The University Of Sheffield.

COM1008: Web and Internet Technology

Lecture 17 Information Security

Dr. Steve Maddock
s.maddock@sheffield.ac.uk

theguardian

Security bug allows remote attack of Uconnect system, letting hackers apply the brakes, kill the engine and take control of steering over the internet

Samuel Gibbs

@SamuelGibbs

Tuesday 21 July 2015
15.30 BST

Shares 6695 Comments 407

Save for later

The Jeep Cherokee is vulnerable to remote cyberattack that allows hackers to take control. Photograph: NRMA Motoring and Services/Flickr

1. Information

- Information is ubiquitous, valuable, available
  - an organisational asset
  - access to information to do our jobs
- Many forms: shared in conversation, on paper, online
- Increasing amounts of online information
  - interaction with companies and public services
  - freely offering personal information, especially younger generation

"Information is the oxygen of the modern age."
(Ronald Reagan, 1989)

113,839 cases of identity fraud in the UK in 2014
[https://www.cifas.org.uk/]

http://www.pwc.co.uk/services/audit-assurance/insights/2015-information-security-breaches-survey.html

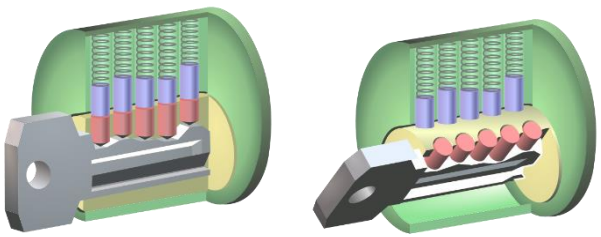
1.1 Benefits of online information

Benefits of the digitally-enabled economy [cphc report, 2014]

- *E-commerce* leads to more efficient, more convenient ways of doing business
- *Smart cities/smart grids* leads to enhanced energy efficiency
- *Connected healthcare* enhances patient experience and outcomes by more efficient and immediate access to relevant medical data
- *Online banking and shopping* allows people more time for other priorities
- *Online learning* makes education more accessible to many
- *Social networking* enables more people to be connected to friends, family, job opportunities and more.

http://cphc.ac.uk/2014/11/02/integrating-cybersecurity-into-computer-science-curricula/

2. How secure is your information?



Consider three aspects:

- Physical security
  - Building, office, cabinet
  - Locks, cards and magnetic strips, passcodes, …
- Information security
  - Protection of assets
  - Policies, encryption, access control
- Network and communication security
  - Authentication, protocols, encryption
  - Firewalls, anti-virus software, VPN, https…

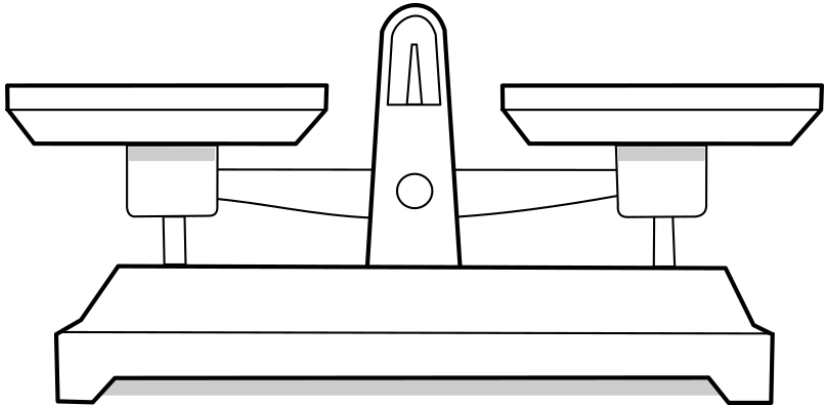
http://www.sheffield.ac.uk/cics/ucards

3. Protection: on balance

- We want to protect against malicious attack by outsiders (and by insiders)

Keep enemies out

Increasingly complex ways to let friends in



- Maximum security with minimum impact on user access and productivity

4. Identifying risk

- Assets
  - For a network: its individual components
- Vulnerabilities
  - Weaknesses or security flaws that makes an attack possible
- Threats
  - Potential dangers to information or system
  - Take advantage of vulnerabilities
- Attacks
  - Actions leading to violation of security

