ENTERPRISE CYBER SECURITY

CYBER SYSTEMS AND RISKS

University of Glasgow

OVERVIEW

- distinguishing between cyberspace, cyber physical systems, information security, cyber security and safety.
- understanding the differences and overlaps in each area.
- differentiating between malicious and non-malicious cyber-risks.

CYBER SPACE

The complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form

CYBER SPACE DEFINITION
ISO27032:2012

CYBER SPACE

- the Internet is a prominent example of a cyber space, but the two terms are not interchangeable.
- an alternative and more general definition of cyber space may lack the idea of being connected to the Internet.
- realistically, many systems are connected to the Internet.
- NSFNET and APRANET are examples of cyber spaces predating the Internet.

CYBER SPACE

- the European Union (EU), as well as the UK, effectively uses the term interchangeable with the Internet.

- the International Telecommunications Union (ITU) prefers the term ‘cyber environment’.

- the National Institute of Standards and Technology (NIST) emphasises cyber space within the context of critical infrastructures.

CYBER SYSTEM

CYBER SYSTEM

- in simple terms a cyber systems are dependent or make use of a cyber space.

- it is important to understand that this dependency is potentially a vulnerability.

- cyber-systems have become increasingly ubiquitous within societies and critical to modern economies.

- such systems are so important to modern life, that they are often referred to as **critical infrastructure**.

CYBER-PHYSICAL SYSTEM

CYBER-PHYSICAL SYSTEM (CPS)

- industry, increasingly academia as well, often focus and discuss cyber-physical systems.
- cyber-physical systems are specific cyber systems that control and react to the physical environment.
- such systems are common within industry (e.g. distributions of clothes, dispatching of goods etc).
- networked actuators and sensors are becoming increasingly relevant beyond industry (e.g. smart grids, autonomous vehicles).

CPS AND ADAPTION

- consider the research, systems could be constructed to adapt to a given context.
- resources could be tailored to the needs of the organisation.
- concerns become how are such resources allocated to individual employees.
- data sources may include calendar, messaging, performance on system etc.

SUGAR WATER WARS

CPS AND ADAPTION

- social and ethical questions arise from the development of such system.

- companies like Apple, are no different to Coca-Cola and Pepsi, they make sugar water and pour into different containers.

- potential for modern infrastructure is that the ‘volume of sugar water’ can be determined just in time.

- key concern is who is ‘mother’, who gets to decide the volume of sugar water and based on what evidence.

CYBER SECURITY

CYBER SECURITY

- cyber security is the defence of cyber systems from **cyber threats**.
- cyber threats can be thought of any threat that makes use of a cyber space.
- threats to systems can be considered malicious or non-malicious.
- cyber security is not so much defined by the **kind of asset**, but rather the **threat to that asset**.

INFORMATION SECURITY

- concerned with the protection of information assets.
- maintaining the **confidentiality**, **integrity** and **availability** of data.
- information is vulnerable from physical threats as well as cyber threats.

CYBER SECURITY AND INFORMATION SECURITY

- standards and guidelines often conflate cyber security and information security.

