



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

ACCA5034

Data Security 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

- Define information security
- Explain how it evolved into information security
- Define key terms and critical concepts of information security
- Describe the information security roles of professionals within an organisation

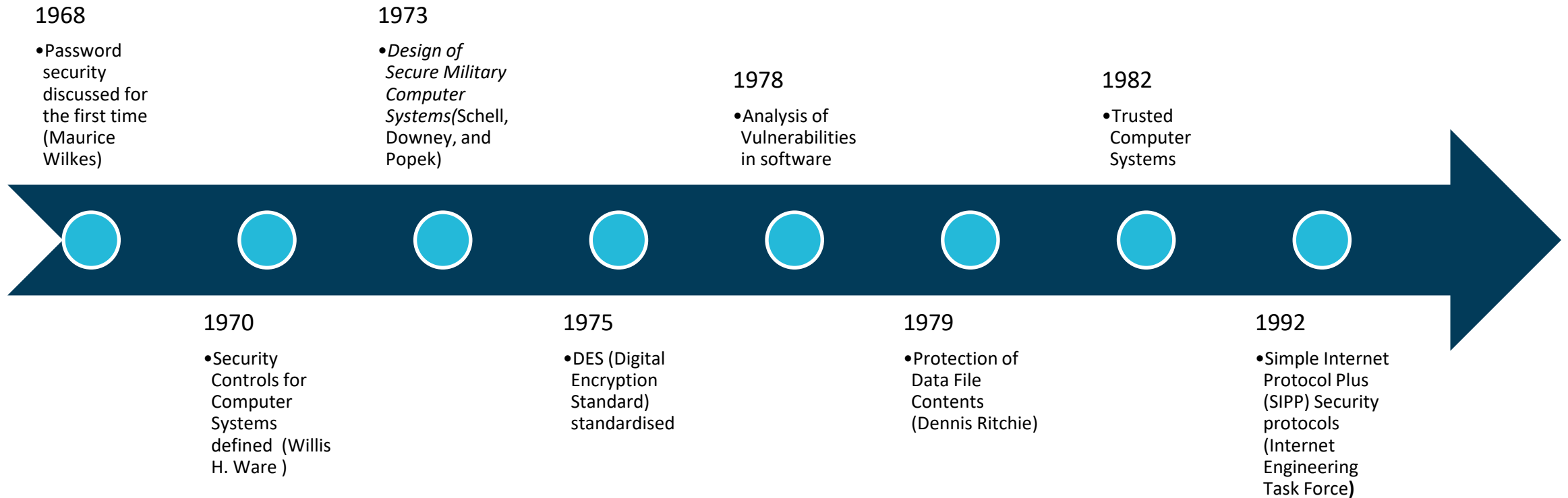
Introduction

- Every organisation, whether public or private and regardless of size, has information it wants to protect.
- Organisations have a responsibility to all their stakeholders to protect that information.
- Unfortunately, there aren't enough security professionals to go around.
- If you're not part of the solution, you're part of the problem.

The History of Information Security

- Computer security began immediately after the first mainframes were developed.
 - Groups developing code-breaking computations during World War II created the first modern computers.
 - Multiple levels of security were implemented to protect these devices.
- During these early years, information security was a straightforward process composed predominantly of physical security and simple document classification schemes.
- The primary threats to security were physical theft of equipment, espionage against products of the systems, and sabotage.

Key Dates in Information Security



2000 to Present

- Exponential growth of the number of insecure devices
- The ability to secure a computer's data was influenced by the security of every computer to which it is connected.
- The growing threat of cyberattacks has increased the awareness of need for improved security.
- Evolution of threat actors from:
 - Semi-professional hackers defacing websites for amusement
 - Professional cybercriminals focusing on theft and extortion
 - Government-sponsored cyberwarfare targeting military, government, and commercial entities

What Is Security?

