Cardiff University
Prifysgol Caerdydd

# CMT116 Cyber Security & Risk Management

Amir Javed

# Module Structure

- Coursework 70%
  - Apply theoretical material and risk methodologies learnt to a specific case study.
  - Students will be required to identify, analyse, evaluate and manage risk to different components of an information system.
  - Identify and articulate different types of threat to, and vulnerabilities of, information systems to a range of audiences.
  - Submit a written report on their finding.
- Exam 30%
  - A computerized test that will assess students' understanding of key cyber security and risks concepts, principles, as well as their knowledge of common security frameworks, standards and regulations, risk assessment and threat modelling methodologies

# Learning Outcomes

- Determine, establish and maintain appropriate information security governance within an organisation.
- Identify, analyse, evaluate and manage risks related to different components of an information system (i.e. data, people, processes, hardware, software and network) accounting for current threat landscape
- Identify and effectively articulate different types of threat to, and vulnerabilities of, information systems to a range of audiences (e.g. top management, end users, non-technical and technical experts)
- Be aware of the wide range of security countermeasures, as well as select and justify appropriate security countermeasures to mitigate risks in an information system

# Learning Outcomes

- Apply popular risk assessment methodologies to a case studies (e.g. Octave Allegro, STRIDE, DREAD)
- Define and implement effective security policies and processes within an organisation
- Effectively use common information security management frameworks (e.g. ISO/IEC 27000, COBIT, NIST)
- Be aware of the current computer misuse, data protection, copyright and privacy legislation, as well as security ICT regulations and guidelines, including GDPR
- Evaluate and calculate return of security investments and economic impact of a security-related incident on business

# Bruce Schneier

- An American cryptographer, computer security professional, privacy specialist and writer. He is the author of several books on general security topics, computer security and cryptography.

# Why we need information security?

*Information is power, if you have information about the whole planet, you have power over the whole planet-* Jacob Appelbaum

What's the most precious thing in information security, for an individual and for a company ?

Its Data

how often do we share the information that we have been victim of a cyber attack ?

Is it in a companies best interest to share information that they have been breached?

# Data Breaches

- Only measured since around 2003 when disclosure laws came into effect.
- Thousands of breaches now reported allowing us to analyze trends, sources, motivations and methods.
- Sources come from hackers, malicious insiders, careless and untrained employees, thieves and poor disposal of equipment.
- So many terms used now (phishing, pharming, viruses, worms etc.), we need to define and understand them.

Example - British Airways is facing a record fine of £183m for last year's breach of its security systems. The data breach happened after users of British Airways' website were diverted to a fraudulent site.

