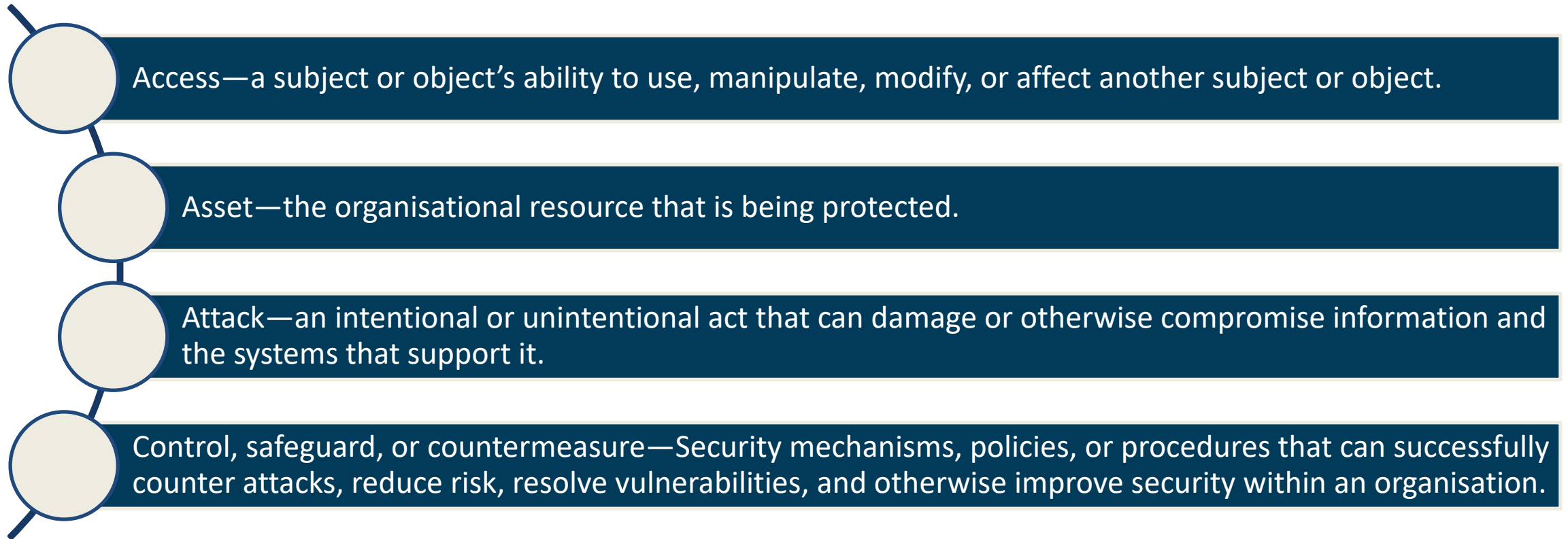


Retail

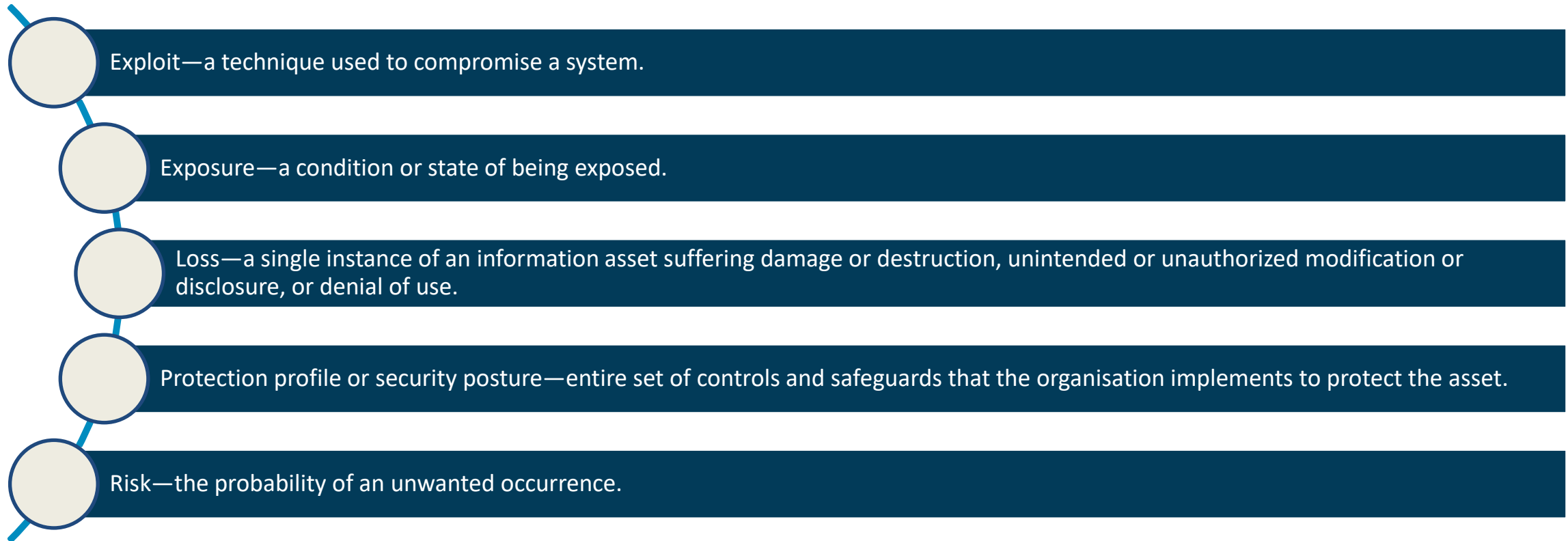
- PCI DSS (Payment Card Industry Data Security Standard) - Global standard



Key Information Security terms & concepts (1)



Key Information Security terms & concepts (2)



Key Information Security terms & concepts (3)



Subjects and objects—a computer can be either an agent entity used to conduct an attack or the target entity.