Definition of Security

- State of being secure and free from danger or harm
- Actions taken to ensure security

Definition of Information Security

- Protection of information and its critical elements, including systems and hardware used to store, transmit, and process information

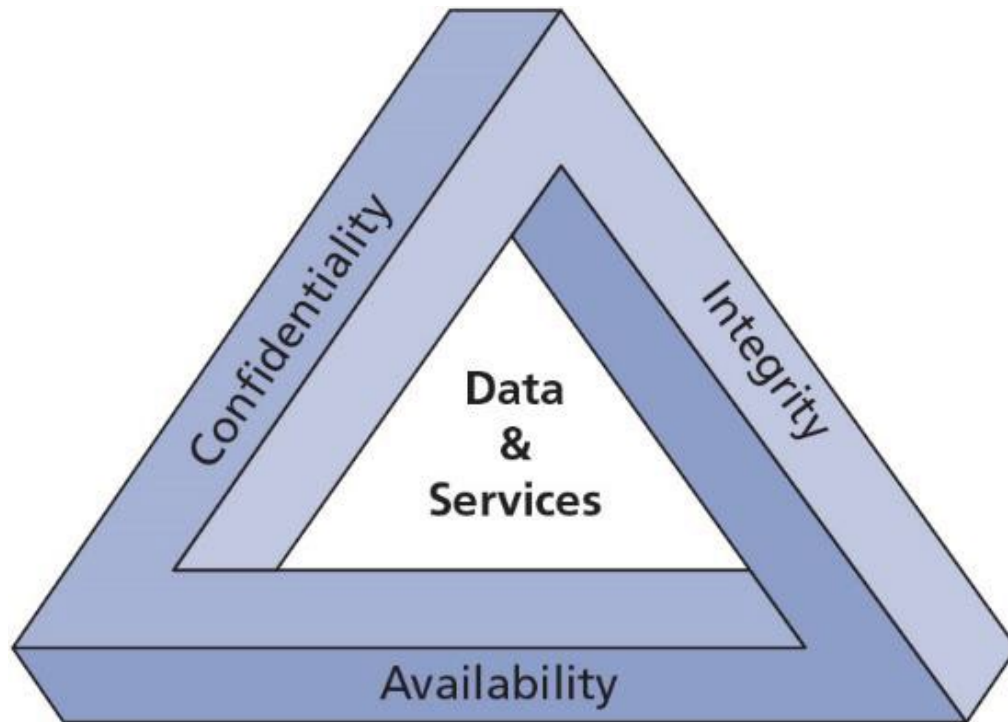
Components of Information Security (InfoSec)