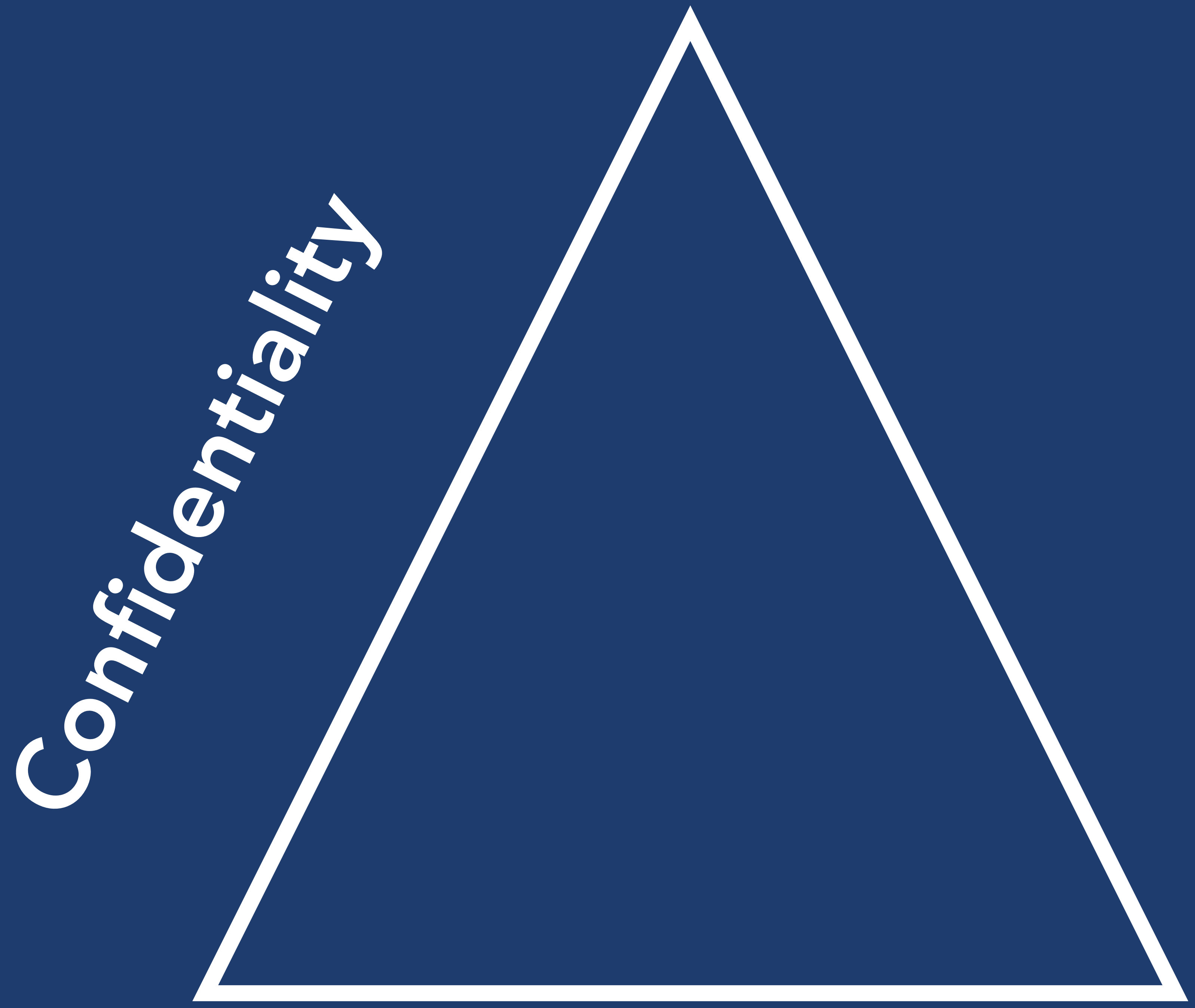
- cyber security as a topic goes **beyond** the defence of information from cyber threats.

- nevertheless, Information Security goes **beyond** cyber security as it concerned about more than threats emerging from cyber space.