Threat agent—the specific instance or a component of a threat.

Threat source—a category of objects, people, or other entities that represents a danger to an asset.

Vulnerability—weaknesses or faults in a system or protection mechanism that expose information to attack or damage.

An information security breach process

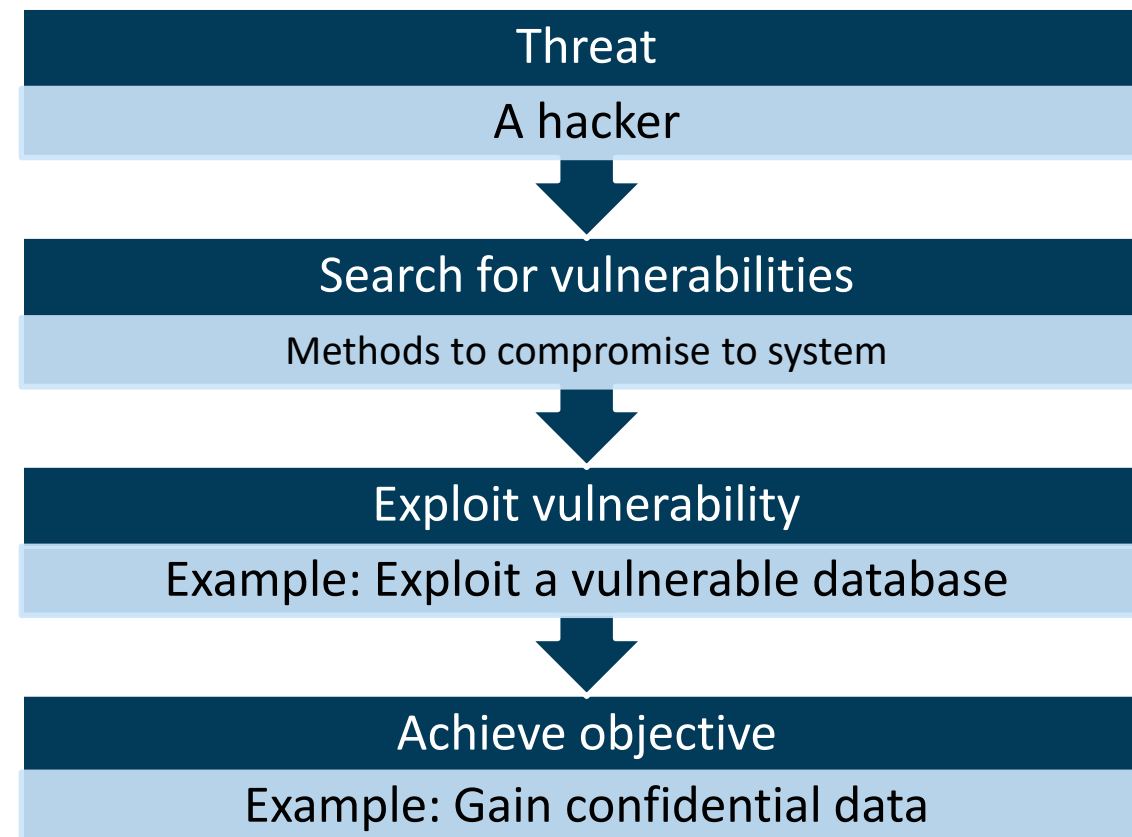
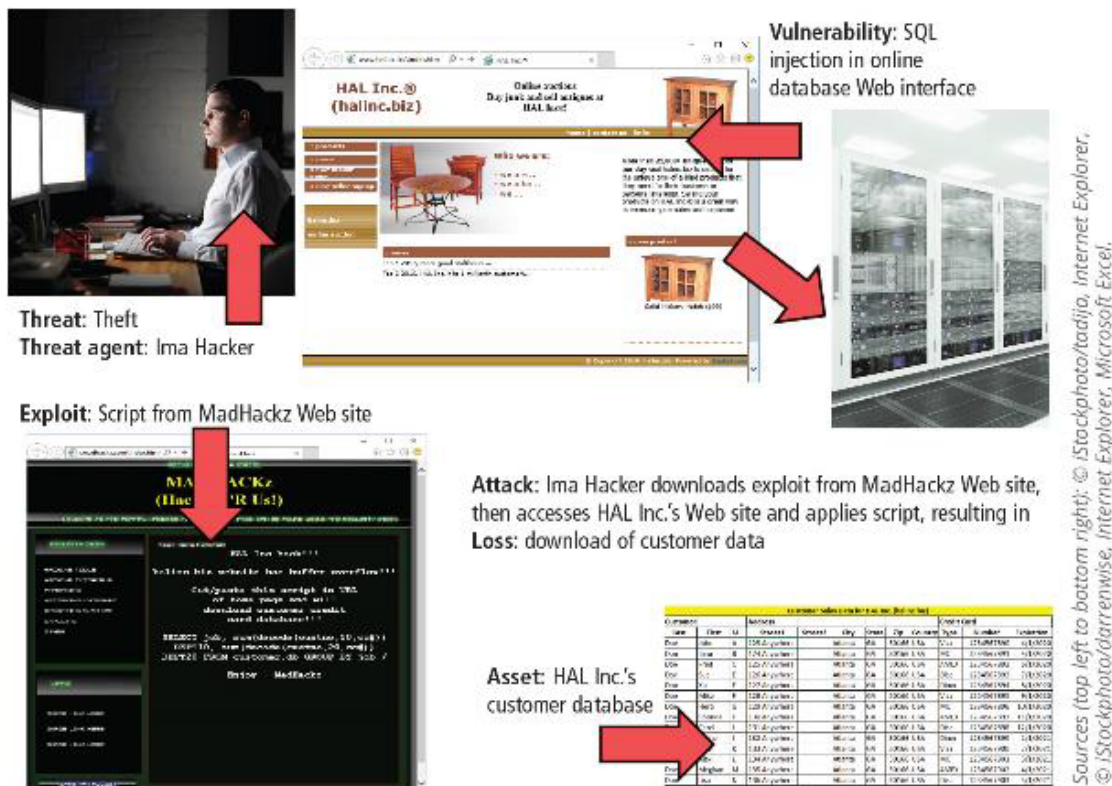