Information
security
management

Data security

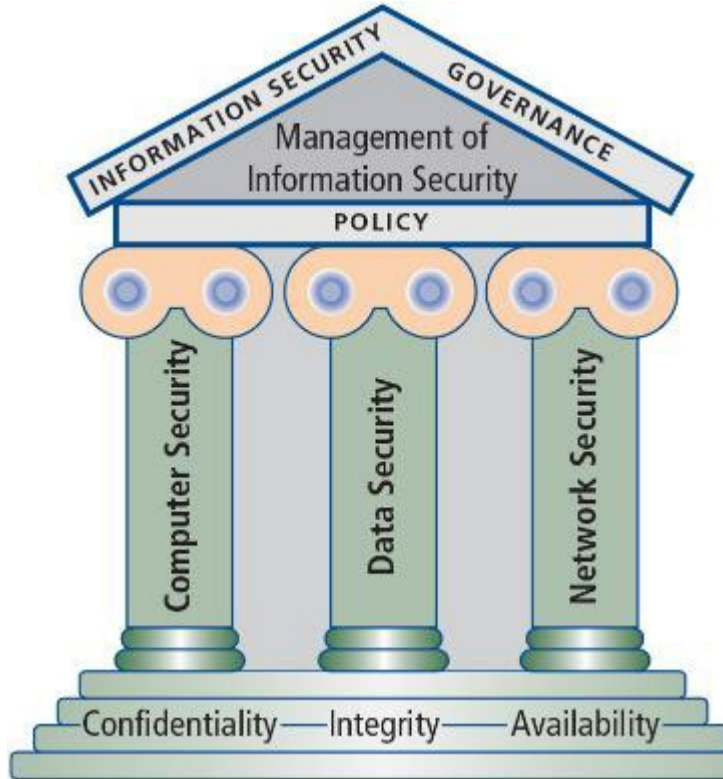
Network
security

Cyber Security Tents- The C.I.A triad



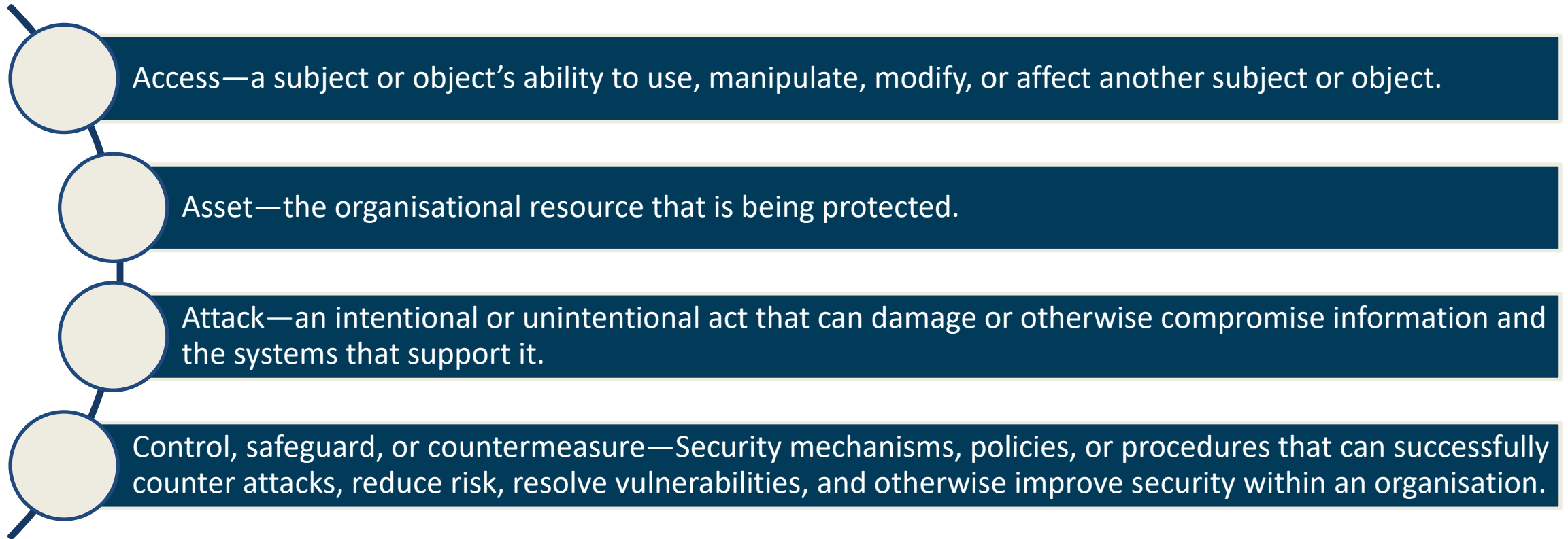
- Based on confidentiality, integrity, and availability
- Now considered inadequate
 - Does not meet all the needs of a modern Information System environment

Modern Security needs!

