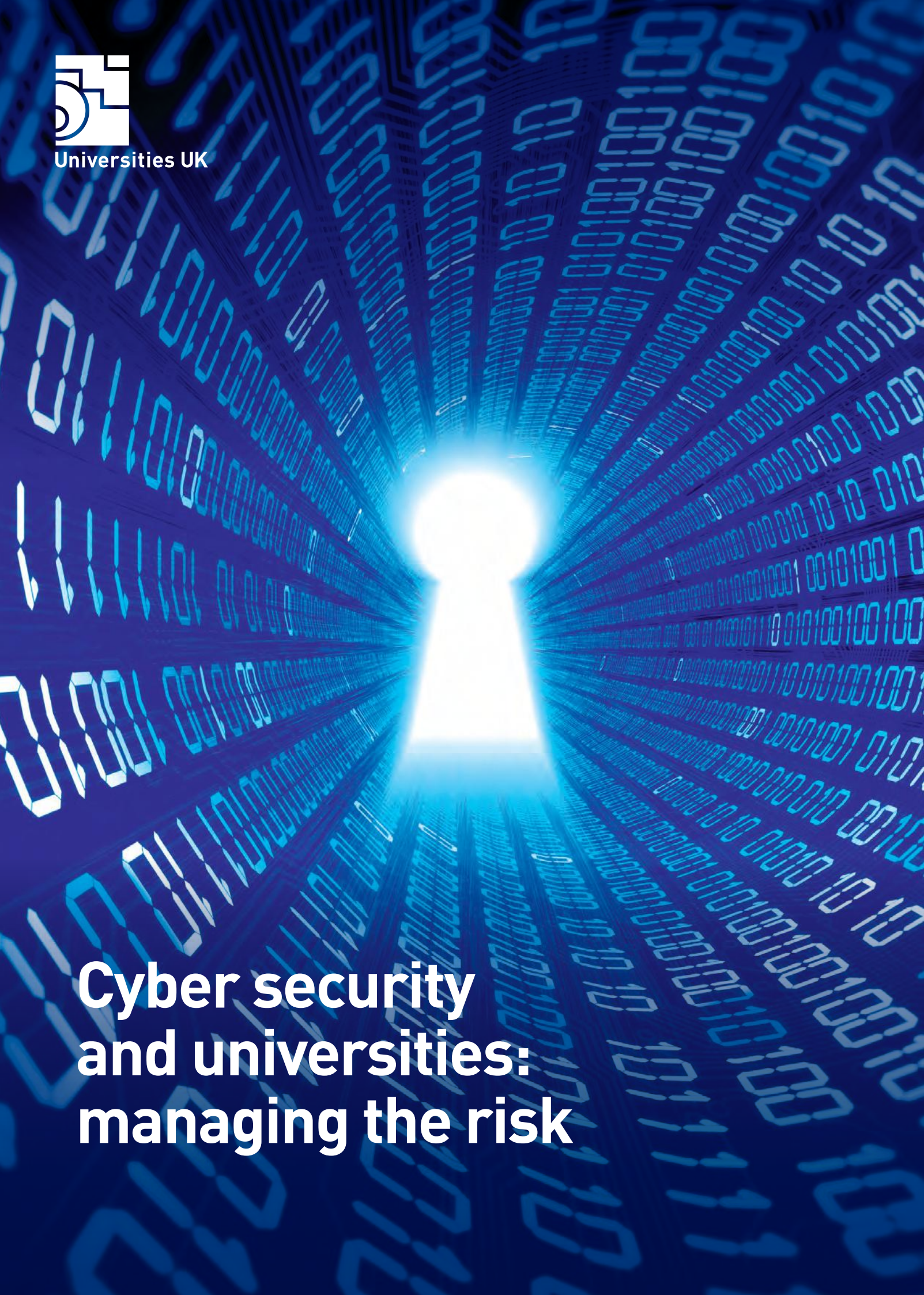


Universities UK

Cyber security and universities: managing the risk

CONTENTS

Executive summary	1
1. Introduction	2
2. The cyber security problem facing universities	3
3. Assessment of institutional risk	6
4. Implementing cyber secure information governance	10
5. Conclusion	16
Annexe A: Bibliography	17
Annexe B: Organisational standards for cyber security	18
Annexe C: Research data management practice	19
Annexe D: Case study information	21

EXECUTIVE SUMMARY

As the importance of digital information and networks grows, cyber security is increasingly fundamental to the success of all organisations.

This report looks at approaches to implementing cyber security in higher education institutions. The report is not written from a technical perspective. Instead, it explores the management steps that are required across the whole organisation in order to be cyber secure. It primarily focuses on the challenge of protecting against targeted, unauthorised attempts to access digital information. The report looks at approaches to evaluating these risks and how these should inform the development of risk based management of cyber security across an institution.

