Dr. Phil Legg

Associate Professor in Cyber Security

Information Risk Management

1: Introduction

UWE Bristol | University of the West of England

Who am I?

Dr. Phil Legg (Office: 2Q17)
Associate Professor in Cyber Security
Programme Leader MSc Cyber Security

Research Interests:

- Visualisation of Cyber Security
- Mitigating adversarial attacks on machine-learning systems
- Cyber Situational Awareness
- Human-machine collaboration

phil.legg@uwe.ac.uk
@dr_plegg
http://go.uwe.ac.uk/phil

UWE Bristol | University of the West of England

Course Delivery and Assessment

- Delivery:
  - A two-hour "lectorial" session each week
  - Self-directed study - preparation and further research

- Assessment:
  - A 3000-word **journal article** on information risk management in the context of a real-world security incident
  - A 15-minute **presentation** that presents the findings from your research and report

- All materials made available via Blackboard

Other Useful Resources

- Course notes and website cover all needed for the course.
- Textbooks are available and will help for exploring deeper into the subject – these are the ones I would recommend (I have preview copies available for students to view if interested).

Learning Outcomes

1. Form deep and systematic understanding of relevant tools, such as ISO27001 and FAIR, in the context of Information Security and Risk management.
2. Identify and analyse the broad range of real-world security issues that face commercial organisations and other institutions.
3. Evaluate and critique the shortcomings of real-world security incidents, and provide clear justification and innovative solutions for how ISMS could help mitigate future incidents, and how FAIR can help quantify and assess risk.
4. Assess and evaluate the appropriateness of security laws and regulations.
5. Reflect on personal capabilities of conducting Information Risk Management providing clear rationale for the methods adopted.

NCSC Security Disciplines

Security Discipline	Skills Group	Indicative Topic Coverage
A. Information Security Management *Principle: Capable of determining, establishing and maintaining appropriate governance of (including processes, roles, awareness strategies, legal environment and responsibilities), delivery of (including polices, standards and guidelines), and cost-effective solutions (including impact of third parties) for information security within a given organisation).* *CESG Knowledge Requirements include:* • *Management frameworks such as ISO 27000 series* • *Legislation such as Data Protection Act* • *Common management Frameworks such as ISO 9000*	**i. Policy, Strategy, Awareness and Audit (A1, A2, A3, A5, G1)**	• The role and function of security policy • Types of security policy • Security standards (e.g. ISO/IEC 27000) • Security concepts and fundamentals • Security roles and responsibilities • Security professionalism • Governance and compliance requirements in law • Third party management • Security culture • Awareness raising methods • Acceptable use policies • Security certifications • Understanding auditability • The internal audit process
	ii. Legal & Regulatory Environment (A6)	• Computer Misuse legislation • Data Protection law • Intellectual property and copyright • Employment issues • Regulation of security technologies

UWE Bristol | University of the West of England

NCSC Security Disciplines

Security Discipline	Skills Group	Indicative Topic Coverage
B. Information Risk Management *Principle: Capable of articulating the different forms of threat to, and vulnerabilities of, information systems and assets. Comprehending and managing the risks relating to information systems and assets.* *CESG Knowledge Requirements include:* • *Information risk management methodologies such as ISO 27005 - Information Security Risk Management* • *Generic risk management methodologies such as ISO 31000 – Risk Management; Principles & Guidelines* • *Key concepts such as threats, vulnerabilities, business impacts, and risk tolerance*	**iii. Risk Assessment and Management (B1, B2)**	• Threat, vulnerability and risk concepts • Threat landscape, adversarial thinking • Asset valuation and management • Risk analysis methodologies • Handling risk and selecting countermeasures/controls to mitigate risk • Understanding impacts and consequences • Security economics

UWE Bristol | University of the West of England

Course Roadmap

1. Introduction – "Managing Risk?", Definitions and Principles
2. Information Security Management Systems (ISMS)
3. Factor Analysis of Information Risk (FAIR)
4. Guest Lecture: UWE Information Security
5. Assessing Risk, Quantifying Risk, Communicating Risk
6. Cyber Value-at-Risk (VaR)
7. Case Studies of Information Risk Assessment
8. Limitations of Risk Assessment
9. Continual Improvements
10. Course Overview and Future Directions

