UNIVERSITY of GREENWICH

# COMP1806: Information Security

Part a: Introduction to COMP1806
Part b: Fundamentals of Information Security

**Dr Sakshyam Panda**
Lecturer
Center for Sustainable Cyber Security (CS2)
s.panda@greenwich.ac.uk

# Module structure and rationale

- Module leader: Sakshyam Panda
- Lecturers: Sakshyam Panda

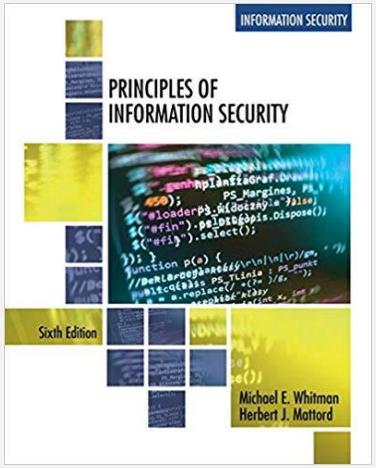
- Lectures: 11 topics in 11 weeks x 1 hrs per week
  - Pre-recorded lectures (made available at least 3 days prior to tutorials)
- Tutorials: 11 topics in 11 weeks x 2 hrs per week
  - Aim: Deeper theoretical understanding of the module content
  - Where: On campus (check your timetable)

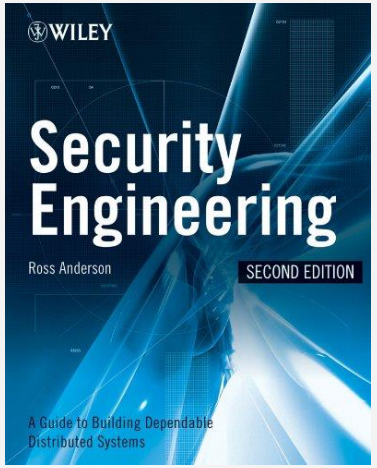
# Module guide

- Slides provide an outline
  - Prepare questions for your lecturers
  - On going to-do: “security-related news monitoring”
    - https://www.theregister.co.uk/security/
    - https://www.hackmageddon.com
    - https://www.securityweek.com/
    - https://krebsonsecurity.com/
    - https://secureframe.com/
- Use the Internet!
  - Google and Wikipedia
    - Treat their results carefully – confirm with primary and authoritative sources

# Reading List

- Background textbooks
  - 6th edition of Whitman, M. E., & Mattord, H. J. (2017). **Principles of information security**. Cengage Learning, ISBN-13: 978-1337102063 (**Most recommended**)
  - Latest edition of Anderson, R. (2018), **Security engineering**. John Wiley & Sons, ISBN-13: 978-0470068526
- High impact factor Scientific journals and magazines
  - IEEE Security & Privacy Magazine
  - Computers & Security Journal (Elsevier)
  - IEEE Transactions on Dependable and Secure Computing
  - IEEE Transactions on Information Forensics and Security
  - ACM Transactions on Privacy and Security
- Industry white papers, reports and products



# Module assessment

- Coursework - 60% weighting
  - Outline Details - The final output is a report to critically discuss a **research and technical topic inspired by the module content**. Carried out in teams of:
    - 5 or 6,
    - Or individually


- Quiz/Exam- 40% weighting
  - Multiple-choice exam, 20 questions - 1 hour

# Key Dates

- Coursework - 60% weighting
  - Release date: 10 Oct 2025, 09:00 BST
  - Submission deadline: 12 Nov 2025, 17:00 BST
- Quiz/Exam- 40% weighting
  - During tutorials

# Indicative lectures (L)

| Week | Date | Lecture |
|---|---|---|
| 1 | 26/09/2025 | Introduction to Information Security |
| 2 | 03/10/2025 | Attacks, Threats and Impact |
| 3 | 10/10/2025 | Security and Privacy for Machine Learning |
| 4 | 17/10/2025 | Risk Assessment |
| 5 | 24/10/2025 | Designing Secure Systems |
| 6 | 31/10/2025 | Defences, Controls, Planning, and Investment |
| **7** | **07/11/2025** | **Skills/PDP Week** |
| 8 | 14/11/2025 | Legal, ethical, and privacy issues |
| 9 | 21/11/2025 | Latest from Industry and Research (**Guest Speaker**) |
| 10 | 28/11/2025 | Introduction to Cryptography |
| 11 | 07/12/2025 | Applications of Cryptography |
| 12 | 12/12/2025 | Summary of all weeks |

