

Why does Information Safety matter?

Information and information systems are increasingly important to universities and colleges: a failure of information may now lead directly to a failure of the education or research process. Conversely an information system that is trusted by its users will provide much greater benefits to the organisation and the individual user. This paper highlights the need for information and information systems to be lawful, reliable and trusted; the growing threats to these essential attributes; and the need for changes in attitudes and processes, as well as systems, to ensure that organisations have the safe information systems they require. Information Safety is above all a human and management issue: users must be informed and willing to work with safety measures rather than against them and must be supported by consistent policies. Human involvement and commitment are essential.

Who should be interested in Information Safety?

The safety of information should be the responsibility and interest of everyone in educational organisations.

This paper will be of particular interest to those who need to build and use safe information systems, individuals and departments who are responsible for information and processes as well as those who are responsible for the systems that implement them:

- Registrars, Academic Registrars, Heads of Personnel
- Heads of Department, faculty and departmental administrators
- Heads of Management Information Systems and Heads of IT

Key Information Safety issues

Information and information systems are growing in importance for the operation of educational organisations. For some organisations and some functions an information

systems failure may still only be embarrassing and expensive, but for many, information is already a critical asset and a failure at the wrong time will be a catastrophe.

A key feature of current developments is the move to using electronic storage as the master or only copy of information: this can have great benefits but it also exposes information to new threats. Managed Learning Environments are the most advanced instance of this trend, where the entire record of a student's learning and assessment may be contained in an electronic 'file'. This can be very efficient for both student and institution but it also means that a breach of security can cast doubt on the education of an entire class. Electronic records can, in principle, be altered invisibly and without a paper copy for comparison such alteration will be impossible to detect. The same trend can be seen in administration, with many organisations using electronic communications for planning, decision-making and operation. Records of these electronic processes must be protected as carefully, with as much thought and resource, as their paper or parchment predecessors. Moving information to electronic systems need not increase the risks – it will usually increase some and decrease others – but does change their nature and the measures that need to be taken to protect against them.

Electronic information systems and their users are also much less forgiving of faults. Someone scribbling on a printed prospectus for a joke only affects that single copy: an alteration with the same motivation to the online prospectus will be visible immediately to every reader everywhere in the world. Users expect electronic information and services to be instantly available at all times, like electricity or telephones, even though few computers or networks have been designed to meet such demanding standards. Students who have been promised online learning anywhere at any time, researchers who have been promised immediate access to databases and commercial partners who have been promised state of the art facilities will soon go elsewhere if these are not delivered.

Reducing the likelihood of failure, in other words improving the safety of information and information systems, is now essential for the business of education and research.

Lawful, Reliable, Trustworthy

In security theory, systems are usually analysed in terms of confidentiality (information is only seen by those who are authorised), integrity (information only changes under the control of those who are authorised) and availability (information can be obtained when and where it is needed). However, user demands, and hence operators' concerns, are more likely to focus on three related aspects: an information system must be lawful, reliable and trustworthy.

Lawful: There should be no question that information systems need to be lawful; the Data Protection Act 1998, Human Rights Act 1998 and Regulation of Investigatory Powers Act 2000 all place legal requirements on the owners of information systems and controllers of information. Without action to address these, many organisations will be breaking the law.

Reliable: The users' conception of system reliability includes all of confidentiality, integrity and availability. Put most simply, a user expects an information system to behave as they wish: systems will be accessible at all times and information will be handled as the user intends, whether that involves keeping it secret or publishing it to the world. Information systems cannot meet this expectation without considerable and continuing effort.

Trustworthy: An information system is trustworthy when its users believe, and act as if they believe, that it is reliable. Users who trust a system will not take unnecessary, and potentially harmful, precautions such as keeping working copies of information in local data files: they will use and rely on the safety measures provided by the system itself. Trustworthiness relies on users' perception: even the most reliable system will not be trustworthy if its users do not perceive it as such. The greatest threat to trustworthiness is the actions (or failures to act) of users themselves.

None of these desirable attributes is automatically present in any information system: all of them require effort at all stages – design, implementation and operation – of the system's life. Furthermore, all of them are affected by people and processes as much as by equipment and software: a safe information system cannot be achieved by technology alone.