What is *Information?*

What is *Information?*

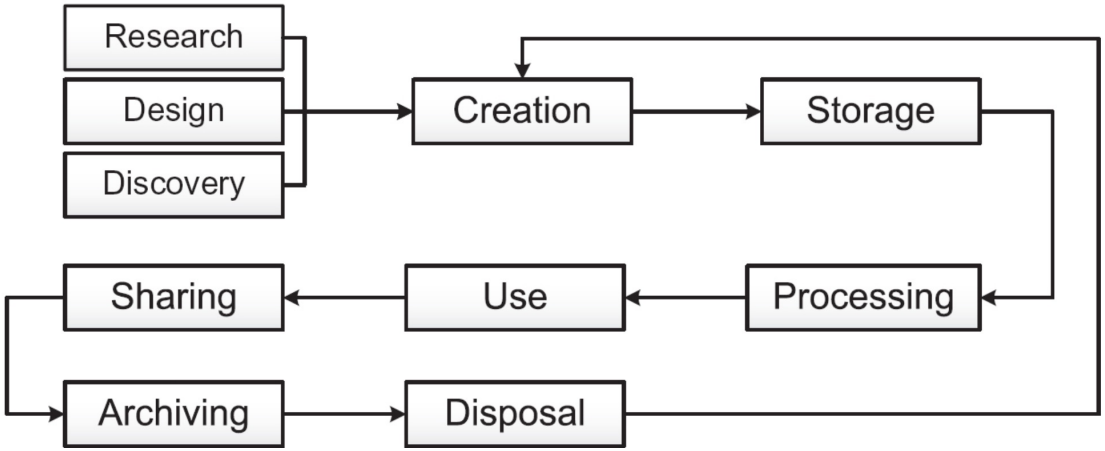
Data is unstructured…
e.g., 42
Information has context…
e.g., 42 customer accounts

2 distinct forms:
Information about information:
i.e., Meta-data
Information in-its-own-right:
e.g., source code
customer record

2 distinct states:
Physical – e.g., paper-based
Electronic – e.g., binary file

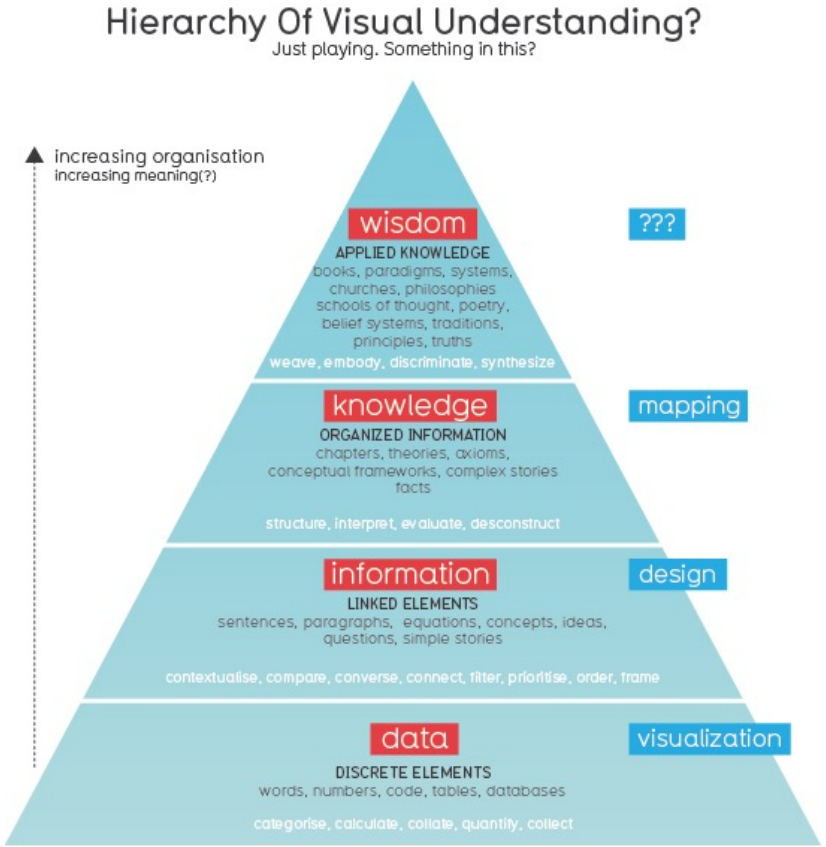
UWE Bristol | University of the West of England

Information Life Cycle



Information lifecycle management (ILM)