# Cyber – a global concern

- Need for cyber
- Organisations
- Domestic life (our houses)
  - Work from home


# Learning Objectives of Lecture 1

UNIVERSITY of GREENWICH

- Motivate the need for information security
- Briefly discuss history of information security
- Learn some fundamental terms of information security
- Learn the high-level approaches to information security implementation

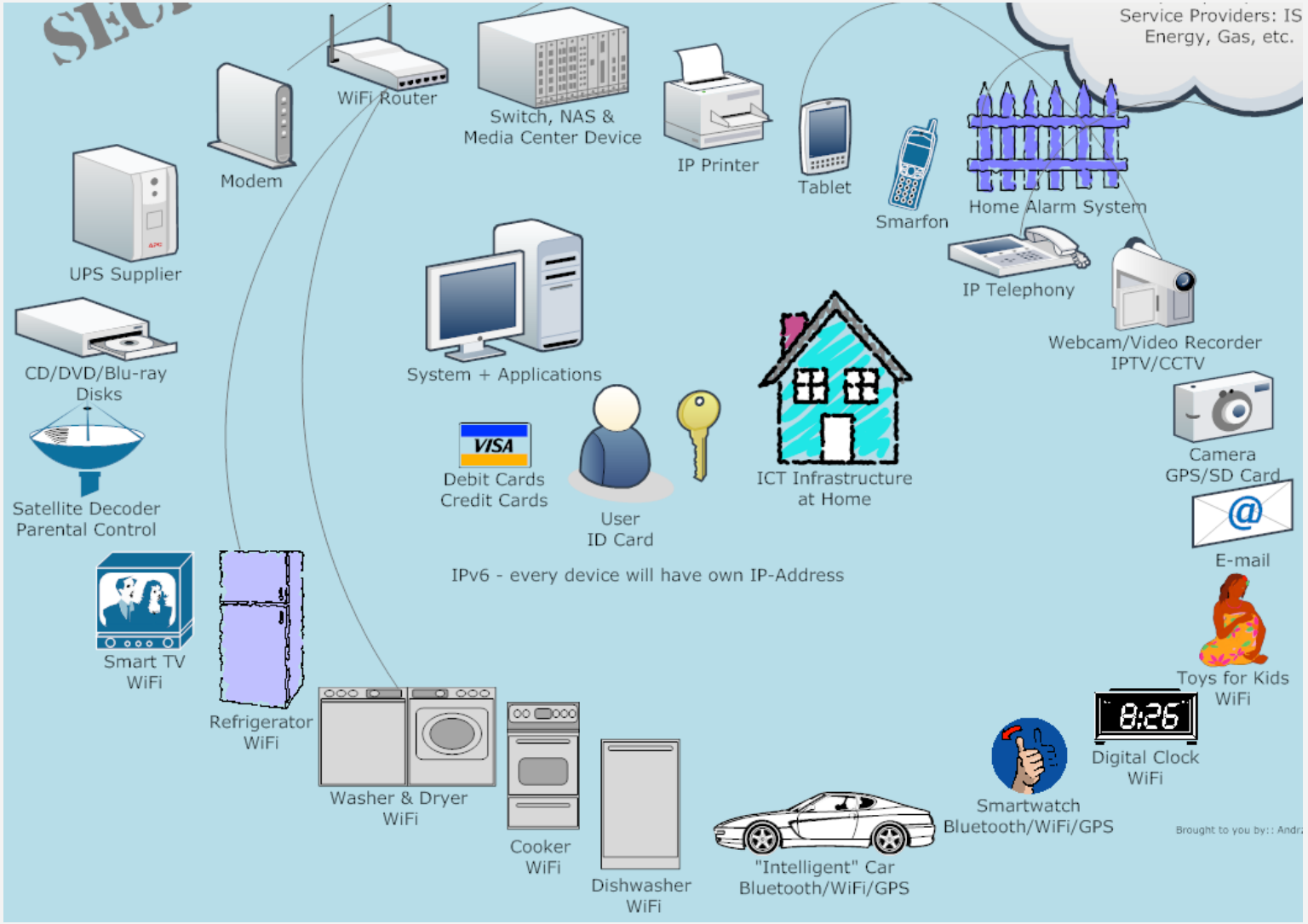
UNIVERSITY of GREENWICH

# Motivation

# Motivation

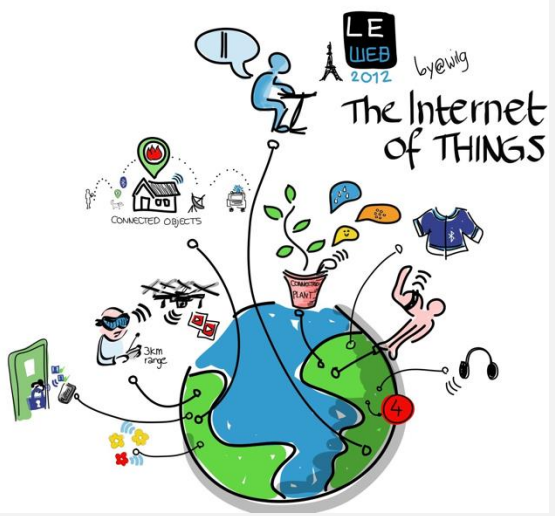
- What is the **mission** of cyber security?
  - To prevent **unauthorised** parties from **accessing**, **deleting** or **modifying** our digital data – and not only…
- Why do we **need** cyber security?
  - We are all concerned
  - Cyber crime can be very **expensive**
    - can seriously affect the functioning of businesses/economies
    - can have life threatening (safety) implications
- What are typical **dangers** in cyber security?
  - Malware
  - Hacking into web sites, databases, systems
  - Stealing passwords
  - Identity theft
  - Denial-of-Service (DoS) Attacks