4. Identifying risk

- Vulnerabilities
  - Weaknesses or security flaws that makes an attack possible
  - Technology, e.g. Windows – how often do you update?
  - Configuration, e.g. passwords (default?), JavaScript in browsers
  - Security policy, e.g. passwords, app installation
  - Fixes: software patches, reconfiguring devices, deploying countermeasures (e.g. firewalls, antivirus software)
- Threats
  - Potential dangers to information or system
  - Take advantage of vulnerabilities
- Attacks
  - Actions leading to violation of security

Annual survey of most used passwords

Rank	Password	Change from 2013
1	123456	*No Change*
2	password	*No Change*
3	12345	*Up 17*
4	12345678	*Down 1*
5	qwerty	*Down 1*
6	123456789	*No Change*
7	1234	*Up 9*
8	baseball	*New*
9	dragon	*New*
10	football	*New*

http://splashdata.com/blog/

4. Identifying risk

- Vulnerabilities
  - Weaknesses or security flaws that makes an attack possible
- Threats
  - Potential dangers to information or system
  - Take advantage of vulnerabilities
  - From: professional criminals, well-intentioned employees make mistakes, social protest, terrorism
- Attacks
  - Actions leading to violation of security

http://www.pwc.co.uk/services/audit-assurance/insights/2015-information-security-breaches-survey.html

4. Identifying risk

- Assets
  - For a network: its individual components
- Vulnerabilities
  - Weaknesses or security flaws that makes an attack possible
- Threats
  - Potential dangers to information or system
  - Take advantage of vulnerabilities
- Attacks
  - Actions leading to violation of security
  - Examples: reconnaissance, access, denial of service, worms, viruses, Trojans

4.1 Analyse risk to prioritise

- Likelihood of being targeted by an attack
- Probability of success of attack
- Impact on business and harm caused

Which one would you allocate more resources to protecting?

4.2 UK 2010 National Security Strategy: Tier One Priority Risks

- "The Strategy identifies 15 priority risk types, the most pressing of which are:
  - acts of terrorism affecting the UK or its interests
  - **hostile attacks upon UK Cyber Space**
  - a major accident or natural hazard (for example, influenza pandemic)
  - an international military crisis between states, drawing in the UK and allies"
- Potential impact on IT systems for government, infrastructure, business and economy

https://www.gov.uk/government/publications/the-national-security-strategy-a-strong-britain-in-an-age-of-uncertainty

5. Why Does Information Security Concern Me?

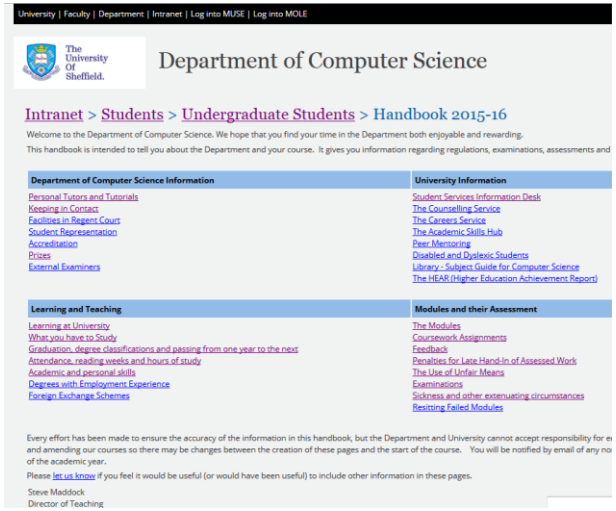
Do you? [vulnerabilities][threats][risks]

- Scan incoming emails with anti-virus software
- Regularly update of anti-virus software
  - [lack of update][virus attack][destruction of…]
- Make back-ups of files
- Forward warning emails to friends/others
- Use a complicated password and change it regularly
  - [lack of access security][unauthorised data access; theft; fraud][loss/destruction of data/software; others acting on behalf of you]
- Apply security patches on PC regularly

6. Consider e-commerce site

Before building

- Identify goals, products, customers
  - Increased sales, reduced processing costs, faster turnaround of orders
  - Sensible solution?
- Be aware of different kinds of site
  - Publishing company info (COM site)
  - Taking orders (supermarket site)
  - Providing services (parcel tracking)
  - Providing digital goods (e-books)
  - Entertainment (online games)
- Understand threats and risk



University | Faculty | Department | Intranet | Log into MUSE | Log into MOLE

The University Of Sheffield.