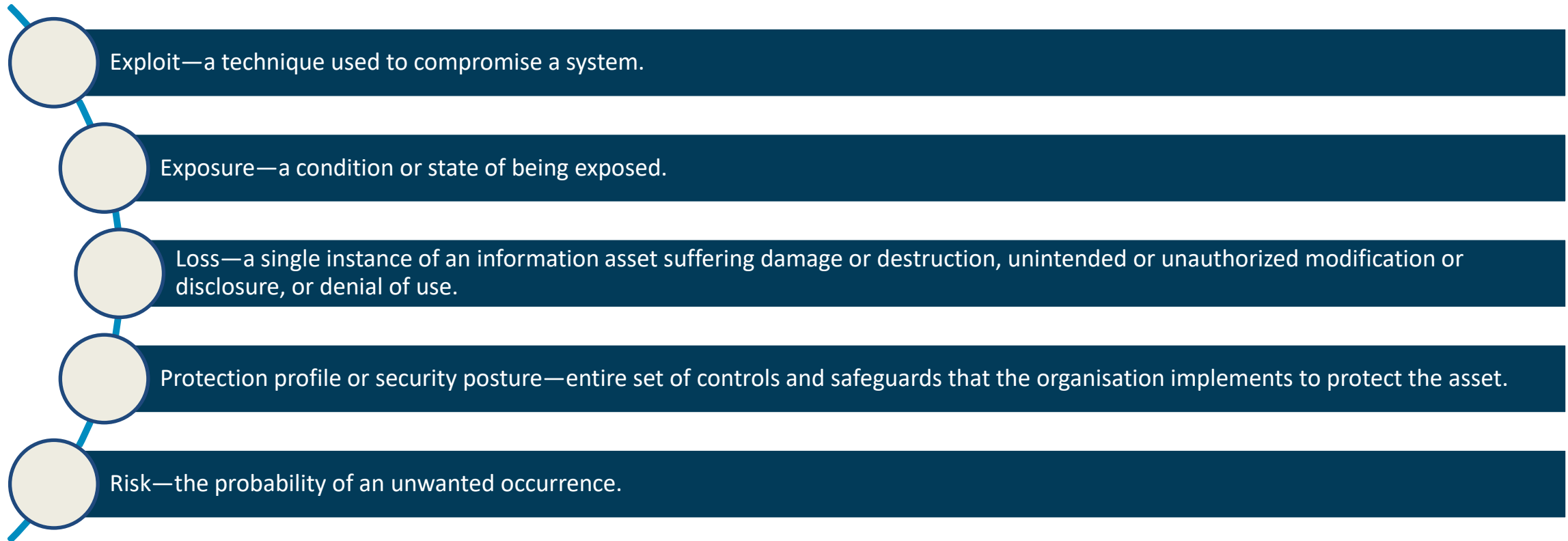


- A successful organisation should have multiple layers of security in place to protect:
 - Operations
 - Physical Infrastructure
 - People
 - Functions
 - Communications
 - Information

Key Information Security terms & concepts (1)



Key Information Security terms & concepts (2)



Key Information Security terms & concepts (3)