# Interconnected world

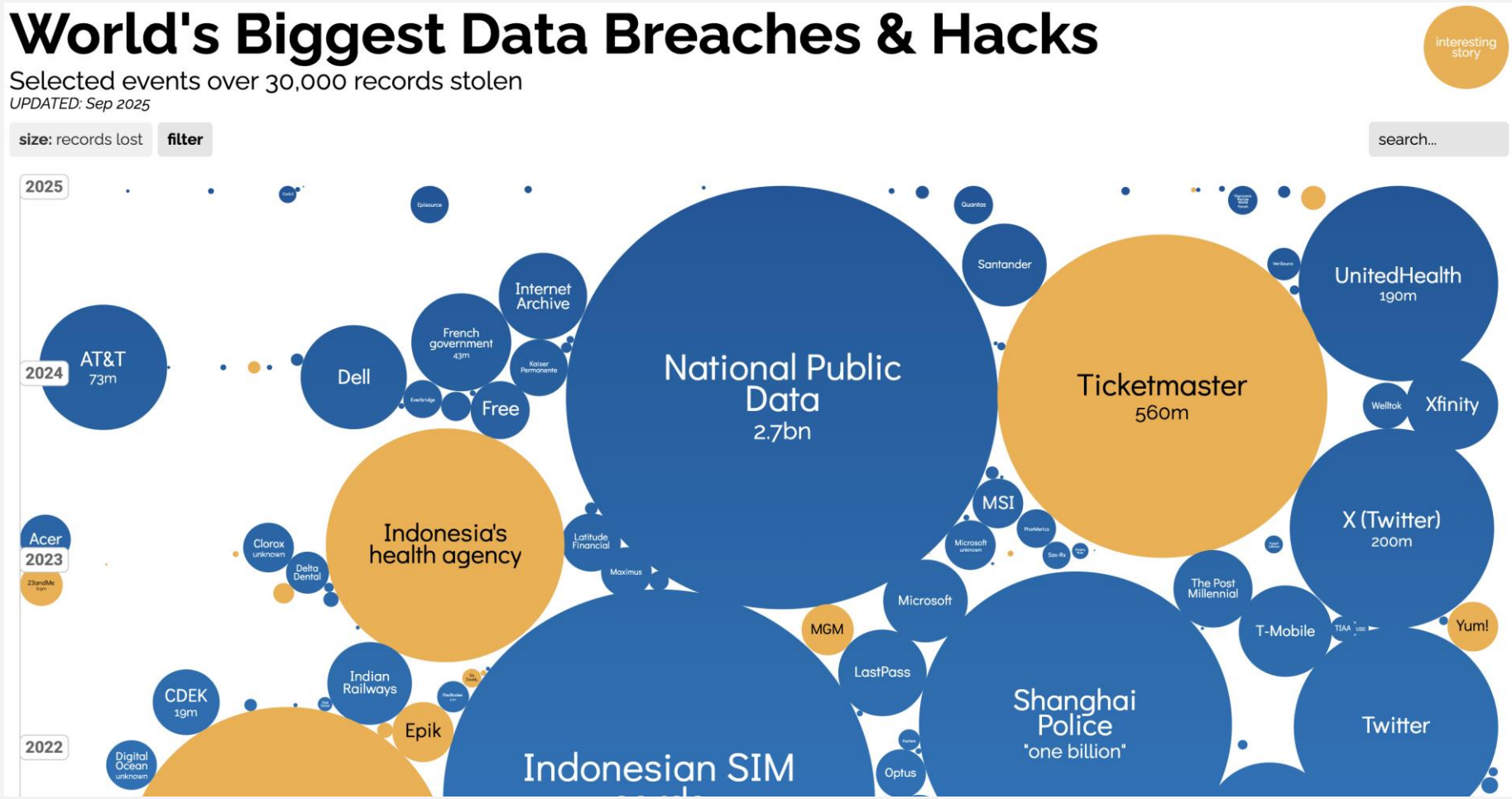


# Cyber security…

- Billions of devices → a cyber attack can be launched from anywhere → very large **attack surface**
  - e.g. IoT, interconnected cars, 5G, healthcare, smart grid
- Attacks to be launched by threat actors to exploit vulnerabilities
  - System, network and software vulnerabilities
  - The use of Artificial Intelligence (AI) introduces new vulnerabilities
- Defender → countermeasures to prevent being hacked
- Countermeasures cost and not only..
  - Obstacle of legacy systems




# It's real




https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

# Question

Which of the following best describes the primary goal of information security?