# What has history shown us?

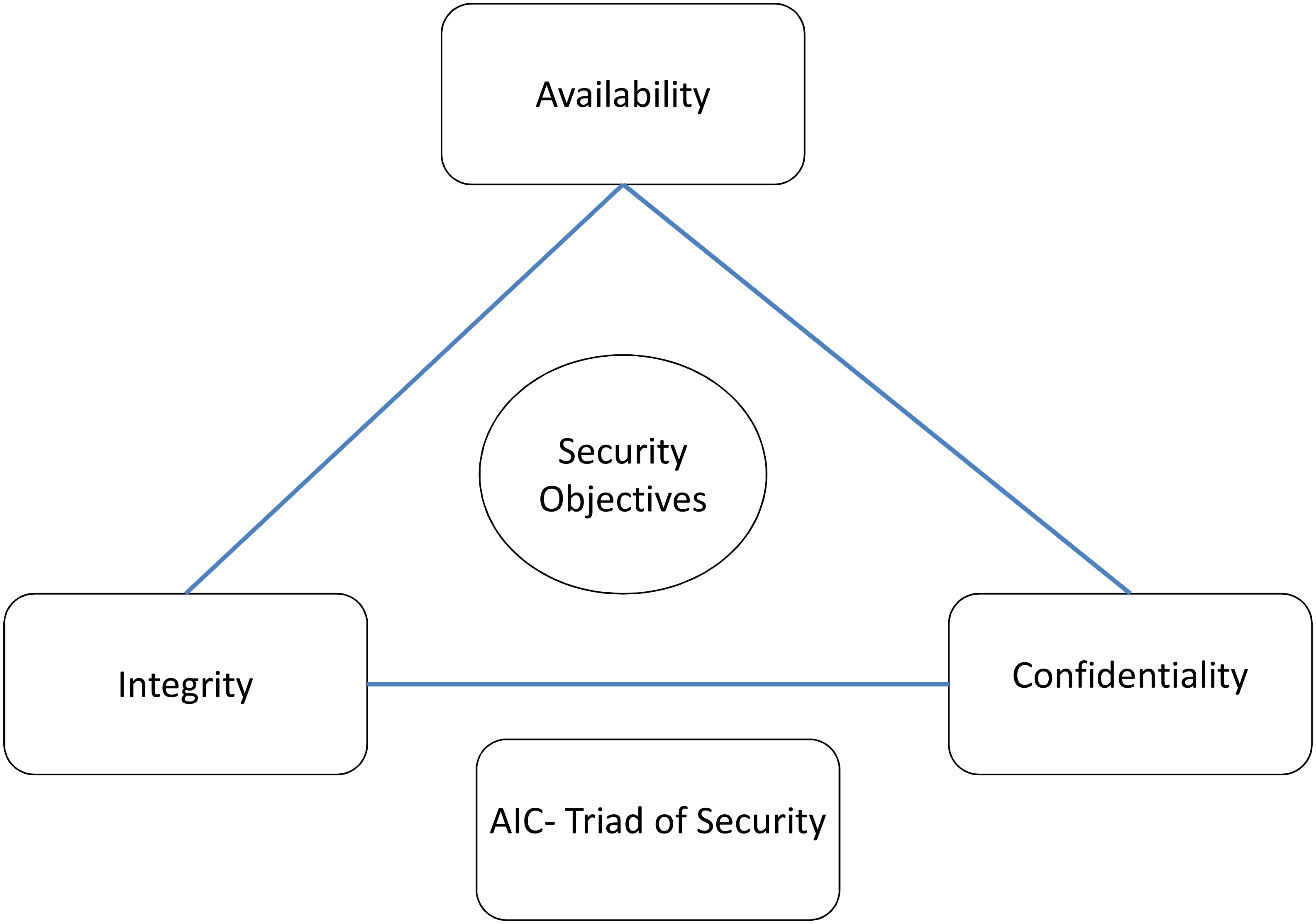
*”The good news is that we can predict the future by knowing we are bound to repeat the past.”*

Kevin Prince (IT security expert)

# Computer Networks

- Built in order to communicate and share information between different humans and computers
- Each computer knows only about what is stored in its own memory and takes streams of data from the network
- How do we know the difference between “good” and “bad” data?
- We have policy and technology
- The trick is getting the right mix of both
- Each system will be different