Higher education institutions present particular cyber security challenges. They rely heavily on digital data both for the smooth operating of the institution as an enterprise and for generating complex, valuable and at times sensitive digital research data. Furthermore, universities carry out a wide variety of activities and often do not have traditional organisational boundaries associated with more conventional enterprises. In light of this universities have to develop cyber security models that target appropriate and proportionate security controls at vulnerable assets.

Based on the work undertaken to date it is our belief that the technical expertise to implement proportionate controls to different parts of networks is already largely available to universities. However, the responsibility for effective cyber security extends across the whole institution. The main elements of developing cyber security in universities include:

- Assessing the institutional risk by identifying information assets, evaluating their vulnerabilities and establishing their management priorities
- Establishing effective oversight and reporting of information risks between the institution's board and the owners, controllers and users of information assets
- Implementing appropriate general and targeted network controls, including sharing and updating awareness of vulnerabilities and practices internally and externally

A significant challenge facing institutions is how to arrive at an informed assessment of the legal, reputational and financial risks posed by the different types of information that they hold, including research with potential economic value. We recommend that institutions consider devolved models of risk assessment and management that link to research data management policy and practice. These steps should aim to establish proportionate and appropriate controls that focus protections on high-risk information, whilst supporting the research and teaching practices that are central to the long term success of the institution.

Universities have to develop cyber security models that target appropriate and proportionate security controls at vulnerable assets.'

1. INTRODUCTION

As the importance of online technologies grows, effective cyber security is an essential element to the success of any organisation. This report looks at the growing challenge of cyber security and evolving approaches to implementing cyber security in higher education institutions.

The report is not written from a technical perspective. Instead, it looks at the management steps that are required across the whole institution in order to be cyber secure. It primarily focuses on the challenge of protecting against targeted, unauthorised attempts to access digital information, including research. The report looks at approaches to evaluating these risks and how these should inform the development of risk based management of cyber security across an institution.

The UK Government's National Cyber Security Strategy (HM Government 2011) reflects the central role that online networks play in facilitating many aspects of economic and personal life and the commensurate need to maintain confidence in the security of these systems. The strategy reflects the growing range of general criminal threats alongside increasingly systematic attempts by overseas states to gain economic, military and political advantages through the theft of information online. The strategy identifies universities as a strategic and valuable asset, reflecting the wide ranging economic contribution of UK universities. As a result, it is important that the UK higher education sector understands and addresses this challenge.

This report builds on prior briefings given by Universities UK to its members (UUK 2012b). It explores the challenges that institutions will need to address as part of the process of becoming more cyber secure. In particular it looks at the risk management issues that are raised by the cyber security threat in the context of the organisational structures, cultures and policies of higher education institutions. It does not provide technical network security guidance but highlights how practice is evolving to fit the needs of universities. The report is based on a series of roundtables and conversations held during 2013 with security services, academic centres of excellence in cyber security, directors of IT, registrars and pro-vice-chancellors for research.

Based on this work, it is our belief that the technical expertise to implement proportionate and targeted network controls is largely available to universities. However, responsibility for effective cyber security extends across the whole institution. A particular challenge for universities is developing informed assessment of the legal, reputational and financial risks posed by the different types of information that they hold. We recommend that institutions consider devolved models of risk assessment and management that link to research data management policy and practice. Measures should establish proportionate and appropriate controls that focus protections on high-risk information, whilst supporting the research, teaching practices and cultures that are central to the long term success of the institution.

It is our belief that the technical expertise to implement proportionate and targeted network controls is largely available to universities.'

2. THE CYBER SECURITY PROBLEM FACING UNIVERSITIES

Universities face a variety of cyber security threats. These include disruption to the functioning of a university network, through to more general and targeted attempts to obtain valuable information from networks and their users. Universities also face a growing challenge from advanced, persistent and targeted threats that reflect the sector's important contribution to innovation and economic development in the UK and beyond.

Effective management of these various threats is increasingly central to the success of organisations across every sector, not just higher education.

Given the diversity of activities that university networks support, this report primarily focuses on the challenge from more targeted attempts to obtain potentially valuable information from universities. The importance of developing effective approaches to this challenge for universities is commensurate with the importance of digital data to their work. Digital information is at the core of almost all of a university's activities and the safety and security of this information is important for a number of reasons:

1. Universities produce data as a core intellectual asset that needs to be stored, accessed and used appropriately to fully realise its academic or commercial value. This might include data produced for commercial contractors or which has commercial potential, through to politically sensitive data, such as economic or climate modelling.