A. To ensure that only authorized users can access information
B. To prevent all cyberattacks from occurring
C. To maintain the confidentiality, integrity, and availability of information
D. To monitor all user activities within a system

# Question

Which of the following best describes the primary goal of information security?

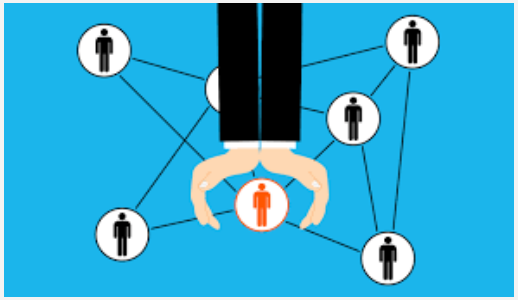
A. To ensure that only authorized users can access information
B. To prevent all cyberattacks from occurring
C. To maintain the confidentiality, integrity, and availability of information
D. To monitor all user activities within a system

UNIVERSITY of GREENWICH

# Definitions

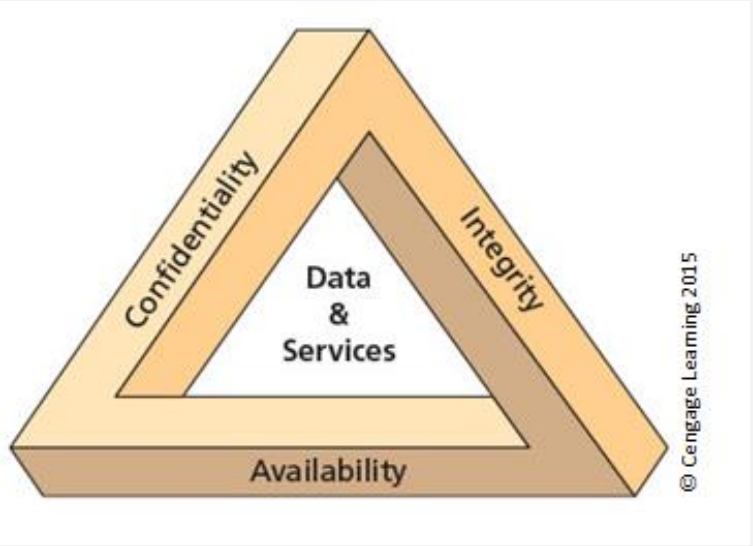
# What is security?