# Fundamental Principles of Security



Availability

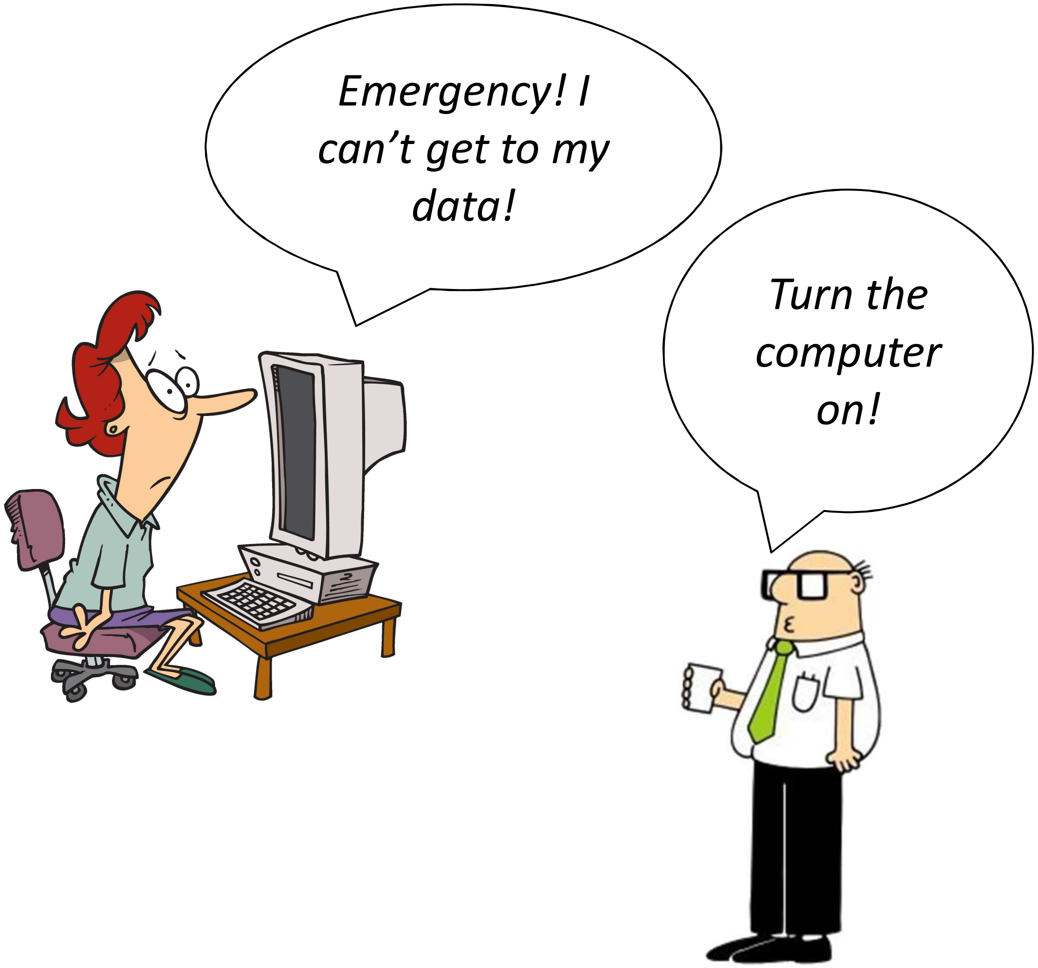
Security Objectives

Integrity

Confidentiality

AIC- Triad of Security

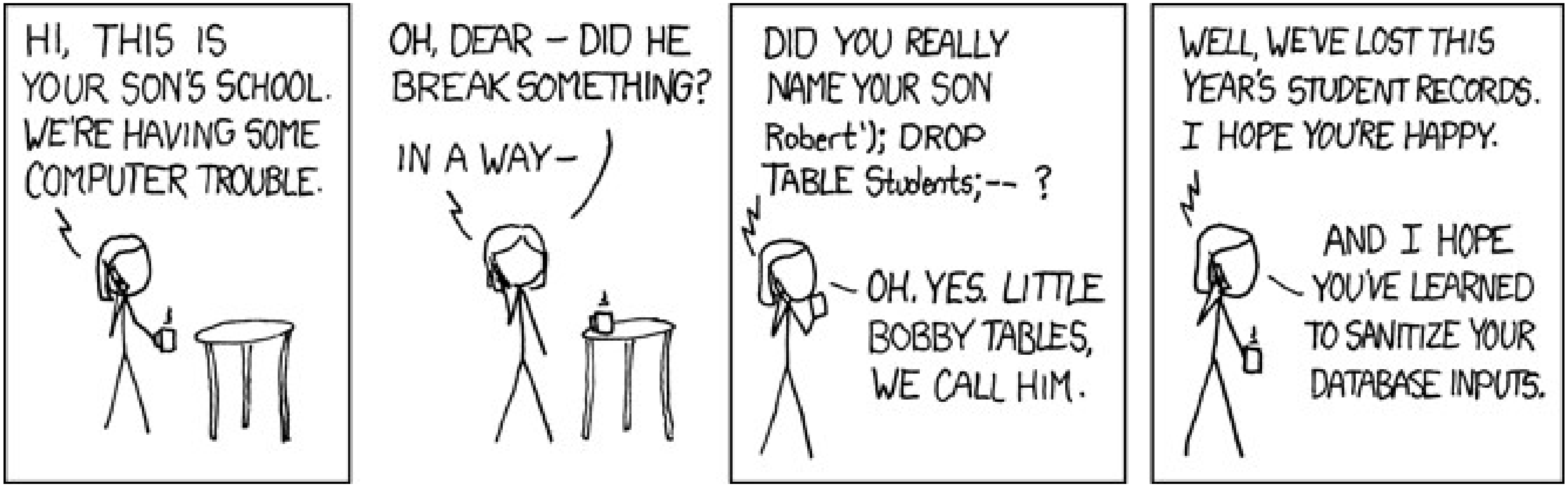
# AIC- Triad



**Availability :** Protection ensures reliability and timely access to data and resources to authorized individuals.

**List Cyber Attacks that could compromise Availability and one counter measure**

# AIC- Triad


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

**Integrity :** is upheld when the assurance of the accuracy and reliability of information and systems is provided and any unauthorized modification is prevented.

**List Cyber Attacks that could compromise Integrity and one counter measure**

# AIC- Triad

**Confidentiality**

- Ensures that the necessary level of secrecy is enforced at each junction of data processing and prevents unauthorized disclosure.
- This level of confidentiality should prevail while data resides on systems and devices within the network, as it is transmitted, and once it reaches its destination.

**List Cyber Attacks that could compromise Confidentiality and one counter measure**

# Controls to counter cyber attack

- Availability
  - Redundant array of inexpensive disks (RAID)
  - Clustering
  - Load balancing
  - Redundant data and power lines
  - Software and data backups
- Integrity
  - Hashing (data integrity)
  - Configuration management (system integrity)
  - Change control (process integrity)
- Confidentiality
  - Encryption for data at rest (whole disk, database encryption)
  - Encryption for data in transit (IPSec, SSL, PPTP, SSH)
  - Access control (physical and technical)