Figure 1-7 Key concepts in information security

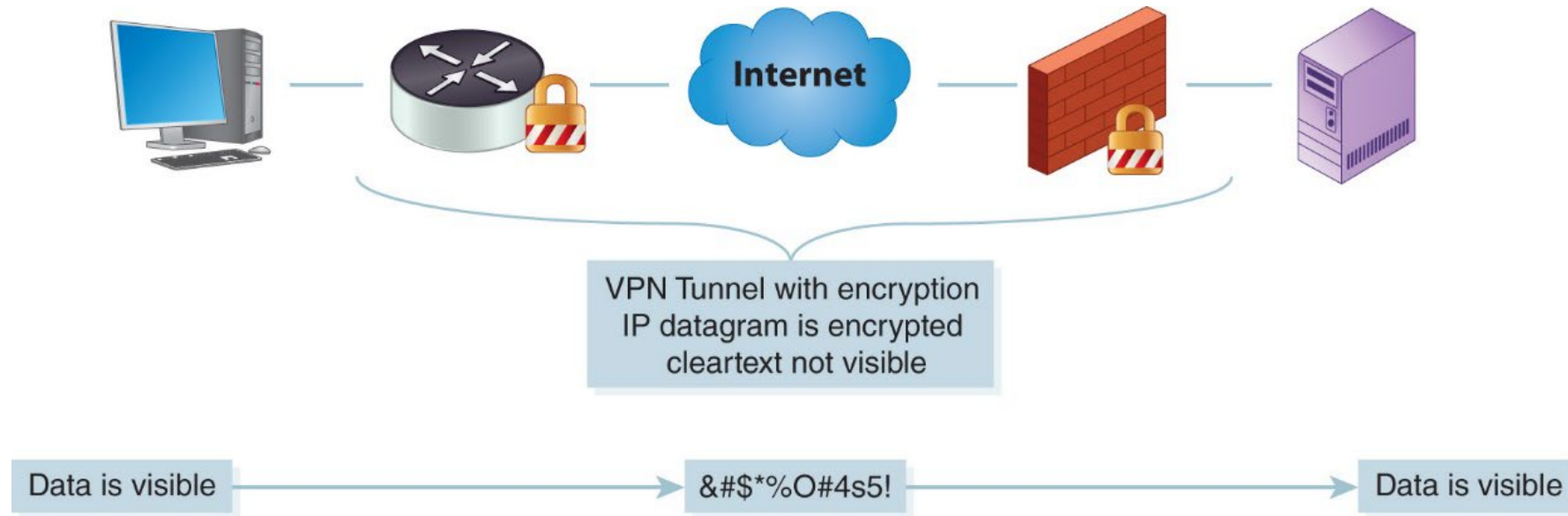
Tenets of Information Security

- Confidentiality
 - Only authorised users can view information
- Integrity
 - Only authorised users can change information
- Availability
 - Information is accessible by authorised users whenever they request the information