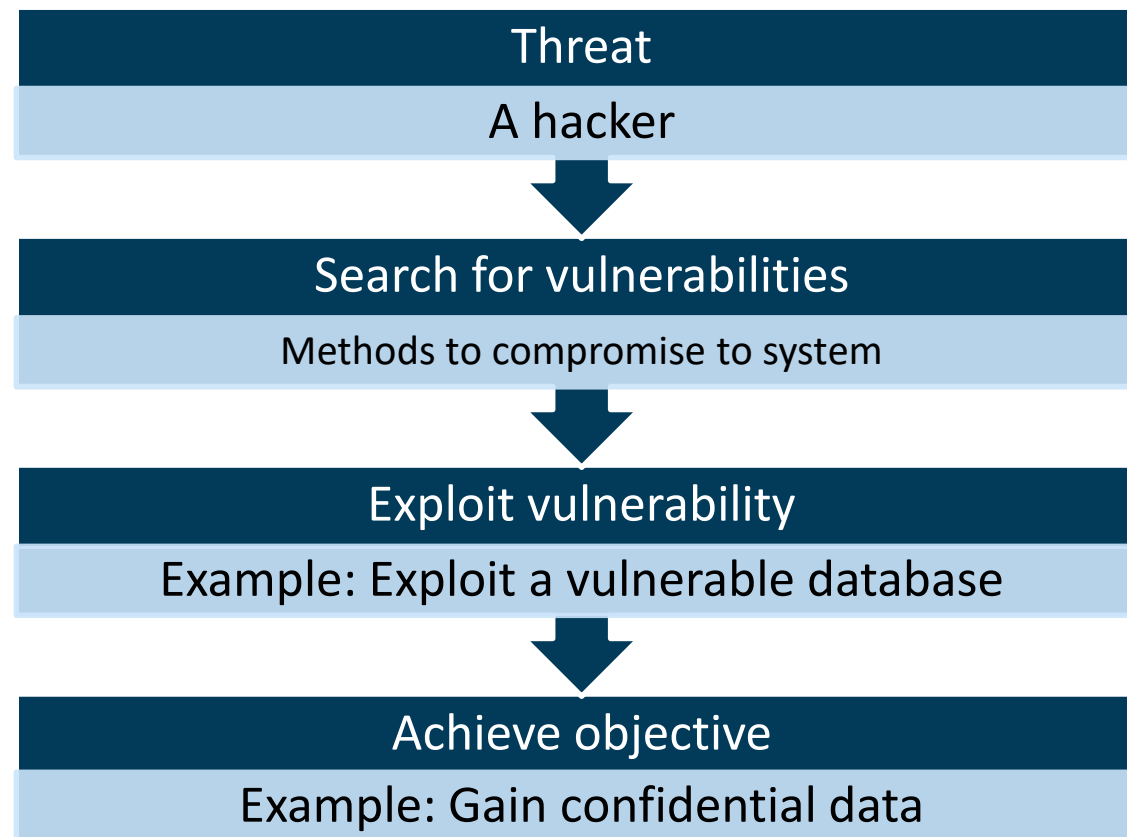
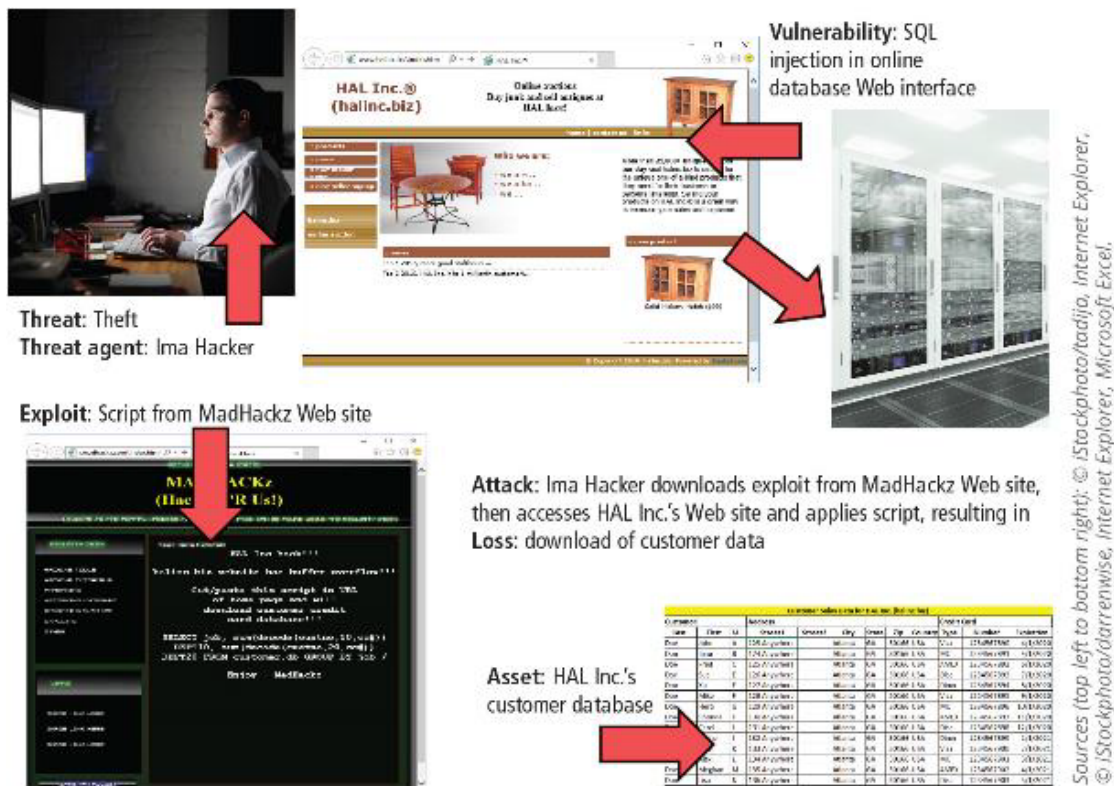
Subjects and objects—a computer can be either an agent entity used to conduct an attack or the target entity.