# Security Definition

I am vulnerable and see you as a threat.
Good ☺

**Key Security Terms**

1. *Vulnerability*
2. *Threat*
3. *Threat agent*
4. *Risk*
5. *Exposure*
6. *Control*

# Definitions

*Vulnerability*

is a lack of a countermeasure or a weakness in a countermeasure that is in place.

*In a security environment what all elements are vulnerable and can be exploited?*

- Software
- Hardware
- Humans
- Procedural

# Definitions

Threat

A ***threat*** is any potential danger that is associated with the exploitation of a vulnerability.

*From a company's perspective*

The threat is that someone, or something, will identify a specific vulnerability and use it against the company or individual.

Threat Agent

The entity that takes advantage of a vulnerability is referred to as a ***threat agent***

*Example* **:** An intruder accessing the network through a port on the firewall

# Definitions

Risk

A ***risk*** is the likelihood of a threat agent exploiting a vulnerability and the corresponding business impact.

Example : If an intrusion detection system (IDS) is not implemented on a network, there is a higher likelihood an attack will go unnoticed until it is too late.

*Can a company say they are 100% secure and risk free?*

Risk ties the vulnerability, threat, and likelihood of exploitation to the resulting business impact

# Definitions

*Exposure*

An ***exposure*** is an instance of being exposed to losses.

How ?

A vulnerability exposes an organization to possible damages.

Example  : If password management is lax and password rules are not enforced, the company is exposed to the possibility of having users' passwords captured and used in an unauthorized manner