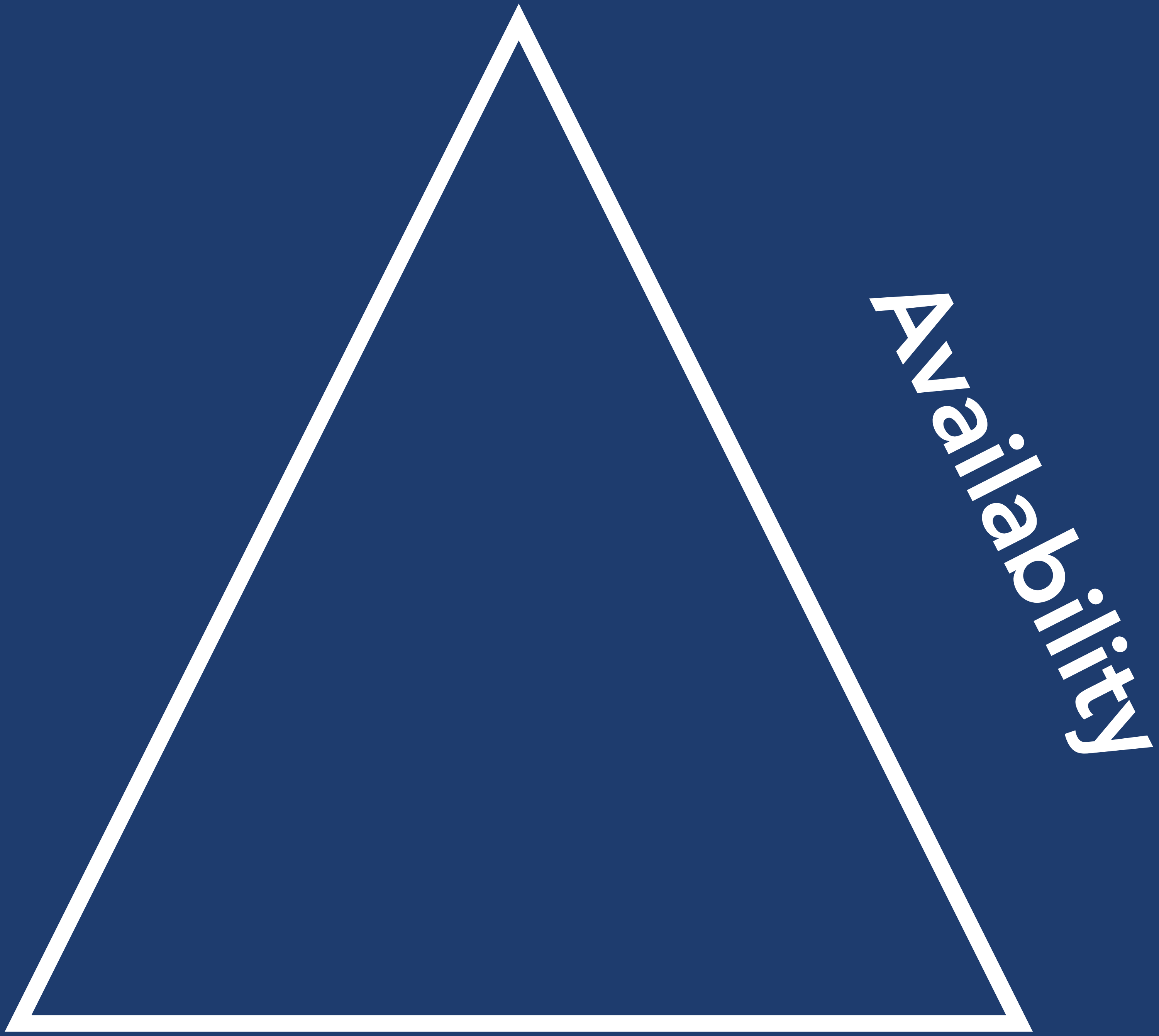
Preservation of confidentiality, integrity and availability of information.