Data informs Information, Knowledge and Wisdom



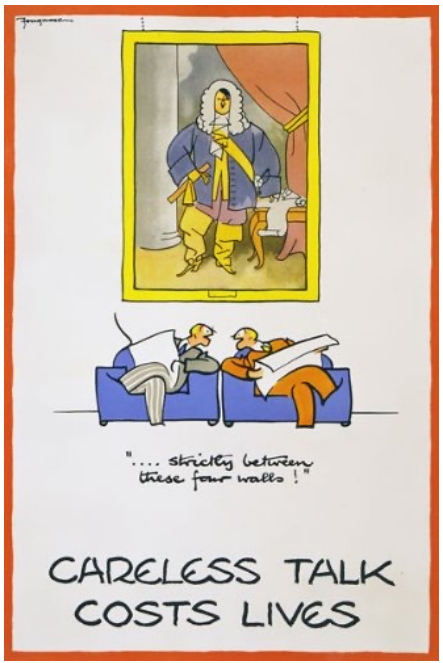
UWE Bristol | University of the West of England

Wikipedia DIKW pyramid
http://www.informationisbeautiful.net/2010/data-information-knowledge-wisdom/

Why do we need Information Risk Management?

UWE Bristol | University of the West of England

1940's poster campaign



UWE Bristol | University of the West of England

Information Classification

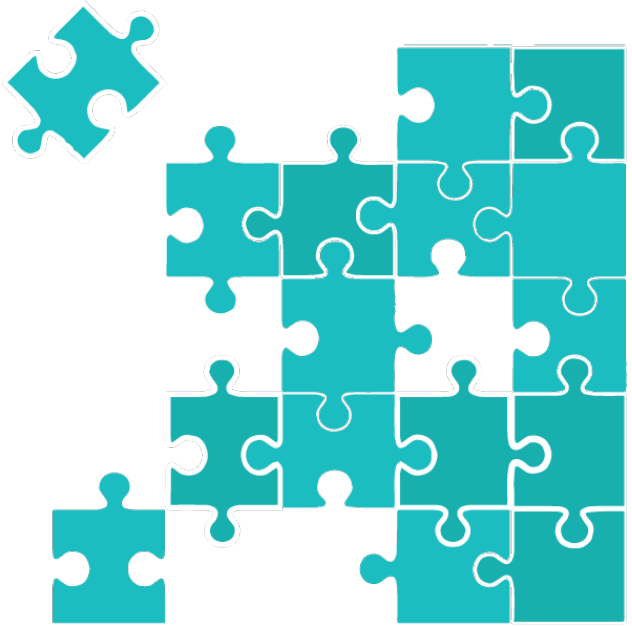
- Information classification may address the sensitivity, handling, storage, access or distribution, and ultimately its disposal.

- The only problem with information classification is that it does not usually reveal the potential value (monetary or otherwise) of the information either to the organisation itself, or to an adversary who might be able to benefit from obtaining it.

Government Security Classifications: https://www.gov.uk/government/publications/government-security-classifications

Information Aggregation

- Aggregated data (e.g., summary statistics) may be regarded as 'masking' the original data, and so are acceptable to share (e.g., Office National Statistics)
- Even then, can disparate aggregated features be compiled to identify complete information on individuals?
- What is the "Risk" of sharing aggregate data?



Information Risk Management

Risk Management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level
(National Institute of Standards and Technology)

Information Risk Management is focussed on how our information assets (i.e., data) can be assessed

Information Security Concepts

Information Security (IS).
Preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved. *(ISO 27001)*

Information Assurance (IA).
The confidence that information systems will protect the information they carry and will function as they need to, when they need to, under the control of legitimate users. *(UK Cabinet Office)*

Cyber Security
The protection of internet connected systems, the data on them and the services they provide, from unauthorized access, harm or misuse. (NCSC)

Information Security Principles

Confidentiality.
The property that information is not made available or disclosed to unauthorised individuals, entities or processes.

Integrity.
The property of safeguarding the accuracy and completeness of assets.

Availability.
The property of being accessible and usable upon demand by an authorised entity.

Asset.
Anything that has value to the organisation, its business operations and its continuity.

UWE Bristol University of the West of England

Definitions from ISO27000

Key Terminology

- **Information assurance** – IA is the practice of assuring information and managing risks related to the use, processing, storage and transmission of information or data and the systems and processes used for those purposes.

- IA includes protection of the confidentiality, integrity, availability, authenticity and non-repudiation of information. It uses physical, technical and procedural controls to accomplish these tasks.

- Whilst focused predominantly on information in digital form, the full range of IA encompasses not only digital information but also analogue or physical information. Protection applies to information in transit, both in physical and electronic forms as well as information at rest in various types of physical and electronic storage facilities. IA as a subject area has grown from the practice of information security.