- Security means to be protected from adversaries, from those who would do harm, intentionally or otherwise
  - **State** of being secure and free from danger or harm
  - The **actions** taken to make someone or something secure
- The protection of **information** and its **critical elements**, including systems and hardware that use, store, and transmit that information (CNSS)
- Includes:
  - Information security management
  - Data security
  - Network security



# What is security? (cont…)

- A successful organisation should have multiple layers of security in place to protect major components of an Information system:
  - Software
  - Hardware
  - People
  - Procedures
  - Data
  - Network



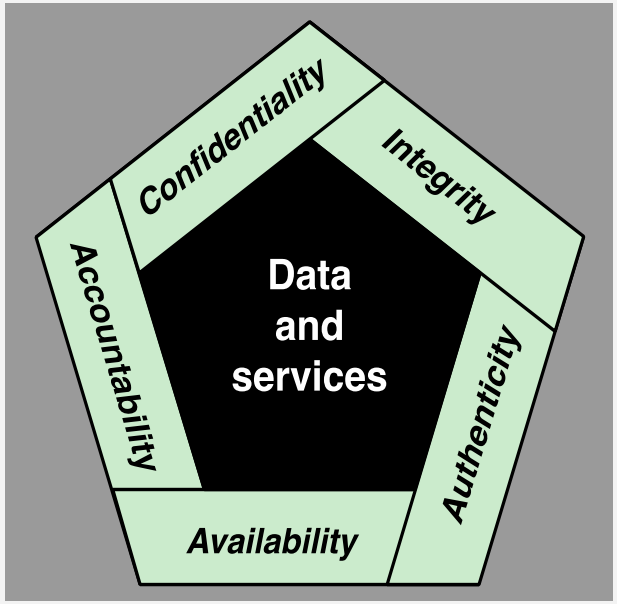

- **C.I.A. triad**
  - Is a **standard** based on confidentiality, integrity, and availability
    - has been considered the industry standard for computer security since the development of the mainframe
  - expanded model consists of a list of **critical characteristics of information**

# Protection

- Information security management, controls to protect:
  - **Confidentiality (C)**
    - Information has confidentiality when it is protected from disclosure or exposure to unauthorized individuals or systems
  - **Integrity (I)**
    - Information has integrity when it is whole, complete, and uncorrupted
  - **Availability (A)**
    - Enables authorized users—persons or computer systems—to access information without interference or obstruction and to receive it in the required format
- Data security: protecting digital data
- Network security: prevent and monitor for malicious intrusions
  - Unauthorised access
  - Misuse
  - Modification
  - Denial of resources

# Beyond CIA

- Additional principles
  - **Authenticity**
    - The property of being genuine and being able to be verified and trusted
  - **Accountability**
    - requirement for actions of an entity to be traced uniquely to that entity



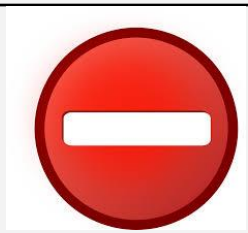
# Computer security challenges

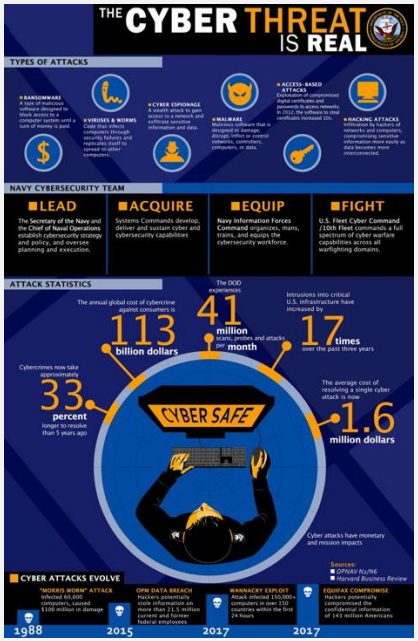
UNIVERSITY of GREENWICH

1. Computer security is not as simple as it might first appear to the novice
2. In developing a particular security mechanism or algorithm, one must always consider potential attacks on those security features
3. Procedures used to provide services are often counterintuitive
4. Physical and logical placement needs to be determined
5. Security mechanisms typically involve more than a particular algorithm or protocol and also require that participants be in possession of some secret information which raises questions about the creation, distribution, and protection of that secret information
6. Attackers only need to find a single weakness, while the designer must find and eliminate all weaknesses to achieve perfect security
7. Security is still too often an afterthought to be incorporated into a system after the design is complete, rather than being an integral part of the design process
8. Security requires regular and constant monitoring
9. There is a natural tendency on the part of users and system managers to perceive little benefit from security investment until a security failure occurs
10. Many users and even security administrators view strong security as an impediment to efficient and user-friendly operation of an information system or use of information

