1 What is information security?

This chapter describes the basic concepts of information security, the context within which educational organisations operate, and introduces the topic of information security management. It forms part of Stage 1 – Foundations and Stage 3 – Implementation, support and operation in the Toolkit Route map.

Key topics

- **The three aspects of information security**
- **How threats to information are changing**
- **The purpose of information security management**

1.1 The purpose of information security

Information takes many forms. It can be stored on computers, transmitted across networks, printed out or written down on paper, and spoken in conversations. In an academic context, information is a crucial asset.

Regardless of its form and content, information has value. This value is maintained by its:

- confidentiality: it is accessible to the right people
- integrity: it has not been tampered with or damaged
- availability: it is there when needed.

Information security is intended to protect information to an appropriate extent by maintaining the level of risk to the organisation at an acceptable level. Effective information security management enables information to be used and shared while protecting its value. In this way, an organisation can maintain efficient operations, achieve legal compliance and maintain its reputation.

Each organisation will have its own attitude to information risk, and should take this into account when deciding what controls to implement.

All members of an organisation are responsible for contributing to its management of information security: their actions, or inaction, can protect or expose information to risk.

1.2 Context

All universities are facing increasing threats to their information from a wide range of sources, including organised crime, as noted in the Universities UK publications on Cyber Security. New sources of threat, such as nation states, and ideologically motivated organisations, continue to emerge. Such threats are becoming more widespread, more ambitious and increasingly sophisticated. Attacks can also be carried out without an attacker even having to leave their home.

According to the Ponemon Institute, the cost of a data breach in 2014 was $145 (£90) per record, including recovery costs, fines/legal costs and impact to normal operations. Thus the overall cost of a breach affecting a database containing 2,000 student records would be expected to be £180,000.

Attackers motivated by money will attack anything from which they can make a profit: e.g. by reselling the

The UK National Security Strategy identifies attacks in cyber space and cyber-crime as a "Tier 1" threat on a par with terrorism.

use of IT resources, by selling personal data, financial data and industrial secrets, or by holding valuable information for ransom. Attackers motivated by the desire to further their country's interests will seek to gather information in bulk and to determine how to disable rival countries' capabilities. Attackers motivated by ideology will seek to spread fear and disorder, for example by destroying high-profile targets.

At the same time, due to organisations' evolving usage of IT, they are becoming more vulnerable to less obvious threats. The growth of cloud services, outsourced approaches to information management and external collaborations present new opportunities for misuse and error, and reduce the role of central, specialised control of IT facilities.

Furthermore, since research activities are increasingly intended to show real-world relevance and benefit, it is reasonable to expect that their work will become more appealing to attackers, as it will be more likely to have a value on the black market.

Educational institutions have other unique properties which make their information risks, and approaches to handle them, different from other organisations (see Chapter 2, Information security governance, for more information).

As their awareness of information risk increases, institutions are seeking to align their operational information security activities to business goals, and asking information security teams to provide assurance of information risk management.

1.3 Legal and contractual requirements

Legislation, including the Data Protection Act 1998, the Copyright, Designs and Patent Act 1988, the Regulation of Investigatory Powers Act (RIPA) 2000 and the Computer Misuse Act 1990, places requirements on businesses to protect personal privacy and to ensure the confidentiality and security of their information. For example, holders of personal data must not only be registered with the Information Commissioner's Office but must also take adequate steps to protect that data from unauthorised access. Fines for breaching the Data Protection Act can be up to £500,000. It is also worth mentioning the Privacy and Electronic Communications Act 2003.

Other contractual agreements bring with them further sources of requirements, such as the Health and Social Care Information Centre's Information Governance Toolkit (IG Toolkit) and the Payment Card Industry Data Security Standard (PCI DSS).

Finally, in order to be granted permission to use certain datasets for research purposes (medical records, for example), organisations are increasingly being required to provide evidence of mature information governance.

1.4 What is information security management?

Creating and maintaining an information security management system (ISMS) is an ongoing activity; as with gardening, there is no moment when it is possible to say that it is finished, and there is no more work to do.

If information security is concerned with protecting the confidentiality, integrity and availability of information to an appropriate extent, then information security management is the means by which this can be achieved. The international standard ISO/IEC 27001 describes a way to manage information security, by creating what it calls an information security management system, or ISMS. This is a combination of processes, policies, governance activities, and specific security measures which work together to enable an organisation to manage information risk effectively, and to demonstrate that it is doing so.

Summary

- Information security applies to all forms of information
- Threats are becoming more sophisticated and revenue-led
- Information security is the responsibility of all members of an organisation

Resources

Template for an information security strategy proposal

Reading list

The UK National Security Strategy
www.ucisa.ac.uk/ismt5
www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf

Cyber security and universities: managing the risk
www.ucisa.ac.uk/ismt6
www.universitiesuk.ac.uk/highereducation/Documents/2013/CyberSecurityAndUniversities.pdf

Ponemon Report: 2014 Cost of Data Breach Study
www.ucisa.ac.uk/ismt7
http://www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/

Monetary Penalty Notices: Information Commissioner's Office
www.ucisa.ac.uk/ismt8
https://ico.org.uk/enforcement/fines