Department of Computer Science

Intranet > Students > Undergraduate Students > Handbook 2015-16

Welcome to the Department of Computer Science. We hope that you find your time in the Department both enjoyable and rewarding.

This handbook is intended to tell you about the Department and your course. It gives you information regarding regulations, examinations, assessments and

Department of Computer Science Information	University Information
Personal Tutors and Tutorials	Student Services Information Desk
Keeping in Contact	The Counselling Service
Facilities in Regent Court	The Careers Service
Student Representation	The Academic Skills Hub
Accreditation	Peer Mentoring
Prizes	Disabled and Dyslexic Students
External Examiners	Library - Subject Guide for Computer Science
	The HEAR (Higher Education Achievement Report)

Learning and Teaching	Modules and their Assessment
Learning at University	The Modules
What you have to Study	Coursework Assignments
Graduation, degree classifications and passing from one year to the next	Feedback
Attendance, reading weeks and hours of study	Penalties for Late Hand-In of Assessed Work
Academic and personal skills	The Use of Unfair Means
Degrees with Employment Experience	Examinations
Foreign Exchange Schemes	Sickness and other extenuating circumstances
	Resitting Failed Modules

Every effort has been made to ensure the accuracy of the information in this handbook, but the Department and University cannot accept responsibility for e
and amending our courses so there may be changes between the creation of these pages and the start of the course. You will be notified by email of any no
of the academic year.

Please let us know if you feel it would be useful (or would have been useful) to include other information in these pages.

Steve Maddock
Director of Teaching

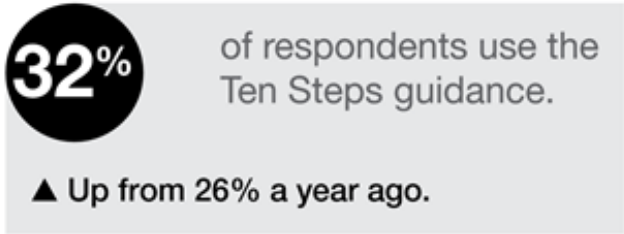
6. Consider e-commerce site

- Business threats
  - Hackers
  - Not getting enough / getting too much business
  - Capacity limitations
  - Hardware failure, network and utility failure
  - Reliance on other companies
  - Competition
  - Software errors
  - Government policies and taxes
- Security threats
  - Exposing confidential data
  - Loss or destruction of data
  - Modification of data
  - Denial of service attacks
  - Errors in software
  - Repudiation – how can Amazon prove you ordered and received a product? Is it worth the cost of doing so?

7. Security policy

- E-commerce site: How will you cope with
  - An earthquake, DDoS attack, IT boss goes on holiday, Fire, Disk crash, Broadband cable is cut, Power cut, Unhappy employees?

- Companies need a security policy
  - 2012: HMG launched its 10 Steps to Cyber Security
  - More recently, The Cyber Essentials Scheme has been created which focuses on Internet-originated attacks against an organisation's IT system.



http://www.pwc.co.uk/services/audit-assurance/insights/2015-information-security-breaches-survey.html

https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary

10 Steps To Cyber Security

CESG

Defining and communicating your Board's Information Risk Management Regime is central to your organisation's overall cyber security strategy. CESG recommend you review this regime - together with the nine associated security areas described below - in order to protect your business against the majority of cyber threats.

User Education and Awareness

Produce user security policies covering acceptable and secure use of the organisation's systems. Establish a staff training programme. Maintain user awareness of the cyber risks.

Home and Mobile Working

Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline build to all devices. Protect data both in transit and at rest.