# Key Information Security Concepts (1/3)

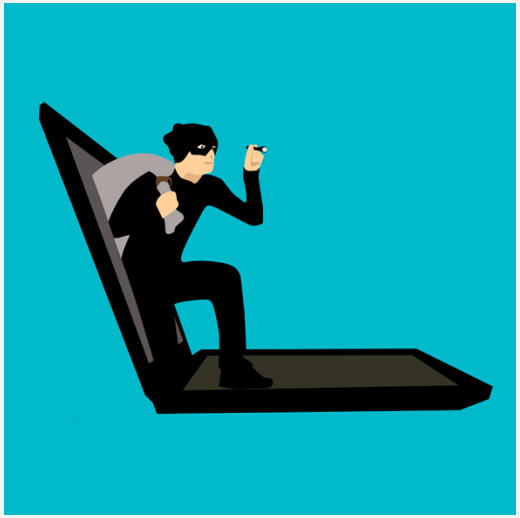
- **Access**: ability to use, manipulate, modify, or affect another subject or object
- **Asset**: protected resource
- **Attack**: an intentional or unintentional act that can damage or otherwise compromise information and systems
- **Control, safeguard, or countermeasure**: Security mechanisms, policies, or procedures that can successfully counter attacks
- **Exploit**: a technique used to compromise a system



# Key Information Security Concepts (2/3)

- **Exposure**: a condition or state of being exposed
- **Loss**: A single instance of an information asset suffering some damage or destruction (impact)
- **Protection profile or security posture**: entire set of controls and safeguards that the organisation implements to protect the asset
- **Risk**: expected impact of an unwanted occurrence
- **Threat**: any event or circumstance that has the potential to adversely affect operations and assets
- **Threat Agent**: the specific instance or a component of a threat

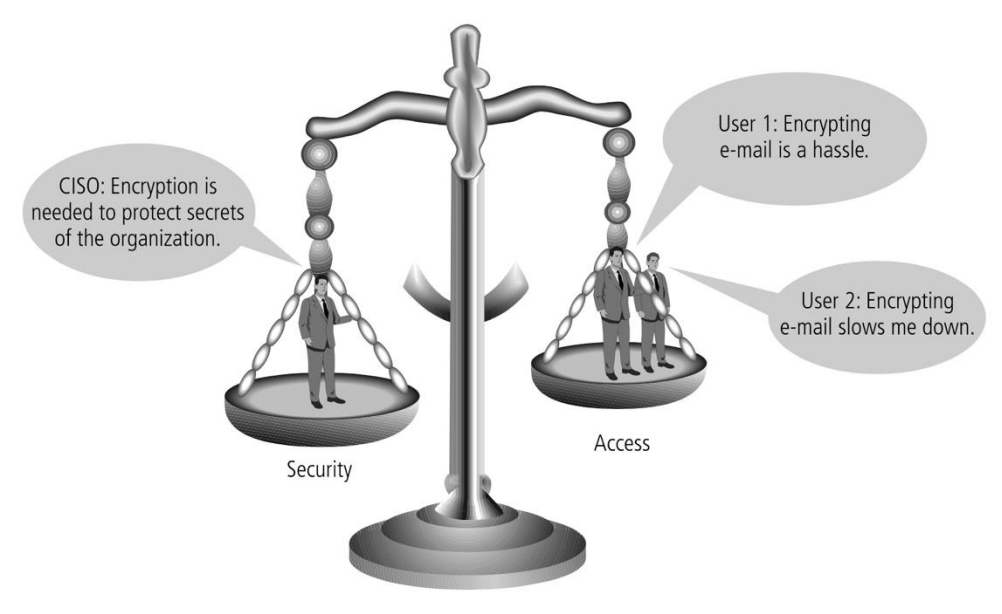



# Key Information Security Concepts (3/3)

- **Threat event**: an occurrence of an event caused by a threat agent
- **Vulnerability**: weaknesses or faults in a system or protection mechanism that expose information to attack or damage
- A computer can be the subject (attacker) of an attack and/or the object (target) of an attack:
  - When it is the subject of an attack, the computer is used as an active tool to conduct attack
  - When it is the object of an attack, the computer is the entity being attacked