Confidentiality

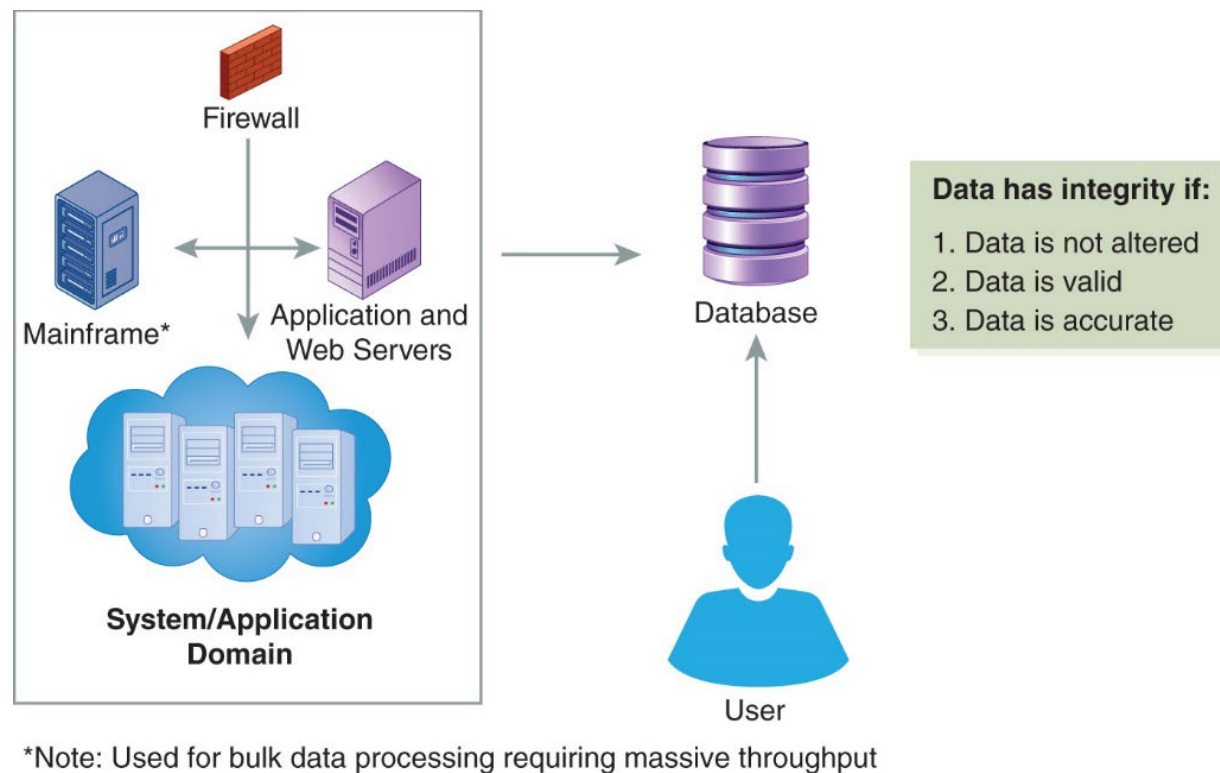
- Confidentiality is “an attribute of information that describes how data is protected from disclosure or exposure to unauthorized individuals or systems”
- Confidential information includes:
 - Private data of individuals
 - Intellectual property of businesses
 - National security for countries and governments
- Examples of confidentiality measures and controls include:
 - Cryptography
 - Practice of hiding data and keeping it away from Unauthorised users
 - Encryption
 - The process of transforming data from cleartext into ciphertext
 - Ciphertext
 - The scrambled data that results from encrypting cleartext

Encryption of Cleartext into Ciphertext



Integrity

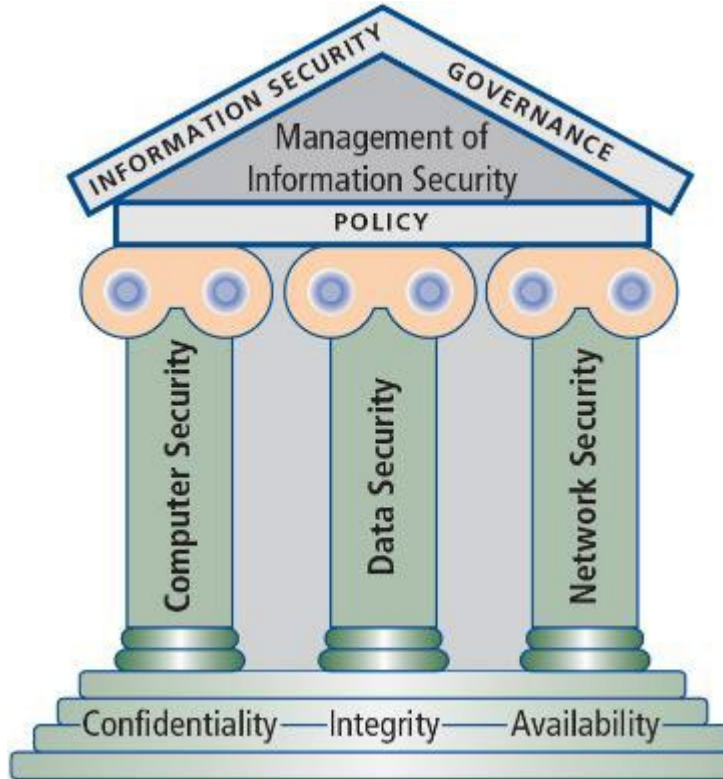
- Maintain valid and accurate information
- Integrity is “an attribute of information that describes how data is whole, complete, and uncorrupted”
- The integrity of information is threatened when it is exposed to corruption, damage, destruction, or other disruption of its authentic state
- Corruption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



Availability

- In the context of information security
 - The amount of time users can use a system, application, and data
- 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

Modern Security needs!



- A successful organisation should have multiple layers of security in place to protect:
 - Operations
 - Physical Infrastructure
 - People
 - Functions
 - Communications
 - Information

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 (the meaning usually associated with the word); it means that the information will be used only in ways approved by the person who provided it

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 has 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

Authorisation

- Authorisation 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, authorisation 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

Critical Characteristics of Information: The value

Confidentiality

Prevents disclosure or exposure to unauthorized individuals or systems

Integrity

Maintains a complete, uncorrupted, and authentic state
Threatened by corruption, damage, or destruction

Availability

Accessible to authorized users without interference
Available in the correct format when and where needed

Critical Characteristics of Information: The value

Accuracy:

Free from mistakes or errors

Must meet user expectations; inaccurate if modified intentionally or unintentionally

Authenticity:

Genuine and original, not a reproduction

Reflects the information originally created, stored, or transferred

Utility:

Information must be in a meaningful format to serve its purpose

Possession:

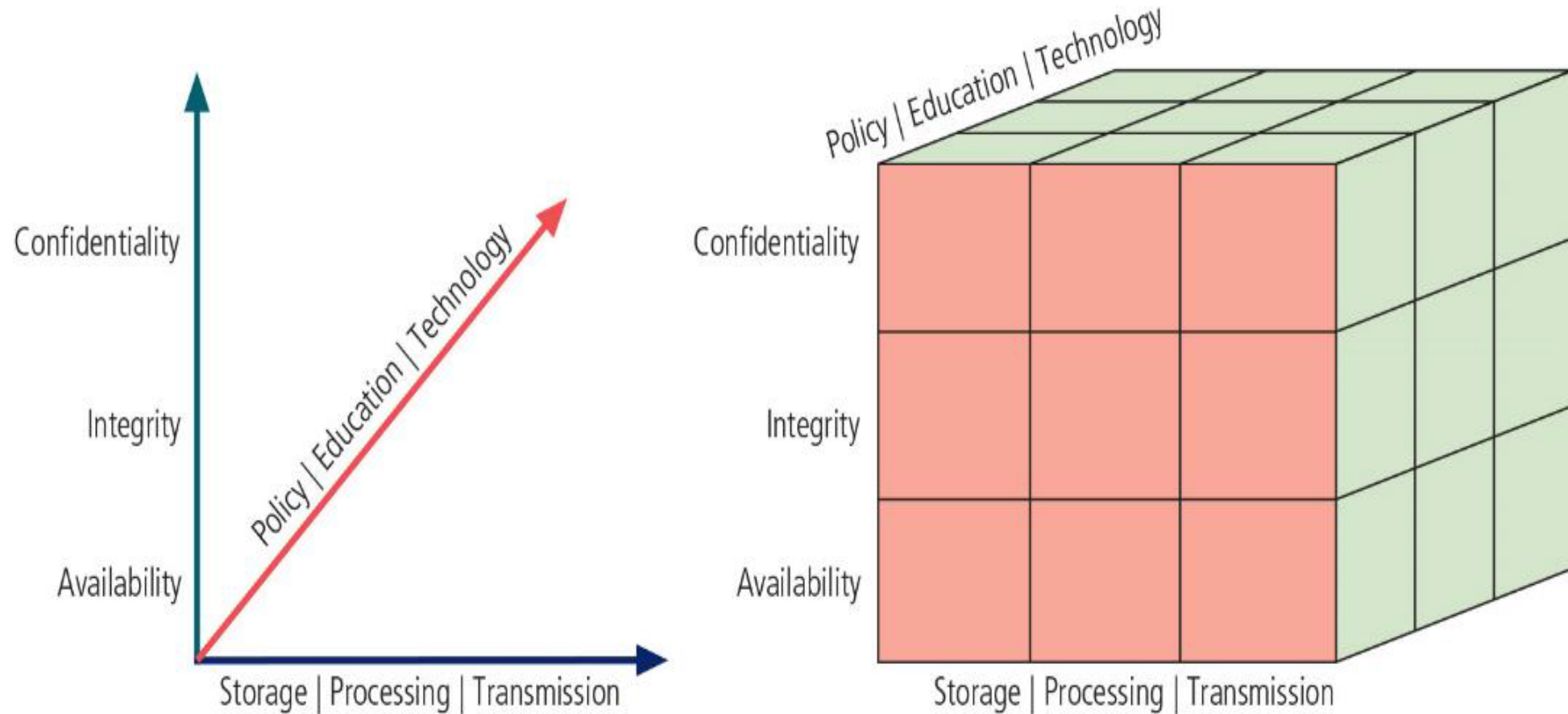
Ownership or control of information

Breach of possession does not always breach confidentiality

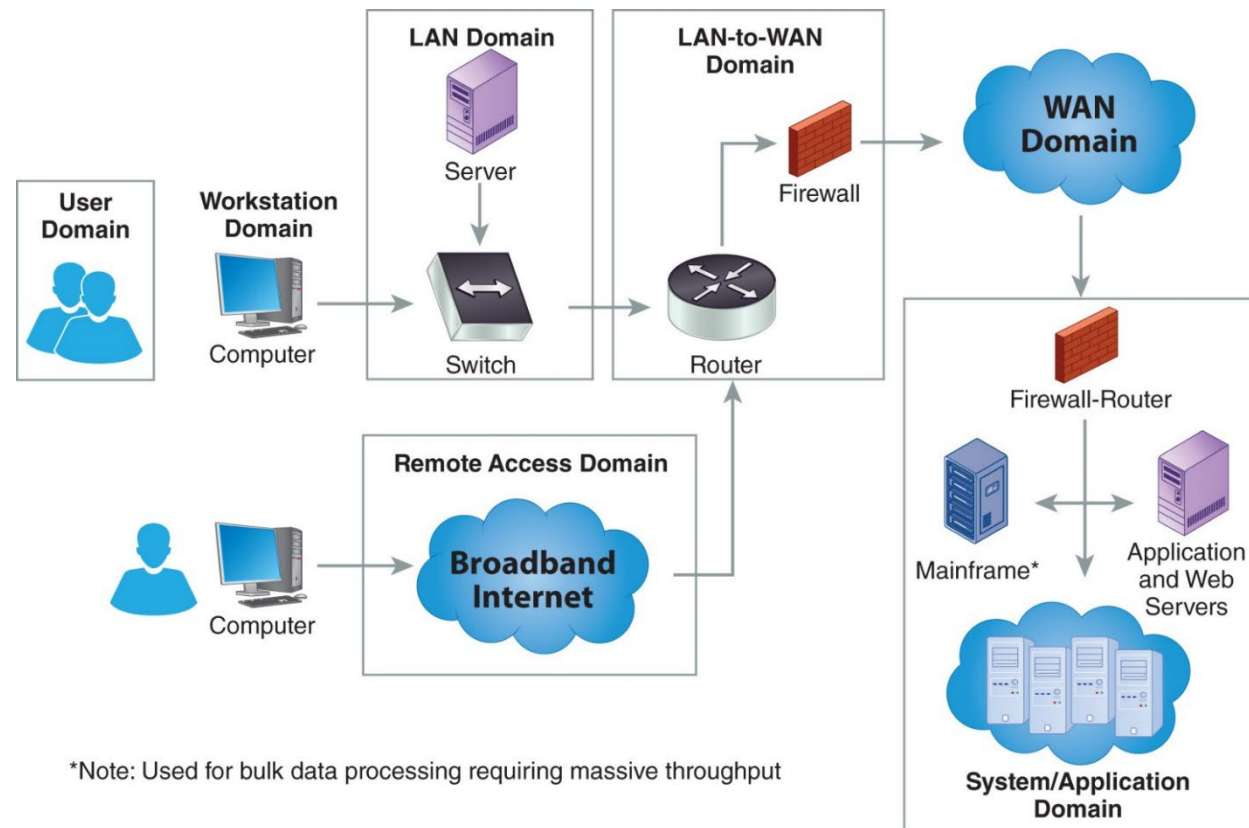
CNSS Security Model

- Developed by the Committee on National Security Systems (CNSS) , also known as the **McCumber Cube**
- The model is composed of a three key dimensions:
 - **Security Goals (The C.I.A. Triad)**
 - **Information States**
 - **Security Countermeasures**
- The CNSS model provides a holistic view of security by considering not just the C.I.A. principles but also the various states of information and the human, technical, and policy-based aspects of security.

CNSSS Security Model



Seven Domains of a Typical IT Infrastructure



User Domain

- Roles and tasks
 - Users can access systems, applications, and data depending upon their defined access rights
- Responsibilities
 - Employees are responsible for their use of IT assets
- Accountability
 - Human resources department is accountable for implementing proper employee background checks

Common Threats in the User Domain

- Unauthorised access
- Lack of user awareness
- User apathy toward policies
- Security policy violations
- User inserting CD/DVD/USB with personal files
- User downloading photos, music, or videos
- User destroying systems, applications, and data
- Disgruntled employee attacking organisation or committing sabotage
- Employee romance gone bad
- Employee blackmail or extortion

Workstation Domain

- Roles and tasks
 - Configure hardware, harden systems, and verify antivirus files
- Responsibilities
 - Ensure the integrity of user workstations and data
- Accountability
 - Ensure that the Workstation Domain conforms to policy

Common Threats in the Workstation Domain

- Unauthorised workstation access
- Unauthorised access to systems, applications, and data
- Desktop or laptop operating system and software vulnerabilities
- Desktop or laptop application software vulnerabilities and patches
- Viruses, malicious code, and other malware
- User inserting CD/DVD/USB with personal files
- User downloading photos, music, or videos
- Security risk due to user violation of acceptable use policy (AUP)
- Bring Your Own Device (BYOD)

LAN Domain

- Roles and tasks
 - Includes both physical network components and logical configuration of services for users
- Responsibilities
 - Physical components and logical elements
- Accountability
 - Maximise use and integrity of data within the local area network (LAN) Domain

Common Threats in the LAN Domain

- Unauthorised access to LAN
- Unauthorised access to systems, applications, and data