Secure Configuration

Apply security patches and ensure that the secure configuration of all ICT systems is maintained. Create a system inventory and define a baseline build for all ICT devices.

Removable Media Controls

Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing on to the corporate system.

Managing User Privileges

Establish account management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

Incident Management

Establish an incident response and disaster recover capability. Produce and test incident management plans. Provide specialist training to the incident management team. Report criminal incidents to law enforcement.

Monitoring

Establish a monitoring strategy and produce supporting policies. Continuously monitor all ICT systems and networks. Analyse logs for unusual activity that could indicate an attack.

Malware Protection

Produce relevant policy and establish anti-malware defences that are applicable and relevant to all business areas. Scan for malware across the organisation.

Network Security

Protect your networks against external and internal attack. Manage the network perimeter. Filter out unauthorised access and malicious content. Monitor and test security controls.

Establish an effective governance structure and determine your risk appetite.

Information Risk Management Regime

Maintain the Board's engagement with the cyber risk.

Produce supporting information risk management policies.

Department for Business Innovation & Skills | CPNI Centre for the Protection of National Infrastructure | Cabinet Office

8. Classical goals of information security

protect

- Confidentiality
  - Information only accessible to authorised parties.

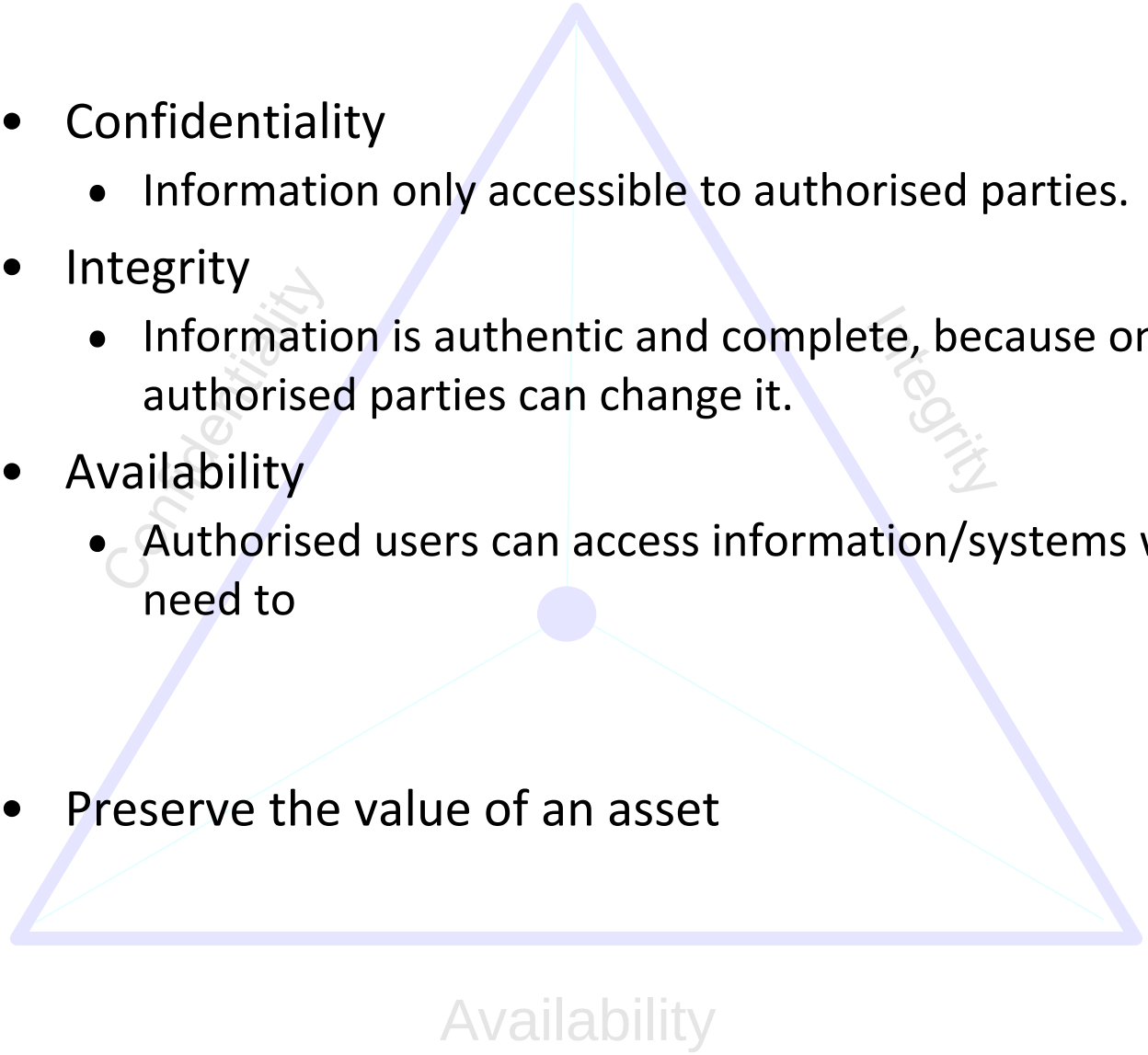
maintain

- Integrity
  - Information is authentic and complete, because only authorised parties can change it.

ensure

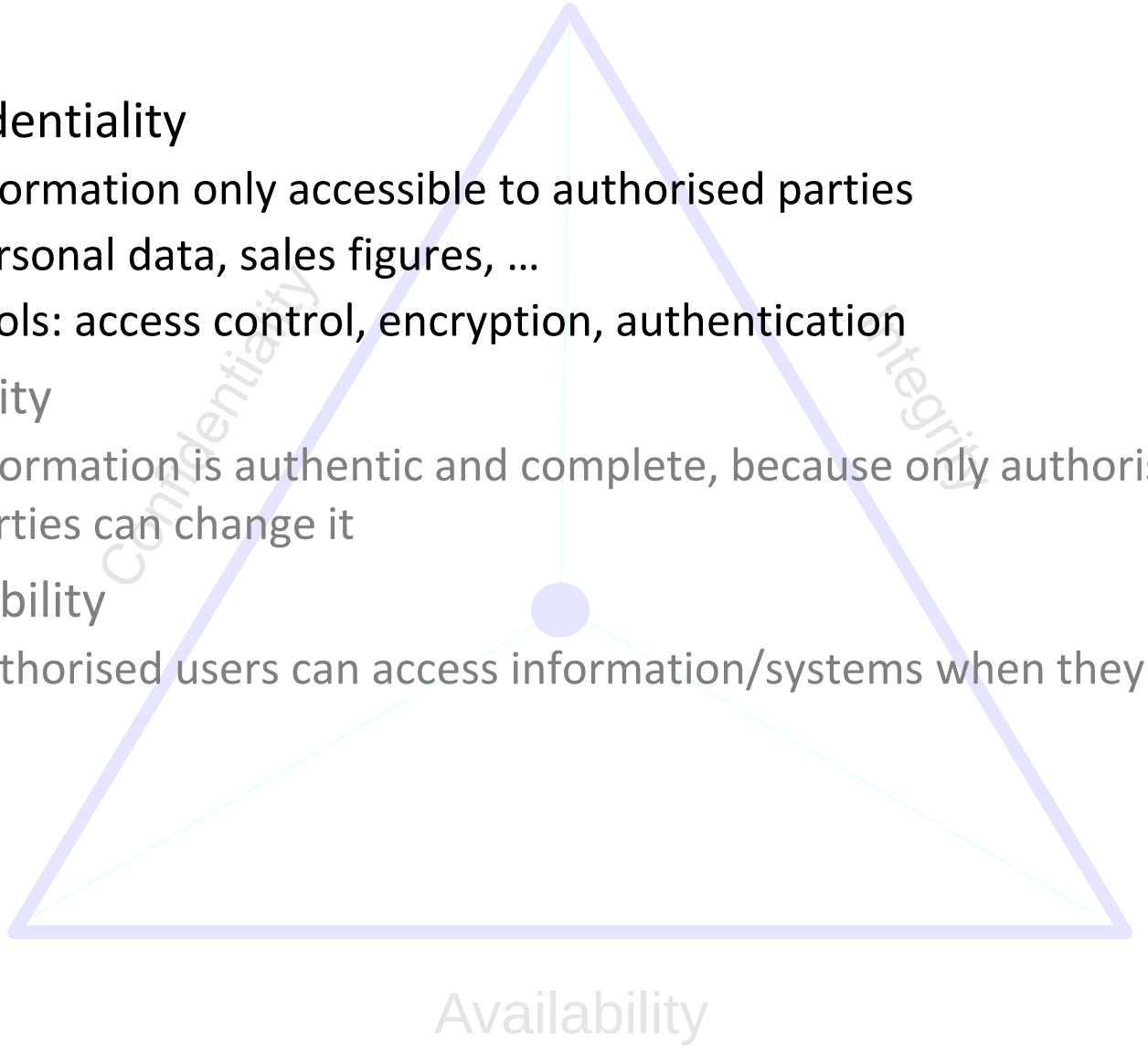
- Availability
  - Authorised users can access information/systems when they need to