# Balancing Information Security and Access

- Impossible to obtain perfect information security
  - Security is not an absolute → 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



UNIVERSITY of GREENWICH

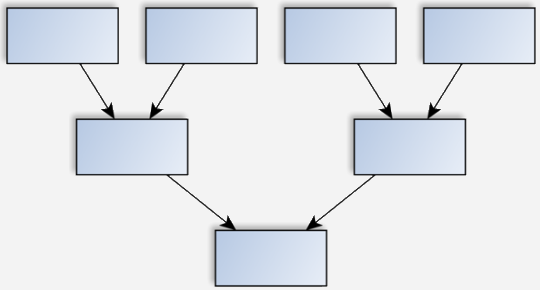
# Implementation of Information Security

# Approaches to Information Security Implementation: Bottom-Up Approach

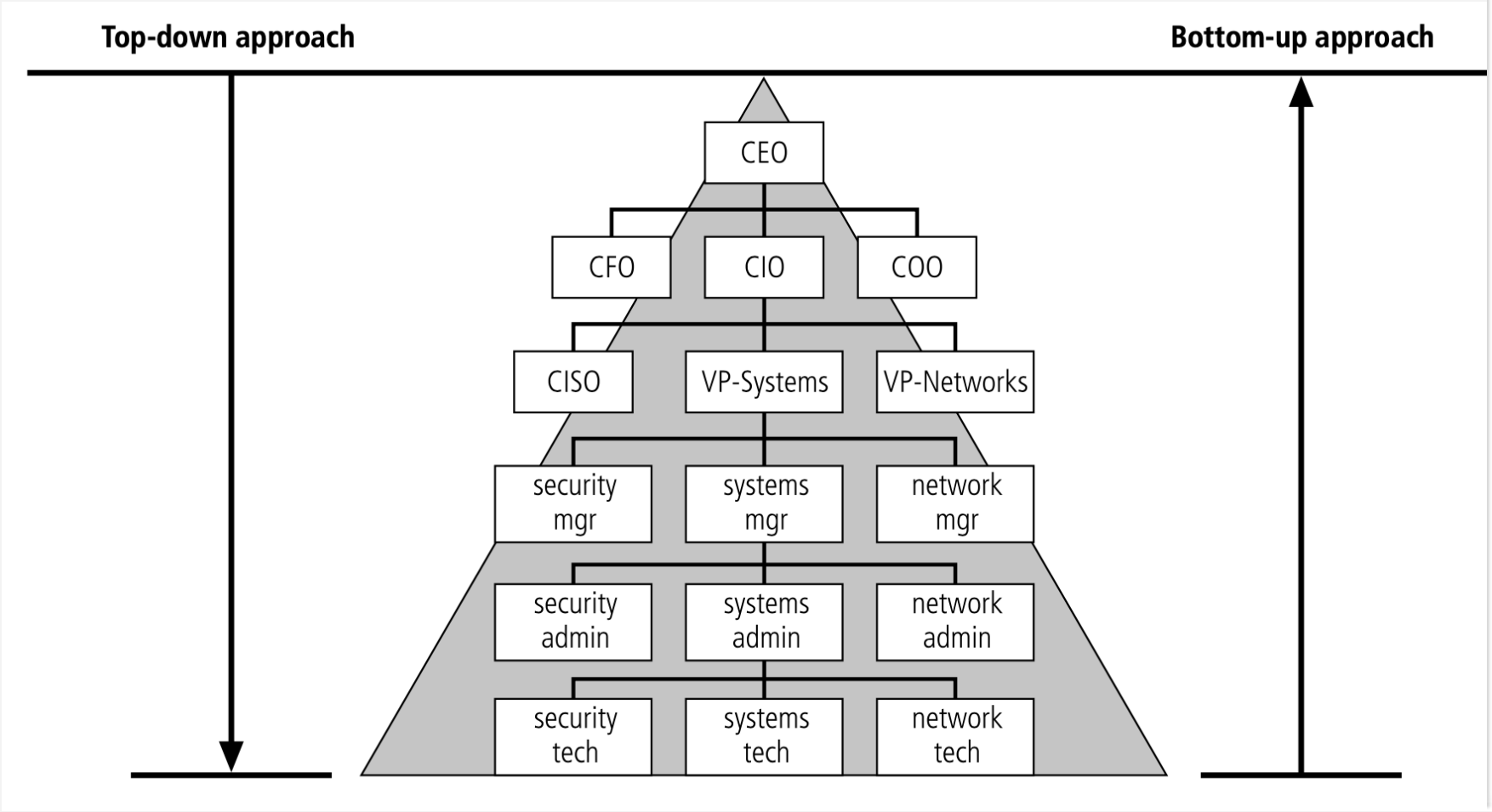
- Systems administrators attempt to improve security of their systems → **Bottom-Up Approach**
- Key advantage: technical expertise of individual administrators
- It lacks several critical features:
  - Participant support
  - Organisational staying power
- An alternative approach, which has a higher probability of success, is called the **top-down** approach