- LAN server operating system software vulnerabilities
- LAN server application software vulnerabilities and software patch updates
- Unauthorised access by rogue users on wireless LANs (WLANs)
- Compromised confidentiality of data on WLANs
- LAN servers with different hardware, operating systems, and software make them difficult to manage and troubleshoot

LAN-to-WAN Domain

- Roles and tasks
 - Includes both the physical pieces and logical design of security appliances; physical parts need to be managed to give easy access to the service
- Responsibilities
 - Physical components, logical elements, and applying the defined security controls
- Accountability
 - Ensure that LAN-to-Wide Area Network (WAN) Domain security policies, standards, procedures, and guidelines are used

Common Threats in the LAN-to-WAN Domain

- Unauthorised network probing and port scanning
- Unauthorised access through the LAN-to-WAN Domain
- Denial of service (DoS)/distributed denial of service (DDoS) attacks
- IP router, firewall, and network appliance operating system vulnerability
- IP router, firewall, and network appliance configuration file errors or weaknesses
- Remote user download of sensitive data
- Download of unknown file type attachments from unknown sources
- Unknown email attachments and embedded URL links received by local users
- Lost productivity due to local users surfing the web

WAN Domain

- Roles and tasks
 - Allow users the most access possible while making sure what goes in and out is safe
- Responsibilities
 - Physical components and logical elements
- Accountability
 - Maintain, update, and provide technical support and ensure that the company meets security policies, standards, procedures, and guidelines

Common Threats in the WAN Domain (Internet)

- Open, public, and accessible data
- Most Internet traffic sent as cleartext
- Vulnerable to eavesdropping
- Vulnerable to malicious attacks
- Vulnerable to DoS and DDoS attacks, TCP synchronize (SYN) flooding, and IP spoofing attacks
- Vulnerable to corruption of information/data
- Insecure Transmission Control Protocol/Internet Protocol (TCP/IP) applications
- Hackers, attackers, and perpetrators email Trojans, worms, and malicious software

Common Threats in the WAN Domain (Connectivity)

- Commingling of WAN IP traffic on the same service provider router and infrastructure
- Maintaining high WAN service availability
- Maximizing WAN performance and throughput
- Using Simple Network Management Protocol (SNMP) applications and protocols maliciously (ICMP, Telnet, SNMP, DNS, etc.)
- SNMP alarms and security monitoring 24/7/365