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



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:

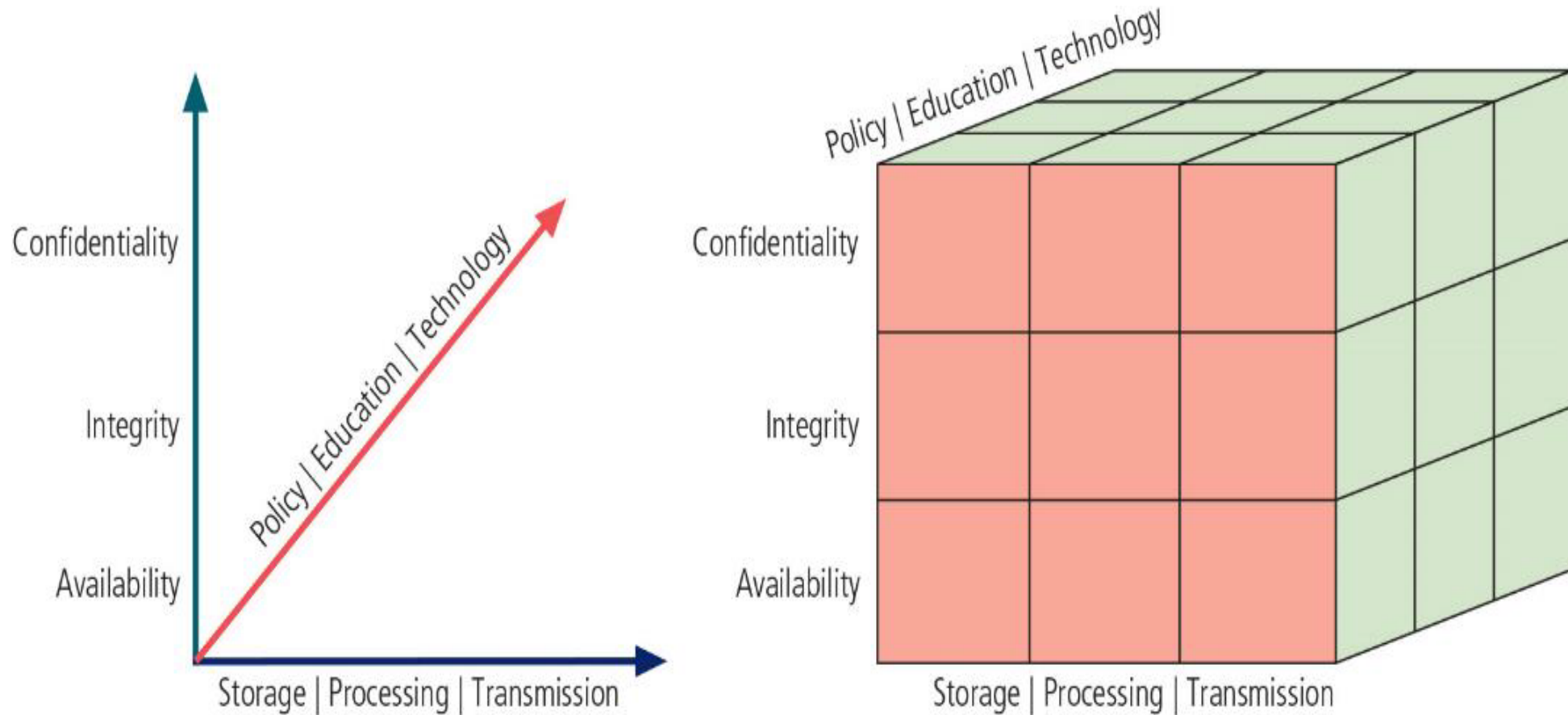
Ownership or control of information

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.

CNSS Security Model



Components of an Information System

- An information system (IS) is the entire set of hardware, software data, people, procedures, and networks that enable a business to use information.
- All of them work together to support personal and professional operations.
- Each one has its own strengths and weaknesses, as well as its own characteristics and uses.
- Each one has its own security requirements.

Balancing Information Security and Access

- It is impossible to obtain perfect information security—it is a process, not a goal.
- Security should be considered a balance between protection and availability.
- To achieve balance, the level of security must allow reasonable access, yet protect against threats.