Key Terminology

- **Confidentiality** – the 'property that information is not made available or disclosed to unauthorised individuals, entities or processes' (ISO/IEC 27000:2014). Confidentiality is concerned with ensuring that information is available to authorised entities, and is not allowed to become available to unauthorised entities, whether they are able to do so deliberately or by accident. It follows therefore that users should only have as much access as they require in order to carry out their task and a formal process is required in order to administer access rights.

- **Integrity** – the 'property of accuracy and completeness' (ISO/IEC 27000:2014). Whilst this definition is fine as far as it goes, the term 'integrity' also suggests a high degree of reliability and assurance, and can apply equally to people as well as to information. Integrity considers both the completeness and accuracy of the information, and, as with confidentiality, users should only have as much access as they require in order to carry out their task and a formal process is required in order to administer access rights. At best, integrity failures can lead to misinterpretation or poor decision-making; at worst they can lead to serious financial impact and embarrassment to the organisation.

Key Terminology

- **Availability** – the 'property of being accessible and usable upon demand by an authorised entity' (ISO/IEC 27000:2014). Availability is often considered the poor relation of CIA, and whilst the other two are very important, if information is not available it becomes frustrating to those who require access to it at the time they require it, and under certain circumstances can have extremely severe consequences. Availability is now a critical element in the delivery or provision of information; not only to customers who shop online at any hour of the day or night, but also to multinational organisations operating across multiple time zone boundaries. Also – a business continuity (BC) issue – the tolerable length of time for which any information asset is unavailable may well vary from one organisation to another.

Key Terminology

- **Authentication** – the 'provision of assurance that a claimed characteristic of an entity is correct' (ISO/IEC 27000:2014). In order to ensure both confidentiality and integrity, authentication mechanisms are used to validate an entity's credentials – this can be either an individual or an application requiring access to information or applications. Authentication mechanisms include such things as passwords, fingerprint and iris scanning and token generators.

- **Accountability** – 'the assignment of actions and decisions to an entity' (ISO/IEC 27000:2012 – for some reason, the term 'accountability' has been omitted from the ISO/IEC 27000:2014 version). Accountability is often confused with responsibility. The two are very different; an entity may be made responsible for carrying out an action, for example an engineer may be responsible for configuring firewall rules, whereas a more senior manager is likely to be accountable for the firewall and/or its rule-set, and may be held to account if things go wrong.

Key Terminology

- **Non-repudiation** – the 'ability to prove the occurrence of a claimed event or action and its originating entities' (ISO/IEC 27000:2014). Non-repudiation can be used both to prove not only that an entity has carried out a certain action but also that an entity has not carried out an action, whether this be carrying out a commercial transaction, editing a document or sending an email. An example of non-repudiation is the use of digital signatures and certificates, which are used to establish the identity of an individual beyond all reasonable doubt.

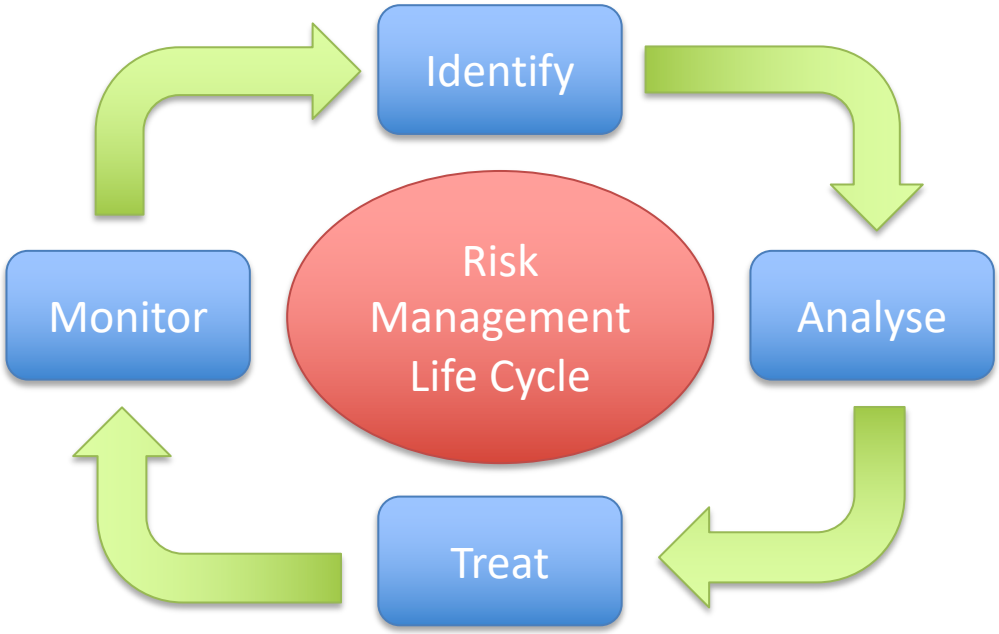
- **Reliability** – 'property of consistent intended behaviour and results' (ISO/IEC 27000:2014). Reliability has similar connotations to integrity, but whereas integrity refers mainly to ensuring accuracy and completeness, reliability leans more towards something that can be repeated with accuracy, for example a process that works in a consistent manner every time.