# Approaches to Information Security Implementation: Top-Down Approach

- Initiated by **upper management**
  - Issue policy, procedures, and processes
  - Dictate goals and expected outcomes
  - Determine who is countable for each of the required actions
- It has
  - strong upper-management **support**
  - a dedicated **champion**
  - dedicated **funding**
  - clear **planning**, and
  - the opportunity to influence organisational **culture**
- Also involves a formal development strategy referred to as a **systems development life cycle (SDLC)**



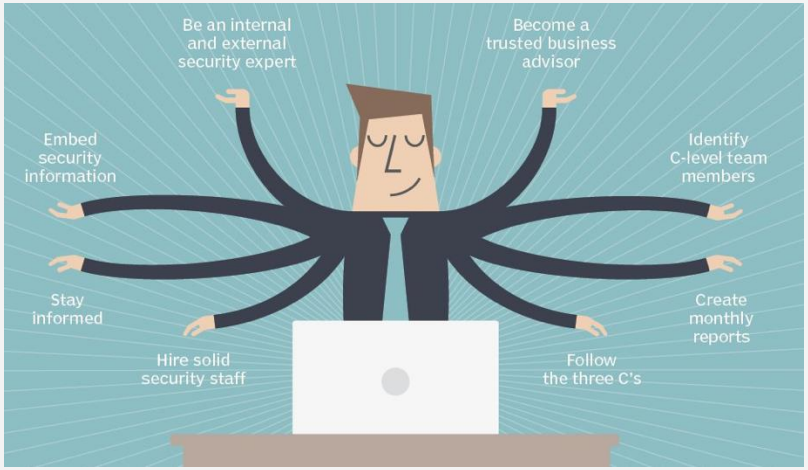
# Approaches to Information Security Implementation



# Security Professionals and the Organisation

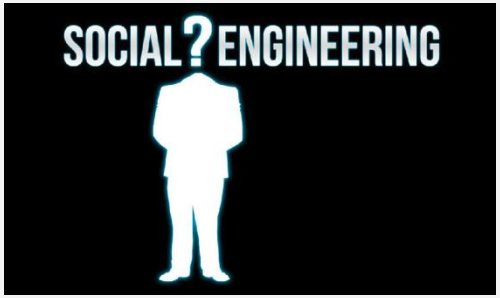
UNIVERSITY of GREENWICH

- It takes a wide range of professionals to support a diverse information security program
- Chief information officer (CIO)
  - Senior technology officer
  - Primarily responsible for advising the senior executives on strategic planning
- Chief information security officer (CISO)
  - Has primary responsibility for **assessment, management**, and **implementation** of IS in the organisation
  - Usually reports directly to the CIO



# Security as a Social Science

- Security begins and ends with the people that interact with the system, intentionally or otherwise
- Social science examines the behaviour of individuals interacting with systems
- End users that need the very information the security personnel are trying to protect may be the **weakest link** in the security chain
- Security administrators can greatly reduce the levels of risk caused by end users and create more acceptable and supportable security profiles



# References


- 6th edition of Whitman, M. E., & Mattord, H. J. (2017). Principles of information security. Cengage Learning.
- Stallings, W. and Brown, L., 2017. Computer Security: Principles and Practice, Global Edition.
- Images sources (labeled to be reused): https://images.google.com

UNIVERSITY of GREENWICH

# Thank You!

# Any Questions?