Approaches to Information Security

Implementation: Bottom-Up Approach

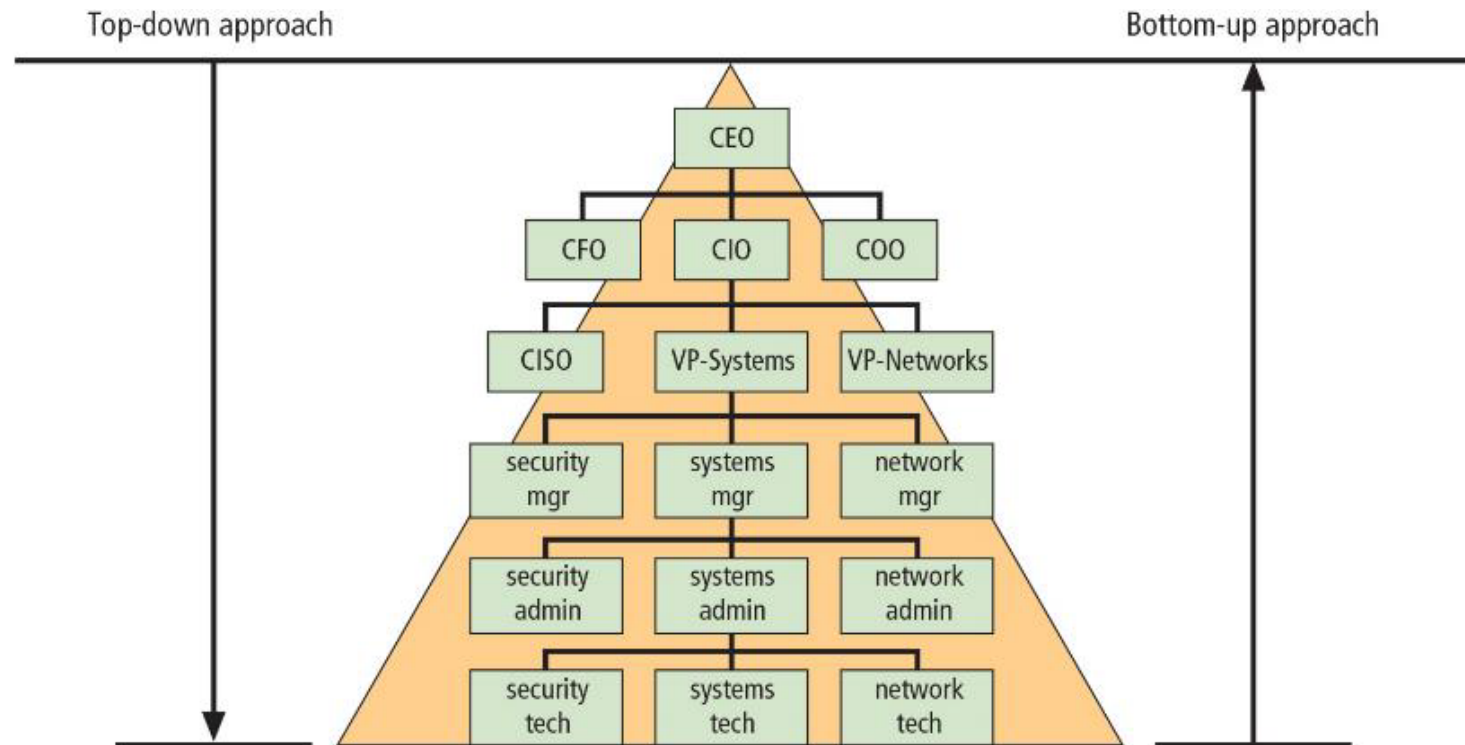
- Grassroots effort: systems administrators work to improve security of their systems.
- Key advantage: technical expertise of individual administrators
- Seldom works, as it lacks a number of critical features:
 - Participant support
 - Organisational staying power

Approaches to Information Security

Implementation: Top-Down Approach

- Initiated by upper management
 - Issue policy, procedures, and processes
 - Dictate goals and expected outcomes of project
 - Determine accountability for each required action
- The most successful type of top-down approach also involves a formal development strategy referred to as a systems development life cycle.

Approaches to Information Security Implementation

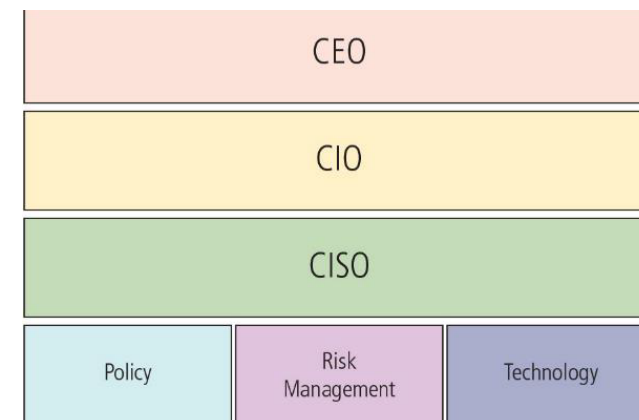


Security Professionals and the Organisation

- A wide range of professionals are required to support a diverse information security program.
- Senior management support is the key component.
- Additional administrative support and technical expertise are required to implement details of an IS program.