Remote Access Domain

- Roles and tasks
 - Connect mobile users to their IT systems through the public Internet
- Responsibilities
 - Maintain, update, and troubleshoot the hardware and logical remote access connection
- Accountability
 - Ensure that the Remote Access Domain security plans, standards, methods, and guidelines are used

Common Threats in the Remote Access Domain

- Brute-force user ID and password attacks
- Multiple logon retries and access control attacks
- Unauthorised remote access to IT systems, applications, and data
- Private or confidential data compromised remotely
- Data leakage in violation of data classification standards
- A mobile worker's laptop is stolen
- Mobile worker token or other authentication stolen

System/Application Domain

- Roles and tasks
 - Includes hardware, operating system software, applications, and data and includes logical design
 - Secure mission-critical applications and intellectual property assets both physically and logically
- Responsibilities
 - Server systems administration, database design and management, designing access rights to systems and applications, and more
- Accountability
 - Ensure that the System/Application Domain is in compliance with security policies, standards, procedures, and guidelines

Common Threats in the System/Application Domain

- Unauthorised access to data centers, computer rooms, and wiring closets
- Downtime of servers to perform maintenance
- Server operating systems software vulnerability
- Insecure cloud computing virtual environments by default
- Susceptibility of client-server and web applications
- Unauthorised access to systems
- Data breach where private data is compromised
- Corrupt or lost data
- Loss of backed-up data as backup media are reused
- Recovery of critical business functions potentially too time consuming to be useful
- Downtime of IT systems for an extended period after a disaster

Weakest Link in the Security of an IT Infrastructure

- Humans are the weakest link in security
- Strategies for reducing risk:
 - Check background of job candidates carefully
 - Evaluate staff regularly
 - Rotate access to sensitive systems, applications, and data among staff positions
 - Test applications and software and review for quality
 - Regularly review security plans
 - Perform annual security control audits

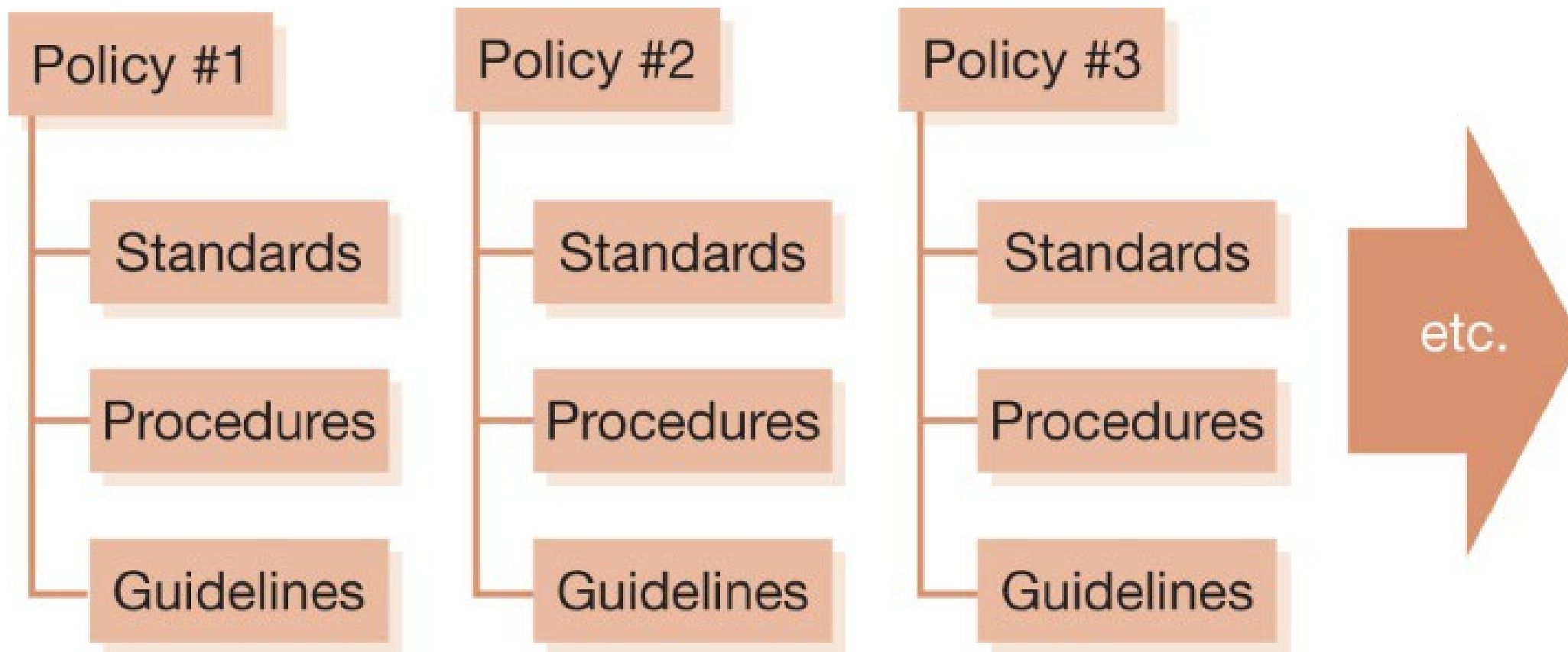
Ethics and the Internet

- Human behaviour online is often less mature than in normal social settings
- Demand for systems security professionals is growing rapidly
- Systems security professionals are responsible for is doing what is right and stopping what is wrong
- The UK Cyber Security Council ethics committee
 - A self-regulatory body for the UK's cyber security profession.
 - Formed in August 2019 the Department for Digital, Culture, Media and Sport (DCMS) appointed the IET as the lead organisation in charge of designing and delivering the new UK Cyber Security Council
 - Responsibilities include defining policies regarding acceptable behaviour or Cyber Security professionals and organisations that retain data for users and looks at ethical breaches.
- The U.S. government and Internet Architecture Board (IAB) defined a policy regarding acceptable use of Internet geared toward U.S. citizens
 - Policy is not a law nor mandated