Key Terminology

- **Information governance** – information governance is the set of multi-disciplinary structures, policies, procedures, processes and controls implemented to manage information at an enterprise level, supporting an organisation's immediate and future regulatory, legal, risk, environmental and operational requirements.

- **Data governance** – data governance refers to the general management of key data resources in a company or organisation. This broad term encompasses elements of data use, storage and maintenance, including security issues and the way data flows from one point to another in an overall information technology architecture.
- Because data or raw information is a key resource for most businesses and organisations, data governance is a logical area of overall information technology strategy focus for many large enterprises.

Managing Security = Managing Risk



What is *Risk*?

UWE Bristol | University of the West of England

What is Risk?

Managing the undefinable

Go to any risk management conference, and you will hear the following complaint:

We have no clear definition of risk. How on earth can we manage something that we haven't defined?

It's a fair point. Risk is such an abstract concept, and it has such a strong influence on all of our lives, yet we can't agree on a definition. Given this, how can we *really* know what everybody else means when they talk about 'risk'?

https://www.ncsc.gov.uk/guidance/fundamentals-risk

What is Risk?

Paradoxically, we see the *lack* of a clear definition as an essential aspect of risk management. The fact that organisations won't necessarily know exactly how everyone defines 'risk' forces us to explain to each other what we mean. It makes us ask questions and challenge assumptions.

This is the fundamental strength of risk management; it provides a way of talking about the future, the outcomes we care about, and how to work to towards them. If we *could* all agree a universal definition of risk, then this could reduce the need for those crucial discussions about the future, uncertainty and risk.

Of course, it may be worthwhile for individual organisations to define, for themselves (and maybe for their supply chains), what they mean by the concept. After all, risks are often analysed from the perspective of organisations, so it is sensible to develop a local definition which is agreed by anyone working on behalf of that organisation. However, avoid trying to make your local definition a universal one.

https://www.ncsc.gov.uk/guidance/fundamentals-risk

National Cyber Security Centre

Managing your information risk

Using technology to deliver business attracts risk. Applying the following principles will help your organisation understand how to approach, assess and manage information and technology risks.

1 Understand the business context

Provide a context in which risk management and assessment is to be conducted. This should outline what your organisation is trying to achieve, the business assets involved, legal and regulatory requirements and third party risk management/contractual considerations. This context must summarise the risks you're prepared (or not prepared) to take and the governance structure in place to support risk management decision taking.

2 Decide on the risk management approach

You must understand and communicate the risk management approach your business is going to take. This provides confidence that the technology and information used is secure. Risk assessment and management requires technical, security and business skills. Choosing the wrong approach can be costly in terms of resource and security compromise.

3 Understand key risk components

Risk assessments have inputs and outputs. Consider fundamental inputs of your risk assessment (e.g. threat, vulnerability and impact). Regardless of risk assessment methods used, the inputs and outputs should be understandable in the context of your organisation.

4 Understand what risks exist

The risk assessment method must be applied in the context of what your organisation is trying to accomplish. You should know which risk management decisions the assessment will inform, who's responsible for making them and the level of detail required. Prioritise the outputs from the assessments to make informed risk management decisions.

5 Communicate risk consistently

Irrespective of your approach to assessing risks, capture the outcome in a way that can be used to inform business decision making. Output from risk assessment and management activities may need to be communicated to interested third parties.

6 Make informed risk management decisions

Make objective decisions about what needs to be done to manage identified risks, informed by subject matter expertise, information and evidence.

For more information go to www.ncsc.gov.uk @ncsc

UWE Bristol | University of the West of England

What is *Risk*?