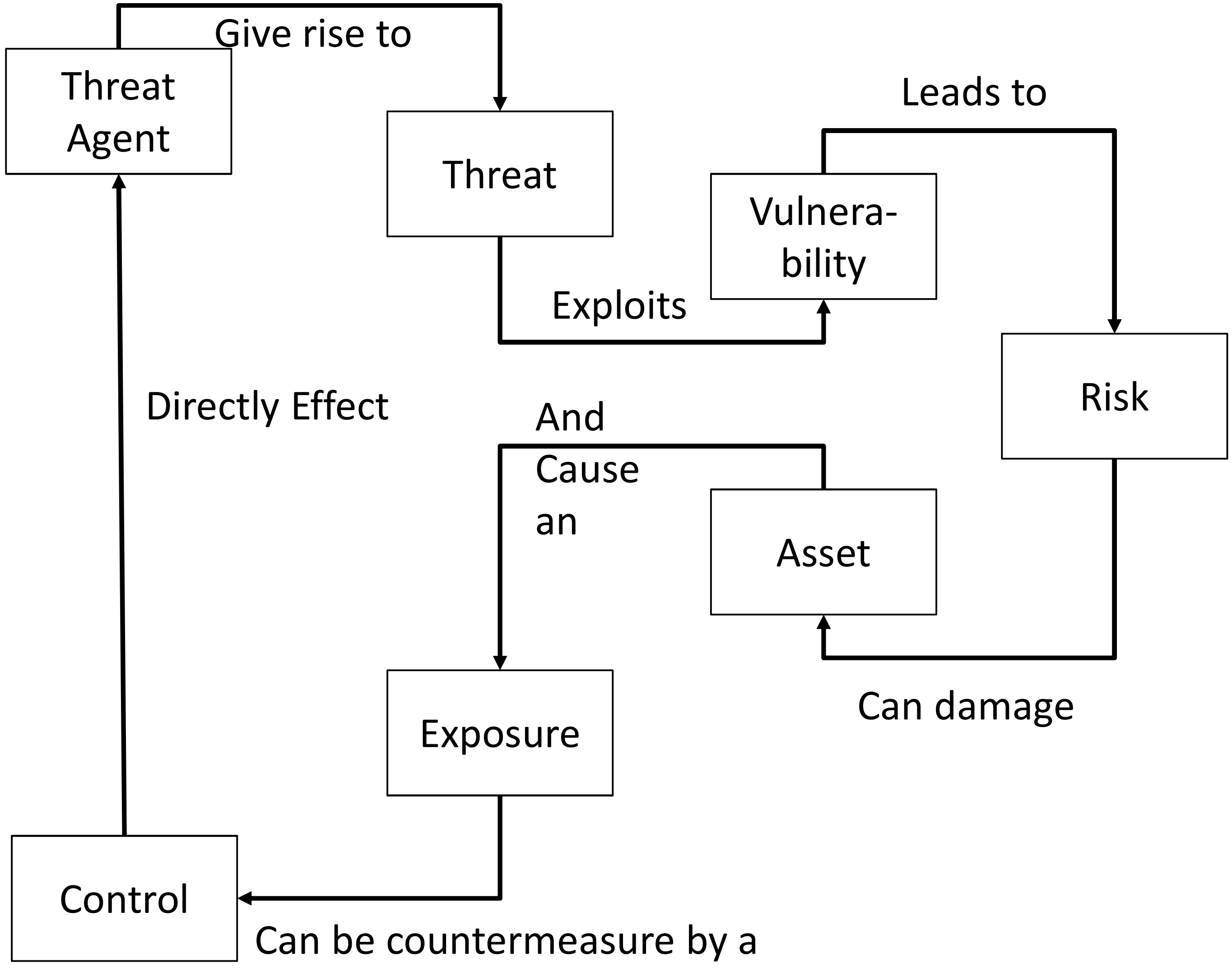
# Definitions

*Control*

- A ***control,*** or countermeasure, is put into place to mitigate (reduce) the potential risk.
- A countermeasure may be a software configuration, a hardware device, or a procedure that eliminates a vulnerability or that reduces the likelihood a threat agent will be able to exploit a vulnerability.

Example  of countermeasures include strong password management, firewalls, a security guard, access control mechanisms, encryption, and security-awareness training.

# Relationship Among Different Security Concepts


Threat Agent
Give rise to
Threat
Leads to
Vulnera-bility
Exploits
Risk
Directly Effect
And Cause an
Asset
Can damage
Exposure
Control
Can be countermeasure by a