IT Security Policy Framework

- Policy
 - A short written statement that defines a course of action that applies to entire organisation
- Standard
 - A detailed written definition of how software and hardware are to be used
- Procedures
 - Written instructions for how to use policies and standards
- Guidelines
 - Suggested course of action for using policy, standard, or procedure

Hierarchical IT Security Policy Framework



Foundational IT Security Policies

- Acceptable use policy (AUP)
- Security awareness policy
- Asset classification policy
- Asset protection policy
- Asset management policy
- Vulnerability assessment/management policy
- Threat assessment and monitoring policy

Data Classification Standards

- Private data
 - Data about people that must be kept private
- Confidential
 - Information or data owned by the organisation
- Internal use only
 - Information or data shared internally by an organisation
- Public domain data
 - Information or data shared with the public

Data Classification Standards

- U.S. federal government data classification standards:
- Top secret
 - Applies to information that the classifying authority finds would cause grave damage to national security if it were disclosed
- Secret
 - Applies to information that the classifying authority finds would cause serious damage to national security if it were disclosed
- Confidential
 - Applies to information that the classifying authority finds would cause damage to national security

Principle 1: There Is No Such Thing as Absolute Security

- Given enough time, tools, skills, and inclination, a hacker can break through any security measure
- Security testing can buy additional time so the attackers are caught in the act

Principle 2: The Three Security Goals Are Confidentiality, Integrity, and Availability

- All information security measures try to address at least one of the three goals:
- Protect the *confidentiality* of data
 - Confidentiality models are primarily intended to ensure that no unauthorized access to information is permitted and that accidental disclosure of sensitive information is not possible
- Preserve the *integrity* of data
 - Integrity models keep data pure and trustworthy by protecting system data from intentional and accidental changes
- Promote the *availability* of data for authorized use
 - Availability models keep data and resources available for authorized use during denial-of-service attacks, natural disasters, and equipment failures

Principles 3: Defense in Depth as Strategy

- Defense in depth
 - Involves implemented security in overlapping layers that provide the three elements needed to secure assets: prevention, detection, and response
 - The weaknesses of one security layer are offset by the strengths of two or more layers

Principle 4: When Left on Their Own, People Tend to Make the Worst Security Decisions

- Takes little to convince someone to give up their credentials in exchange for trivial or worthless goods
- Many people are easily convinced to double-click the attachment or links inside emails

Principle 5: Computer Security Depends on Two Types of Requirements: Functional & Assurance

- Functional requirements
 - Describe what a system should do
- Assurance requirements
 - Describe how functional requirements should be implemented and tested

*Does the system do **the right things in the right way**?*

- **Verification:** *The process of confirming that one or more predetermined requirements or specifications are met*
- **Validation:** *A determination of the correctness or quality of the mechanisms used in meeting the needs*

Principle 6: Security Through Obscurity Is Not an Answer

- Many people believe that if hackers don't know how software is secured, security is better
 - Although this seems logical, it's actually untrue
- Obscuring security leads to a false sense of security, which is often more dangerous than not addressing security at all

Principle 7: Security = Risk Management

- Security is not concerned with eliminating all threats within a system or facility but with **eliminating known threats and minimizing losses** if an attacker succeeds in exploiting a vulnerability
- Spending more on security than the cost of an asset is a waste of resources
- Risk assessment and risk analysis are used to **place an economic value on assets to best determine appropriate countermeasures** that protect them from losses

Principle 8: 3 Types of Security Controls

Preventative, Detective, and Responsive

- A security mechanism serves a purpose by **preventing a compromise, detecting that a compromise or compromise attempt** is underway, or **responding to a compromise** while it is happening or after it has been discovered

Principle 9: Complexity Is the Enemy of Security

- The more complex a system gets, the harder it is to secure

Principle 10: Fear, Uncertainty, and Doubt (FUD) Do Not Work in Selling Security

- Information security managers must justify all investments in security using techniques of the trade
- When spending resources can be justified with good, solid business rationale, security requests are rarely denied

Principle 11: People, Process, and Technology Are All Needed to Adequately Secure a System or Facility

- **People controls**
 - Dual control and separation of duties
- **Process controls**
 - Different people can perform the same operation the same way every time
- **Technology alone without people and process controls can fail**
- **People, process, and technology controls are essential elements of security practices** including operations security, applications development security, physical security, and cryptography

Principle 12: Open Disclosure of Vulnerabilities Is Good for Security!

- Keeping a given vulnerability secret from users and from the software developer can only lead to a false sense of security
- The need to know trumps the need to keep secrets to give users the right to protect themselves

References

- Lectures slides are devices from the recommended books resources.
 - Pearson Education 2014, Information Security: Principles and Practices, 2nd Edition
 - Fundamentals of Information Systems Security, by David Kim , and Michael G. Solomon



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Any Questions?

Trawsnewid Addysg; Trawsnewid Bywydau
Transforming Education; Transforming Lives



www.uwtsd.ac.uk