- Preserve the value of an asset



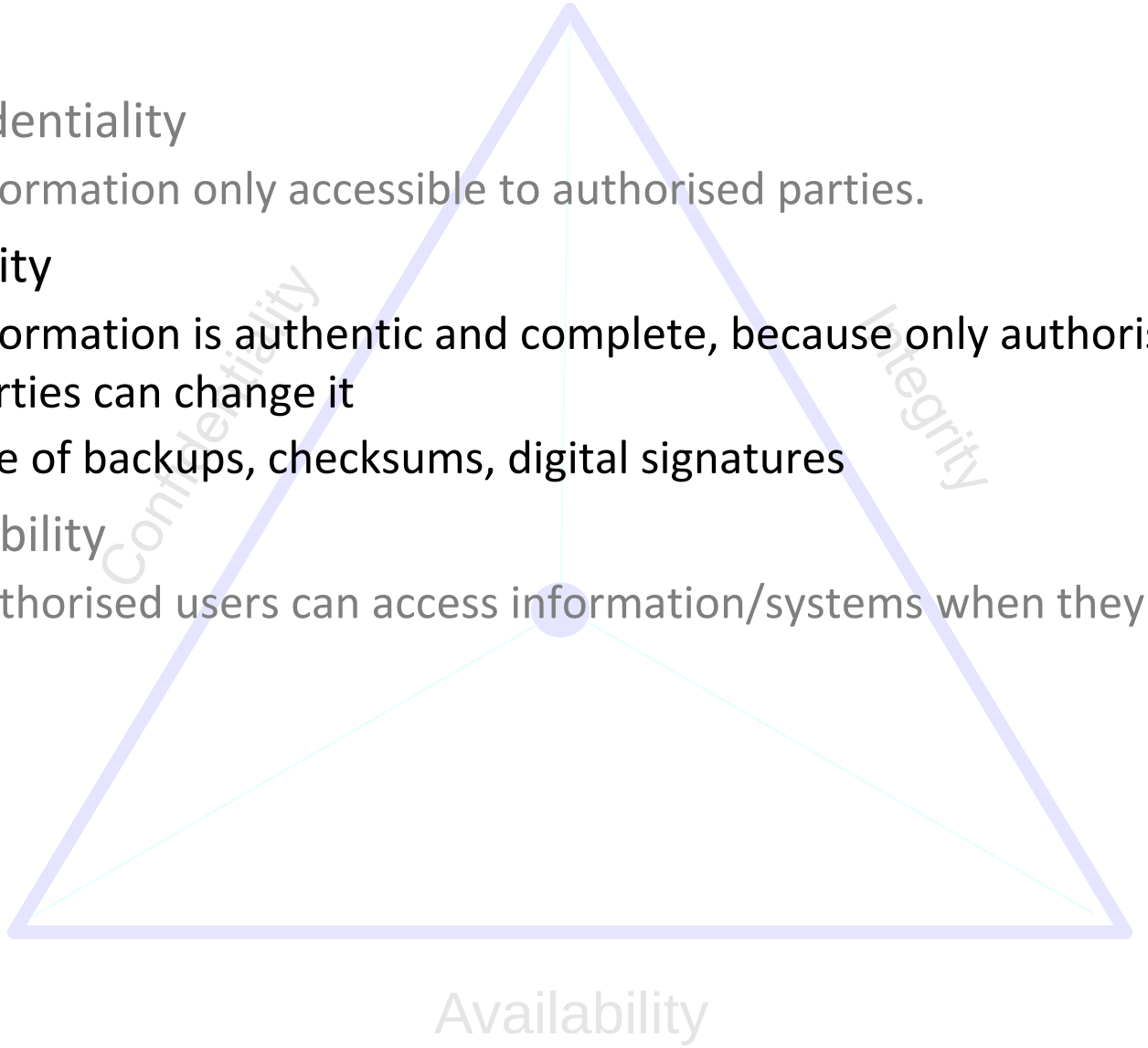
8. Classical goals of information security