INFORMATION SECURITY DEFINITION
ISO27000:2016

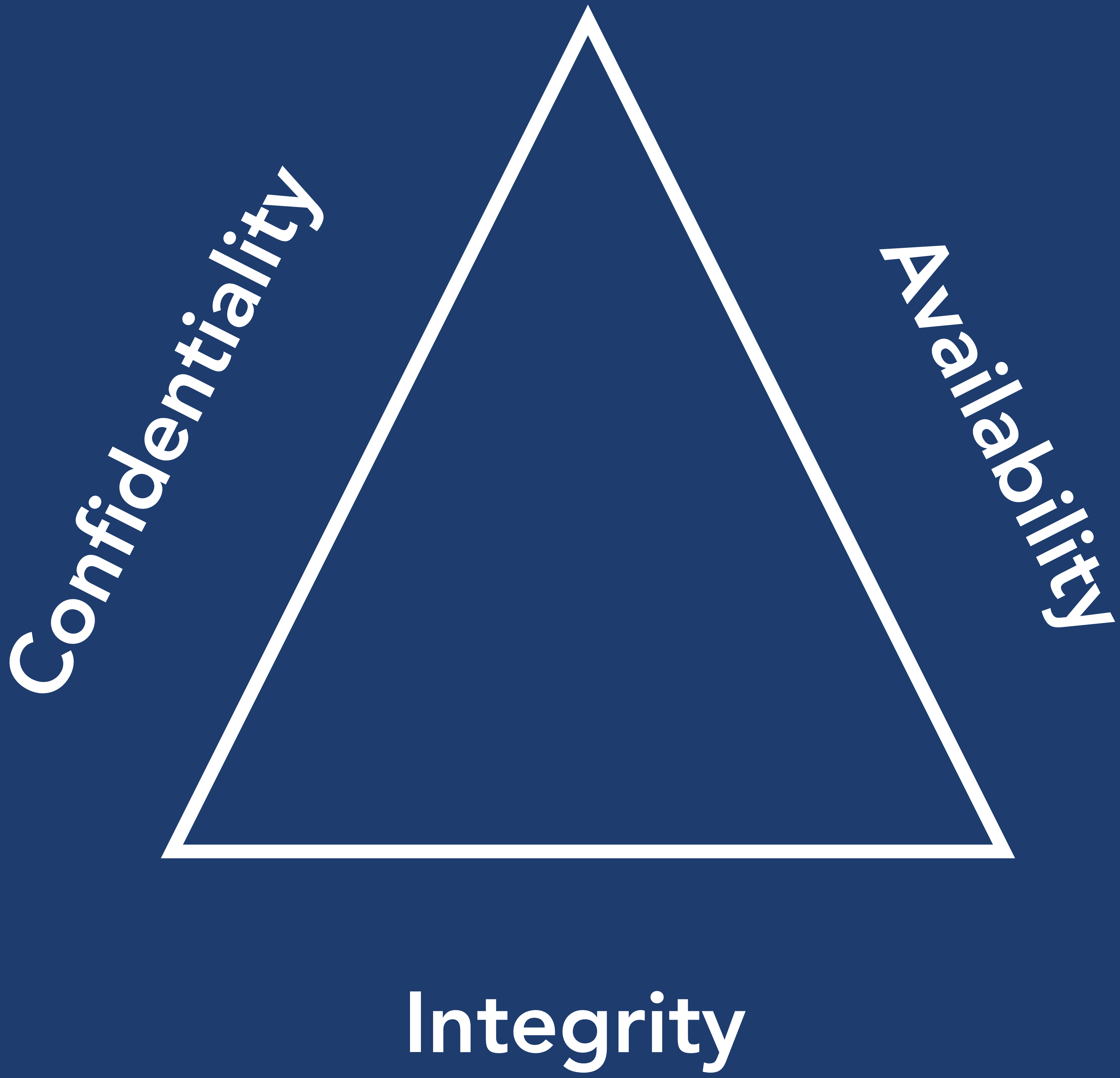
CIA TRIAD



Confidentiality


Availability

Integrity



Confidentiality

Availability

Integrity

CIA TRIAD (ISO/IEC27000)

- **confidentiality** is the property that information is not made available or disclosed to unauthorised individuals, entities or processes.
- **integrity** is the property of accuracy and completeness.
- **availability** is the property of being accessible and usable upon demand by an authorised entity.