Lawful

The DTI's Information Security Breaches Survey 2002 found that more than half of UK businesses had no documented procedures to ensure compliance with the Data Protection Act. Although an informal survey by UCISA suggests the situation is better in education, it is still likely that offences against data protection law are committed every day. Similarly, any organisation that has not updated its policies and practices to address the Human Rights and Regulation of Investigatory Powers Acts is likely to be committing criminal offences in running its own network.

Recent legislation has concentrated on protecting the legitimate rights of individuals: those who use information systems and those whose details are stored on them. Protecting individual rights should in any case be the aim of educational organisations as society expects us to behave responsibly towards staff, students and stakeholders. Failure to do so can result in very bad publicity. Breaking the law can also have serious consequences for the individual, the organisation and its management. Punishment for criminal offences includes fines and imprisonment, with personal liability for institution managers in some cases. Civil breaches can lead to very large payments for damages. Equipment or information may be seized as evidence; injunctions may prevent use of all information that may have been gathered or used unlawfully. The disruption caused by these interim measures may be more costly than any eventual fine.

The law does not, in general, prohibit reasonable actions, but does require that they be authorised and justified. There is a recognition that a balance needs to be struck between protecting the individual and protecting the community. Documented authority, controlled by processes, checks and balances are the best way to achieve legal compliance and to give users confidence that powers will not be misused.

Reliable

Many JANET sites have already learned that an unreliable information system may do more harm than good. A common situation is where a dedicated system to handle student recruitment fails at the critical time because of insufficient care to ensure reliability. Such failures are very public and very embarrassing.

Information and information systems must be present and accurate when they are needed. Like any other complex system in a hostile environment, this requires capacity to handle normal and peak loads, protection from known threats and maintenance to ensure that new threats can be resisted. Threats may come from authorised users, deliberate internal or external attacks, or from the

background noise of random attacks to which any system is now exposed when connected to a shared network. Networks, especially those with an Internet connection, must now be considered hostile to the reliability of information and not the harmless places they may once have been.

Protection can often be implemented by technical means on the information system or network. Such measures can provide rapid improvements in reliability. For example, routers and firewalls can and should block unknown network traffic before it reaches the protected system. Information systems should not run software they do not need as this will increase their exposure to threats as well as reducing their ability to perform their intended tasks. Threats change over time, so key software and systems must also be maintained to address new threats. This requires a continuing process to ensure that the necessary staff time, skills and resources are allocated.

To some extent there is a trade-off between protection and maintenance. Systems that are not maintained need the highest level of protection that can be provided by external means. Systems that are maintained effectively may permit some relaxation of these protecting controls. However, a reliable information system will almost always require both technical protection and human maintenance.

Trustworthy

Trustworthiness should be the goal for any information system, since without it no system can achieve its potential benefits. Indeed, in the long term a system that is not trusted may be harmful. If the institution's systems for managing the learning and assessment process are not trusted to collect and keep accurate records of student achievement then staff, students and employers will be unwilling to rely on them. If central databases are not trusted to be readily and conveniently accessible then staff will keep their own personal copies which will inevitably diverge: a disaster for effective operation and for compliance with the Data Protection and Freedom of Information Acts.

Everyone who uses or relies on an information system must have confidence in its results, that information is accurate and disclosed as authorised. Reliability gives a basis for confidence, but is not sufficient, as confidence is a human attitude, not a technical fact. A system may in fact be very reliable, but if its users perceive it as unreliable then it will never be trusted. Trust is therefore very fragile as it can be damaged by any unexplained event or plausible rumour. It is very dangerous to adopt information systems for key functions but at the same time blame all problems on 'computer error'.

Information systems involve information, systems and people, and these all need to work together to create a trustworthy system. Processes for the collection, processing and disposal of information need to be designed to be worthy of trust. Those who own information should be identified and given the authority and tools to ensure that it is used safely. Indeed, once an information system is technically reliable, the greatest threat to it comes from its users: a member of staff who leaves an unprotected terminal logged in to a database casts doubt on all the information and applications to which they had access. Trustworthy systems require trustworthy users who know what can be expected of the system and what cannot. Users who understand the importance of the systems and information they use are more likely to develop responsible behaviour and attitudes: this requires information and advice to be made available, promoted and, above all, followed by those in authority.