- Confidentiality
  - Information only accessible to authorised parties
  - Personal data, sales figures, …
  - Tools: access control, encryption, authentication
- Integrity
  - Information is authentic and complete, because only authorised parties can change it
- Availability
  - Authorised users can access information/systems when they need to



8. Classical goals of information security

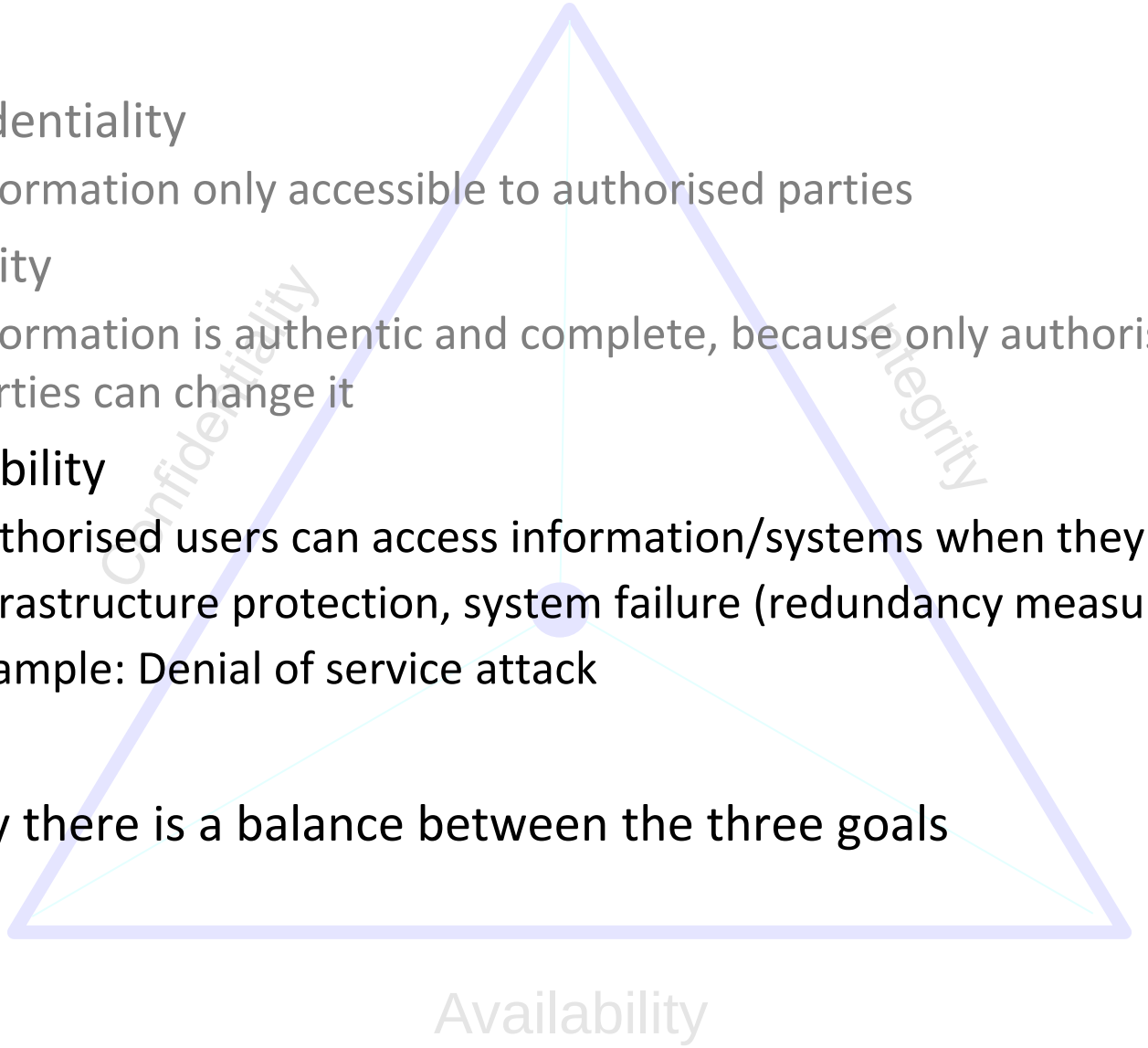
- Confidentiality
  - Information only accessible to authorised parties.
- Integrity
  - Information is authentic and complete, because only authorised parties can change it
  - Use of backups, checksums, digital signatures
- Availability
  - Authorised users can access information/systems when they need to