CRITICAL INFRASTRUCTURE PROTECTION

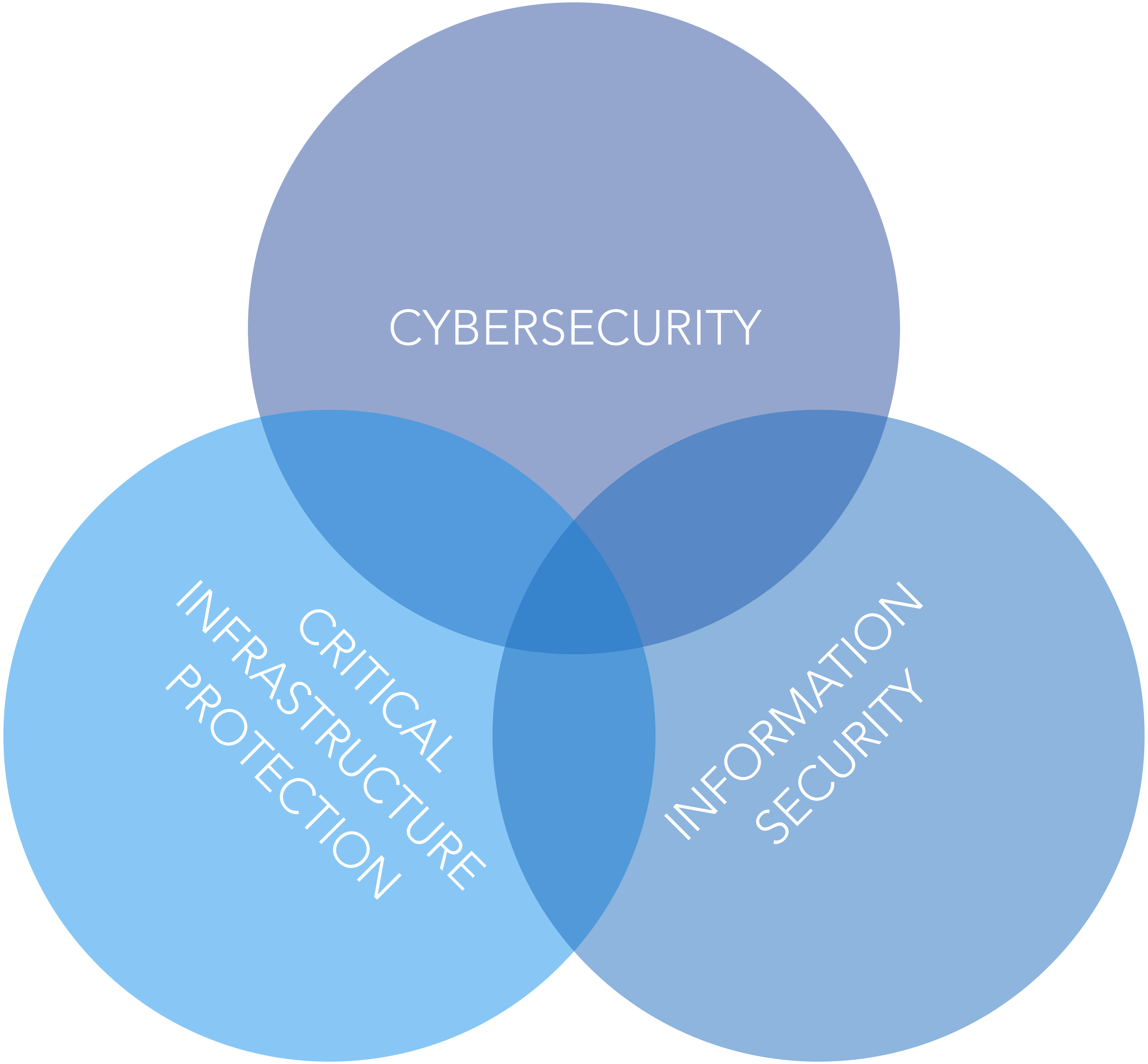
CRITICAL INFRASTRUCTURE PROTECTION (CIP)

- safeguarding infrastructure crucial to modern society from interruption and destruction.

- critical infrastructure includes telecommunication networks, supplies of energy and water as well as emergency services.

- critical infrastructure typical make use of a cyber space and needs protection from cyber threats.

- critical infrastructure protection goes beyond cyber security as it also refers to systems that do not make use of a cyber space.


CYBERSECURITY
CRITICAL INFRASTRUCTURE PROTECTION
INFORMATION SECURITY

SAFETY

SAFETY

- safety can be defined as being free from unacceptable risk to human life, injury or damage (IEC 61508).
- safety is typically concerned with assets that are associated with human life and/or environment.
- nevertheless, while they can be differentiated this does not mean that safety can not impact on cyber security.
- similarly, cyber security incidents could have an impact on safety.

RISK

RISK

RISK

- in simple terms we can think of this as something going wrong that causes harm or loss.

- risk is really the chance of something happening and ramification for a given thing.

- ‘something happening’ can be considered more formally as an **incident**.

- an irrelevant or low value thing is no real interest, a thing of value or **asset** to something.

RISK

- the something could be an individual, enterprise, body but is generally referred to as the **party**.
- chance is the probability or the **likelihood** of something happening.
- ramification refers to the **consequences** of a given incident occurring.
- when considering the consequence and likelihood we arrive at the **risk level**.