Trustworthy information systems are essential but they will only be achieved when each person recognises their responsibility and acts so as to create them.

Actions to Take

Every organisation will be at a different stage in its need for, and implementation of, information security. However, the following measures are likely to be useful first steps in improving the safety of information in most educational organisations.

Lawful: Problems are most likely in the areas of information handling and network operations. All staff who collect or process personal data must fulfil their obligations under the Data Protection Act 1998; these may require changes to current processes. Staff involved in the operation of computer systems and networks must be formally authorised to comply with the Data Protection, Regulation of Investigatory Powers and Human Rights Acts; procedures need to be documented and published to reassure staff and users that this authority will not be abused. The JISC Briefing Papers on these Acts and UKERNA's Charter for System Administrators provide further guidance.

Reliable: Information systems connected to today's hostile Internet can be made more reliable by technical measures. Systems that are exposed to the network must be assigned staff resources to configure and maintain them for security. Those systems where this

cannot be guaranteed must be protected at the network level: default-deny router or firewall configurations should be the norm. The details of these measures should be based on an assessment of the risks to the organisation to avoid spending resources to counter minor threats while leaving major ones unattended. Standard pre-packaged solutions are unlikely to meet any organisation's specific needs. The JISC study on "Use of Firewalls in an Academic Environment" provides an excellent discussion of these measures.

Trustworthy: Technical measures alone cannot achieve the best possible reliability, and will never achieve trustworthiness. All users need to be educated in the part they have to play in the security of the systems they own; through learning and following good practice they should also come to appreciate what can and cannot be expected of information systems, and to trust the service

they provide. This process of raising user awareness will take time, so should be started as soon as possible. A JISC study surveyed user awareness in UK HE institutions; James Madison University has an excellent online awareness programme.

These measures will be easier to implement, and more effective, if they are supported by an organisational policy on Information Security. The UCISA/JISC Information Security Policy Toolkit and JISC Senior Management Briefing Paper are highly recommended. Without such a policy there is a much greater risk of resistance and exceptions being claimed. Even in this environment some improvement should be possible but an information system that is not supported by all users, from the most junior to the most senior, will inevitably be less reliable, trustworthy and lawful, more expensive and harder to use, than one that is. Each organisation should aim to develop a culture of safe information, involving people's beliefs and behaviours. People are the most important part of information safety.

Where to find out more

Threats:

- Information Security Breaches Survey, www.security-survey.gov.uk
- 'Can You Trust Your Data?', www.jiscinfonet.ac.uk

Legal:

- JISC Legal Information Service, www.jisclegal.ac.uk
- JISC Senior Management Briefing Papers:
 - Data Protection Act, www.jisc.ac.uk/index.cfm?name=pub_smbp_dpa1998
 - Regulation of Investigatory Powers Act, www.jisc.ac.uk/index.cfm?name=pub_smbp_ripa
 - Freedom of Information Act, www.jisc.ac.uk/index.cfm?name=pub_ibsm_foi
- Charter for System and Network Administrators, www.ja.net/development/legislation/sysadmin-charter.html

Reliable:

- Use of Firewalls in an Academic Environment, www.ja.net/documents/technical_guides.html
- JANET-CERT website, especially www.ja.net/CERT/JANET-CERT/prevention/
- UCISA/JISC Information Security Policy Toolkit, www.ucisa.ac.uk/resources/infosecurity/

Trustworthy:

- JISC Assist information security workshop, www.jisc.ac.uk/index.cfm?name=event_infosec_0102
- JISC project on Human and Organisational Issues associated with security, www.jisc.ac.uk/index.cfm?name=project_network_security
- James Madison University has an excellent awareness programme, including:
 - Online training, www.jmu.edu/computing/security/sa
 - Detailed information, www.jmu.edu/computing/runsafe

Policy:

- JISC Senior Management Briefing Paper on Information Security Policies, www.jisc.ac.uk/index.cfm?name=jcas_papers_security