8. Classical goals of information security

- Confidentiality
  - Information only accessible to authorised parties
- Integrity
  - Information is authentic and complete, because only authorised parties can change it
- Availability
  - Authorised users can access information/systems when they need to
  - Infrastructure protection, system failure (redundancy measures?)
  - Example: Denial of service attack

- Ideally there is a balance between the three goals



8.1 Exam results

- Computer-generated tables of data and statistical analyses to help Exam Board interpret results of individuals and cohort
- Availability – sensitive to timing
  - One hour unavailable has no adverse effect
  - Unavailable for a day or a week, then problems
  - Rearranged Board, schedules, knock-on effects for other boards
  - Total loss of data would mean reassessment and reputation damage
- Loss of Integrity
  - Damaging if only discovered after results sent out
  - If Board's procedures detect, then impact similar to delay in availability
- Breach of confidentiality
  - Reputation damage if before official announcement of results
  - If identifiable student, then possible legal action

Example from: http://www.open.edu/openlearn/science-maths-technology/computing-and-ict/introduction-information-security/content-section-4.3.1

9. Legal issues and privacy concerns

- One reason for companies to create and follow a security policy is compliance with the law
  - Business liability
- Due diligence – the technology person assesses vulnerabilities, threats and risks
- Then, executives decide based on four strategies:
  - Transfer the risk (insurance)
  - Reduce the risk (apply some intervention)
  - Accept the risk (understand and shoulder loss)
  - Reject the risk (it is not likely to happen)
- Knowledge of legal frameworks is required

https://www.gov.uk/data-protection/the-data-protection-act

9.1 The Data Protection Act, 1998

- Controls how your personal information is used by organisations, businesses or the government. Must make sure the information is:
  - used fairly and lawfully
  - used for limited, specifically stated purposes
  - used in a way that is adequate, relevant and not excessive
  - accurate
  - kept for no longer than is absolutely necessary
  - handled according to people's data protection rights
  - kept safe and secure
  - not transferred outside the European Economic Area without adequate protection
- Information Commissioner's Office [https://ico.org.uk/]
  - The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals

9.2 The UK Computer Misuse Act (1990)

Computer misuse offences:

- Unauthorised access to computer material.
- Unauthorised access with intent to commit or facilitate commission of further offences.
- Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.
- Making, supplying or obtaining articles for use in offence under section 1 or 3

http://www.legislation.gov.uk/ukpga/1990/18/contents

10. Summary

- Information is ubiquitous, valuable, available
- Need to consider physical, information security, and network and communication security
- In identifying risk, consider vulnerabilities, threats and attacks
  - Consider: What are the risks associated with using a computer at home to make an online purchase?
- The three classical goals of information security are **confidentiality**, **integrity** and **availability**
- Be aware of legal frameworks
- *Next week*: some practicalities and encryption

- Online course on 'Protecting Information' at https://infosecurity.shef.ac.uk/