Senior Management

- Chief Executive office (CEO)
 - Focuses on the Strategic Leadership and Business Growth
 - Has ultimate accountability for the organisation, including its cybersecurity posture.
- Chief information officer (CIO)
 - The most senior technology officer
 - Primarily responsible for advising the senior executives on strategic planning that affects the management of information in the organisation
 - Works closely with the CISO to implement cybersecurity technologies and practices.
- Chief information security officer (CISO)
 - Responsible for protecting the organisation's information systems and data from threats.
 - Usually reports directly to the CIO



Information Security Project Team

- A small functional team of people who are experienced in one or multiple facets of required technical and nontechnical areas:
 - Champion
 - Team leader
 - Security policy developers
 - Risk assessment specialists
 - Security professionals
 - Systems administrators
 - End users

Data Responsibilities

- Data owners: senior management responsible for the security and use of a particular set of information
- Data custodian: responsible for information and systems that process, transmit, and store it
- Data trustees: appointed by data owners to oversee the management of a particular set of information and to coordinate with data custodians for its storage, protection, and use
- Data users: have access to information and thus an information security role

Communities of Interest

- Group of individuals united by similar interests/values within an organisation
 - Information security management and professionals
 - Information technology management and professionals
 - Organisational management and professionals

Information Security: Is It an Art or a Science?

- Implementation of information security is often described as a combination of art and science.
- “Security artisan” idea: based on the way individuals perceive system technologists and their abilities
- Security as art: no hard and fast rules nor many universally accepted complete solutions; no manual for implementing security through entire system
- Security as science: technology is developed by scientists and engineers; specific conditions cause virtually all actions in computer systems; almost every security issue is a result of the interaction of specific hardware and software; with sufficient time, developers could resolve all faults.

Security as a Social Science

- Social science examines the behaviour of individuals interacting with systems.
- Security begins and ends with the people that interact with the system, intentionally or otherwise.
- Security administrators can greatly reduce the levels of risk caused by end users and create more acceptable and supportable security profiles.

Summary (1 of 4)

- Information security evolved from the early field of computer security.
- Security is protection from danger. There are many types of security: physical security, personal security, operations security, communications security, national security, and network security, to name a few.
- Information security is the protection of information assets that use, store, or transmit information through the application of policy, education, and technology.
- The critical characteristics of information, including confidentiality, integrity, and availability (the C.I.A. triad), must be protected at all times. This protection is implemented by multiple measures that include policies, education, training and awareness, and technology.

Summary (2 of 4)

- Information systems are made up of the major components of hardware, software, data, people, procedures, and networks.
- Upper management drives the top-down approach to security implementation, in contrast with the bottom-up approach or grassroots effort, in which individuals choose security implementation strategies.

Summary (3 of 4)

- The control and use of data in the organisation is accomplished by the following parties:
 - Data owners, who are responsible for the security and use of a particular set of information
 - Data custodians, who are responsible for the storage, maintenance, and protection of the information
 - Data trustees, who are appointed by data owners to oversee the management of a particular set of information and to coordinate with data custodians for its storage, protection, and use
 - Data users, who work with the information to perform their daily jobs and support the mission of the organisation

Summary (4 of 4)

- Each organisation has a culture in which communities of interest are united by similar values and share common objectives. The three communities in information security are general management, IT management, and information security management.
- Information security has been described as both an art and a science, and it comprises many aspects of social science as well.

Questions to think of for the tutorial!

- What is information security?
- How has the concept of security for the use of computer systems changed over time?
- Information has many characteristics. What are the most critical of these characteristics that need to be kept secure?

References

- Slides are devised from the recommended books:
 - Michael E. Whitman and Herbert J. Mattord, Principles of Information Security, 7th Edition.



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