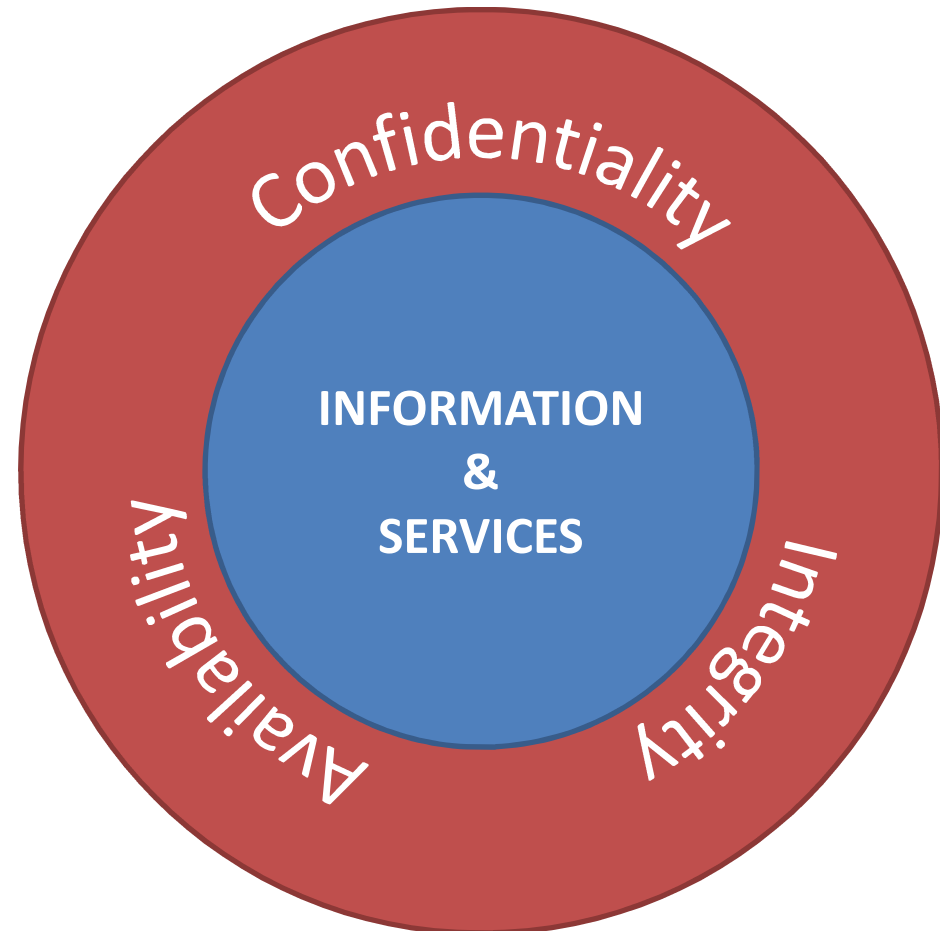# What is information security?
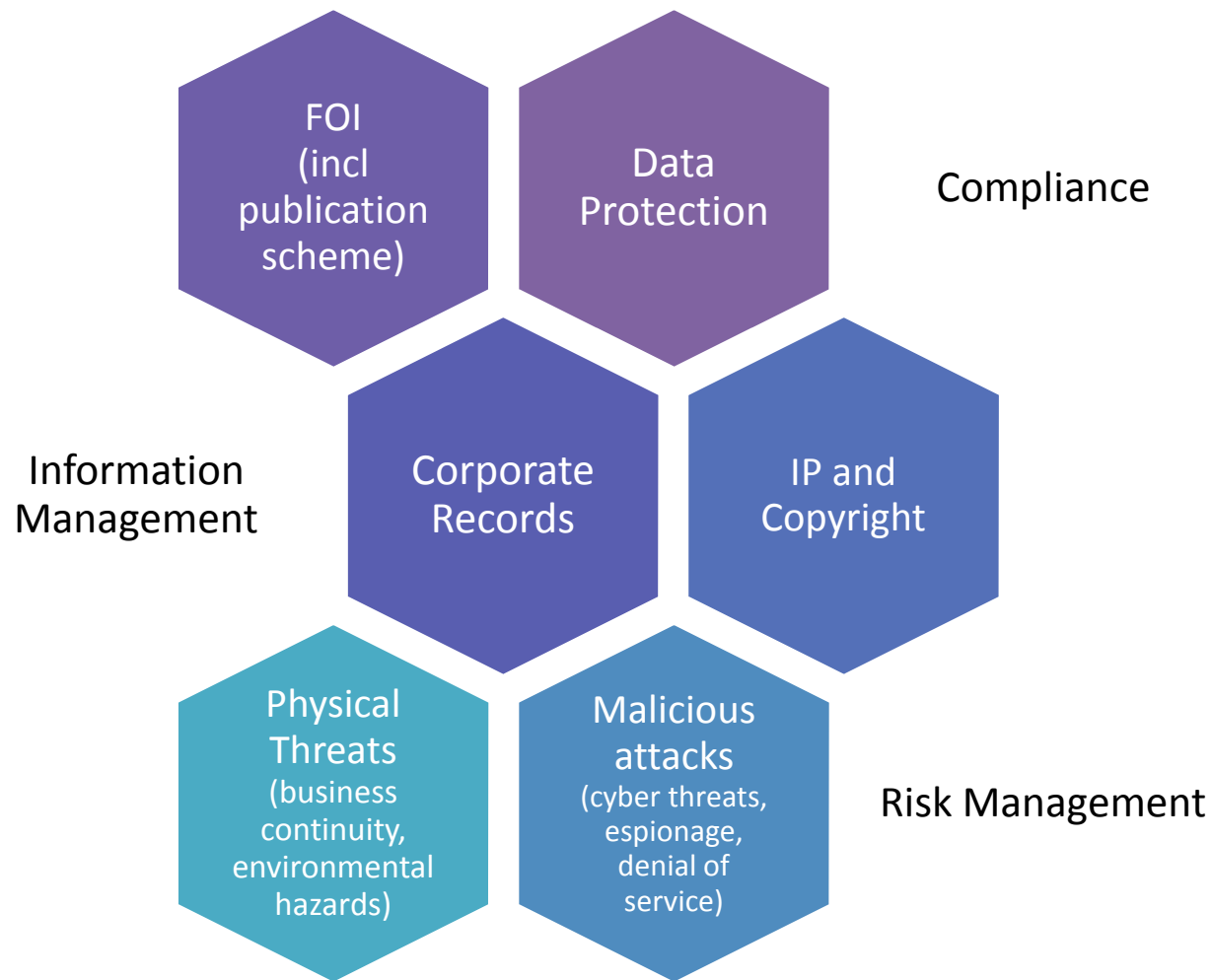
Information is an asset...