CYBER RISK

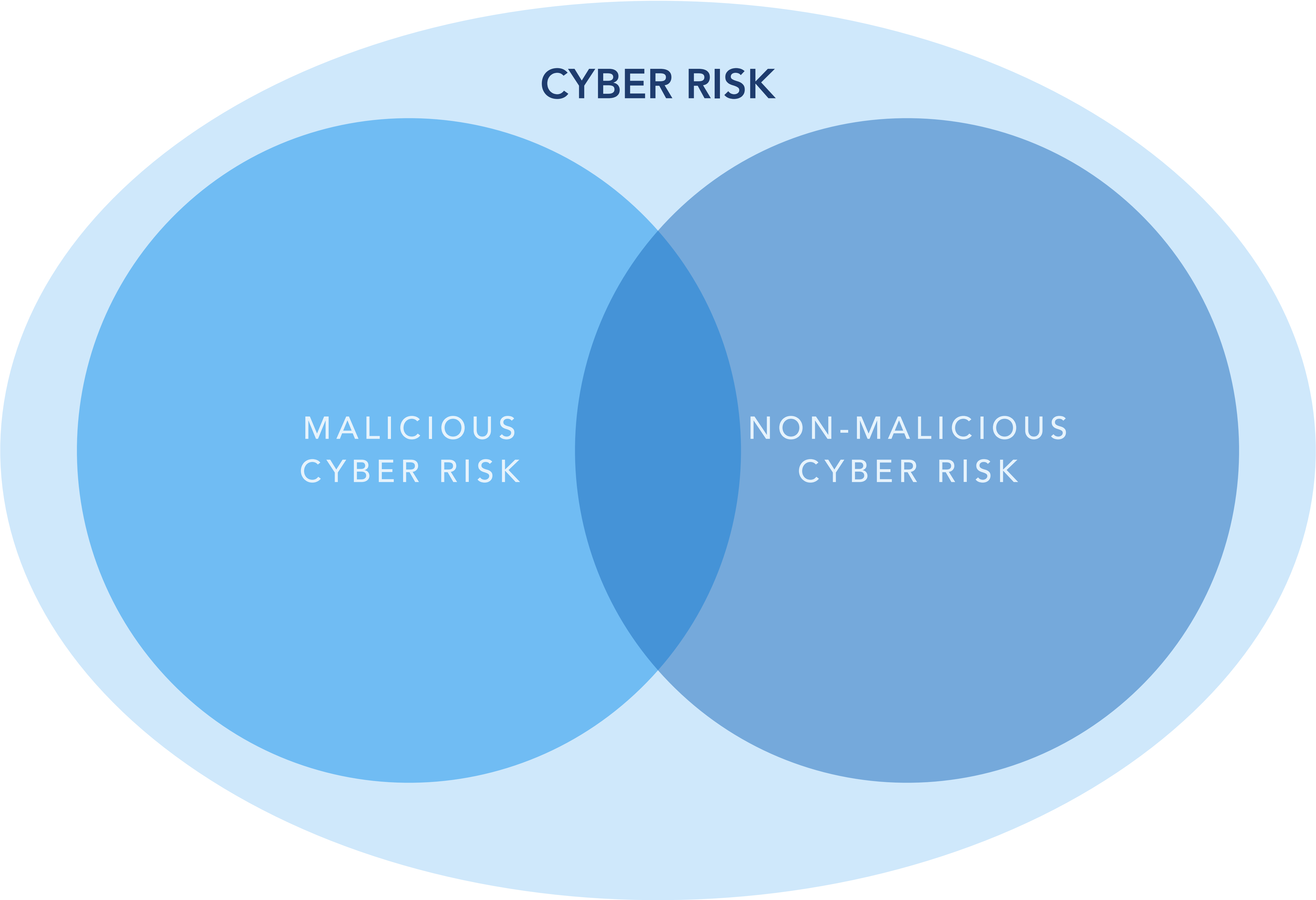
CYBER RISK

- cyber-risk is the product of a cyber threat.

- a cyber system failing due to physical damage, say malicious intent or from flooding is risk, but not a cyber-risk.

- cyber risks are the union of malicious and non-malicious ones.

CYBER RISK


CYBER RISK
MALICIOUS CYBER RISK
NON-MALICIOUS CYBER RISK

CYBER RISK

- The nature of cyber risk can be categorised as **malicious** or **non-malicious**.
- Cyber-risk can also be considered both malicious and non-malicious.
- Cyber-risk could also be the product of both a malicious and non-malicious threat.

SUMMARY

- distinguishing between cyberspace, cyber physical systems, information security, cyber security and safety.
- understanding the differences and overlaps in each area.
- differentiating between malicious and non-malicious cyber-risks.