Risk.
The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organisation. (ISO27000 / ISMS)

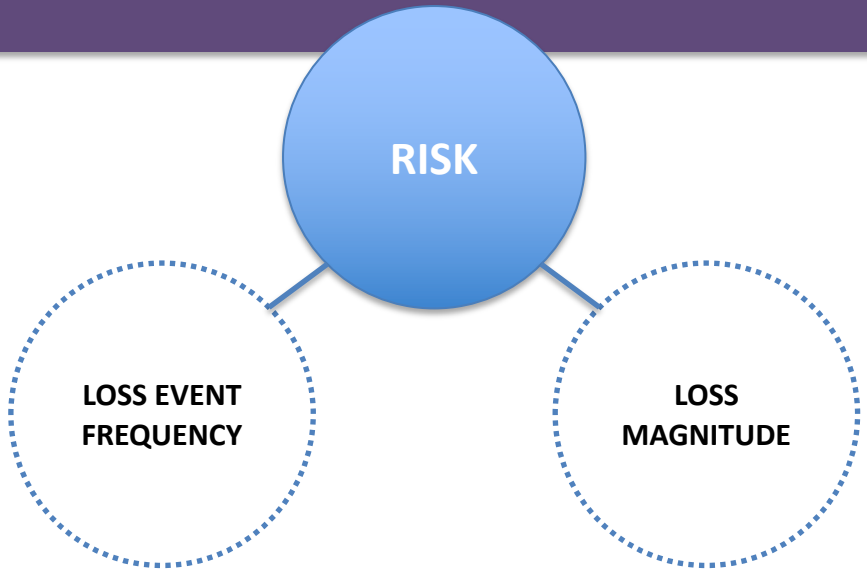
Risk = Threat x vulnerability

Likelihood x severity

UWE Bristol | University of the West of England

What is *Risk*?

"The probable frequency and probable magnitude of future loss"
- Factor Analysis of Information Risk (FAIR)



UWE Bristol | University of the West of England

What is *Risk*?

Cyber risk and risk management
The risks and opportunities which digital technologies, devices and media bring us are manifest. Cyber risk is never a matter purely for the IT team, although they clearly play a vital role. An organisation's risk management function need a thorough understanding of the constantly evolving risks as well as the practical tools and techniques available to address them.

What do we mean by cyber risk?
'Cyber risk' means any risk of financial loss, disruption or damage to the reputation of an organisation from some sort of failure of its information technology systems.

It will never happen to us….
All types and sizes of organisations are at risk, not only the financial services firms, defence organisations and high profile names which make the headlines.

(Institute of Risk Management)
https://www.theirm.org/knowledge-and-resources/thought-leadership/cyber-risk/

UWE Bristol University of the West of England

Exercise:
The Bald Tyre

The Bald Tyre

The follow describes a risk scenario in four simple stages.

Ask yourself how much risk is associated with what's being described.

The Bald Tyre

Picture in your mind a bald car tyre. Image that it is so bald you can hardly tell that it ever had tread.

How much Risk is there?

A little | None | Lots

The Bald Tyre

Next, imagine that the bald tyre is tied to a rope hanging from a tree branch.

How much Risk is there?

A little | None | Lots

The Bald Tyre

Next, imagine that the rope is frayed about halfway through, just below where it's tied to the tree branch.

How much Risk is there?

A little | None | Lots

The Bald Tyre

Finally, imagine that the tyre swing is suspended over an 80-foot cliff with sharp rocks below.

How much Risk is there?

A little | None | Lots

The Bald Tyre

"What about the person using the swing?"

The Bald Tyre

"What about the person using the swing?"

ASSUMPTIONS

We never said anything about people…

The Bald Tyre

Now… let's try to identify the following components.

What was the **Threat**, **Vulnerability**, and **Risk**?

https://www.fairinstitute.org/blog/video-what-is-risk-the-bald-tire-scenario

The Bald Tyre

Now… let's try to identify the following components.

What was the **Threat**, **Vulnerability**, and **Risk**?

Is it even possible?
We are operating without clear knowledge of the problem domain….

The Bald Tyre

https://www.fairinstitute.org/blog/video-what-is-risk-the-bald-tire-scenario

Purpose of Risk Management

"The purpose of risk management is not to chase the unattainable goal of perfectly secure systems and a risk-free business; it is to make sure that you have thought about what can go wrong, and that this thinking has influenced your organisation's decisions."

https://www.ncsc.gov.uk/guidance/fundamentals-risk

Summary

- What is Information, and why do we need Information Risk Management?
- What are the security concepts and terms that relate to IRM?
- How do we define what we mean by Risk?
- How do we measure and assess risk in an accurate manner, without bias or assumption?