As one of our core outputs, it is one of the most valuable assets the University owns

Our assets need to be protected...

The role of information security is to protect our information, and to ensure its confidentiality and integrity, whilst maintaining its availability

Confidentiality

Integrity

Availability

INFORMATION & SERVICES

What does 'Information Security' cover here?

FOI (incl publication scheme)

Data Protection

Compliance

Corporate Records

Information Management

IP and Copyright

Physical Threats (business continuity, environmental hazards)

Malicious attacks (cyber threats, espionage, denial of service)

Risk Management

Key principles of information security

Confidentiality
- Providing access to information for only those individuals with a valid and authorised reason to do so

Integrity
- Ensuring that information is not altered/deleted or otherwise tampered with by people unauthorised to do so

Availability
- Ensuring information and other critical assets are available when needed
- ...it's a fine balancing act!...

It's a fine balancing act!

These are the bases of data protection legislation and industry standards for information security

What are the threats and risks?

Reputational Risk

Reputational Damage:
UEA 'Climategate' Hack by Anti-climate change activists;
near-market or cutting edge research of interest to others for commercial advantage

HEIs hacks:
Common in US with increasing reports in UK media

In 2012, 51 US institutions reported breaches totalling 1,977,412 records; most achieved through password hacking

Financial Risk

Compliance (DPA): Penalties up to £500k
lack of appropriate processes and training has lead to increased fines in recent cases;
proposed higher EU penalties on way

UK Cyber Security Strategy:
National concern of research and IP theft – universities considered part of 'critical national infrastructure'

Business Continuity Risk

Disruption to operations:
by hactivists, disgruntled individuals, state-sponsored groups;
Spamhaus attack 'slowed the internet down' and US banks show heavy losses as computers were 'shut down'

New and emerging technologies
(e.g.Cloud services)
provide opportunities to 'goodies' and 'baddies' alike so risks need to be identified to stay ahead of the game

Internal Risks

Internal compliance:
Weaknesses in policy and processes in terms of coverage and enforcement

Impact of IS Measures on Community:
Information Security processes could be seen as constraining or stifling to a community which is used to open systems and access

What do these threats and risks apply to?

The short answer….everything!

Type of Information	Medium	Core Risks to UoW information
• **Personal info** – identifying living individuals • **Sensitive info** – identifying specifics on individuals – medical, religion, financial details etc. • **Commercial information** – strategic planning, 'trade secrets' • **Research info** – may include any of the above, plus intellectual property • **Our information** and that of **our partners** (info entrusted to us for a specific purpose)	• **The medium doesn't matter**… It can be… • **Paper** • **Electronic data** … XLS, Word, PPT, any type of file or program • On **any kind of media**, using **any kind of storage** … CDs, DVDs, hard drives, flash drives, paper, stored on your desk, in your drawer, in filing cabinets, waiting to be shredded. The list is endless!...	• Theft (physical or cyber) • Accidental loss • Loss of access • Inappropriate disclosure • Loss of privacy • Loss of accuracy in information • Damage to information • Fraud • Espionage (physical or cyber)

# Could the threats and risks happen here?
Yes because...

We have a huge community - with 30+ departments, over 5k staff and over 22k students, that's a lot of people generating information, and information about a lot of people to manage

We have sensitive and highly sought after research (Clinical Trials, WMG) and high profile partnerships (JLR, TATA); we have a perceived lower level of commercial confidentiality because of our public benefit position

We have a greater need to share and collaborate with partners than other businesses so our systems and community are deliberately open
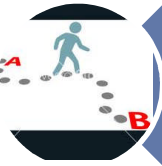
We have a reputation for open systems and collaboration with all sorts of organisations; we are an attractive target as a gateway to these organisations –malicious parties may not be interested in our assets but may be interested in using our infrastructure to gain access or cause disruption to those we work with

We have a reputation for academic excellence and innovation. We have a strategic vision to be in the global Top 50. We need to ensure info security risks don't jeopardise our goals as recognised in the University Risk Register

UoW Information Security Roles

Who is responsible for what

Governance Team

- Develop and promote policy (approval IPSC)
- Provide guidance and training
- Monitor compliance

Legal Services

- Ensure compliance with the Data Protection Act
- Manage Freedom of Information
- Manage copyright
- DP Incident response and facilitates remedial action or reporting

IT Services

- Provide technical implementation of policy (e.g. anti virus)
- Incident response (when IT breaches occur)
- Provide technical expert advice
- Provides metrics of incidents and sector comparison

The community

- HoDs – implement policy at local level and responsible for local compliance
- Individuals – enact best practice and report real/potential incidents
- It's everyone's responsibility!