2. Universities rely on access to sensitive data from third party organisations, such as patient-identifiable data or other clinical data that is provided from medical institutions. Universities may also rely on access to data provided by businesses or other bodies that is considered commercially, operationally or personally sensitive.

3. Universities collect data associated with their enterprise, such as information about students, staff or finances. Data might be considered sensitive by the law, the providers of data or where it informs decision making, such as marketing and recruitment data or, potentially, analytics from virtual learning environments.

As the importance of digital information has grown so has the need to ensure that data is protected from potential corruption, destruction or theft. However, security in all organisations is a trade-off between the likelihood and potential impact of threats and the various costs that are incurred to defend against them. Furthermore, in the case of large, complex organisations like universities, different types of activity may involve different types of risks, management priorities, and associated security measures.

The cyber threats facing universities are varied. There are a variety of general threats to a network and its infrastructure, such as through distributed denial of service attacks that may directly or indirectly target an institution's network. General criminal and fraudulent threats target users in order to obtain personal data for identity fraud. There are also increasingly targeted attempts to obtain potentially sensitive data from organisations. This may include personal data of students or staff held by the institution or certain types of information, such as research, for commercial or political means.

Table 1: Types of threats

Advanced state and corporate threats	Theft of sensitive corporate data for competitive advantage Theft of sensitive corporate data	Theft or damage to valuable research and data
'Hacktivist' and criminal threats	Disruption of infrastructure – eg overloading of websites	Theft of sensitive personal data for fraud or political purposes

The sharing of information on cyber security threats and breaches can be highly sensitive. In order to illustrate the nature of attacks and solutions that can be employed to prevent them, the Department for Business, Innovation and Skills (BIS) and the security services are compiling a composite case study of previous attacks on UK higher education institutions. In addition there are also details in the public domain of general trends around different types of threats (Context Information Security 2012, Mandiant 2013). These illustrate a pattern where persistent threats gain remote access to networks and systems and may remain there for a period of time identifying and taking, or damaging, valuable information.

Examples also illustrate that cyber security vulnerabilities are caused by a combination of the technical and human elements of a system. Technical elements may include software vulnerabilities that allow unauthorised access through a particular program. However, security failures are often traced to various forms of user vulnerability. Legitimate users may be targeted by social engineering that encourages them to take certain actions or divulge information that will allow attackers access to systems. Persistent remote access may also be achieved through unauthorised physical access to networks, such as through unsecured removable media like laptops or mobile devices.

The primary risk from the different types of cyber threat is to the business continuity of the institution; that is to say, theft of information or damage to networks may have immediate impacts that prevent the university and its community from going about their work. Institutions or researchers may lose access to essential data or that data may become corrupted. However, information may also be stolen, including without the owner's knowledge, with eventual costs not realised until later.

This may have a number of implications, for example:

- **Reputation**: information theft and integrity issues may severely harm a university's reputation in the eyes of students, partners, businesses and governments.
- **Legal**: theft of information may leave institutions in breach of legislation or contracts and at risk of prosecution, penalties and withdrawal of existing and future funding.
- **Economic**: theft of information may directly undermine a university's or researcher's ability to capitalise on potential intellectual property or knowledge transfer.
- **Operational**: there may be immediate damage to networks and infrastructure that prevents or hinders an institution's activities and results in significant remedial costs.

The extent of the threat to institutions is growing in line with the growth in digital information, and the size, complexity and portability of the systems they are stored on. The breadth of organisations that are being targeted is also increasing, with small and large organisations affected by costly security breaches (BIS 2013). However, using figures to illustrate patterns of cyber security threats is complex. Observed patterns may be heavily influenced by levels of legitimate usage as well as by the capability to identify and track threats. Furthermore there can often be a reluctance to share information on attacks, particularly where networks have been compromised.

Cyber security represents a complex and evolving challenge for government, industry and higher education. The main challenge for all is developing

The extent of the threat to institutions is growing in line with the growth in digital information.'

appropriate security measures and practices that reflect their organisational models and priorities. The development of effective solutions will be dependent on cooperation between all three sectors. Based on Universities UK's work to date we have identified three broad and essential steps for universities to consider as part of the development of their cyber security strategies. These are:

- assessing the institutional risk by identifying information assets, evaluating their vulnerabilities and establishing their management priorities
- establishing effective oversight and reporting of information risks by the institution's board and the owners, controllers and users of information assets
- implementing appropriate general and targeted network controls, including sharing and updating awareness of vulnerabilities and practices internally and externally

Further details of these steps are set out in the following chapters.

3. ASSESSMENT OF INSTITUTIONAL RISK

Institutions need to develop a considered assessment of their own risks in order to implement targeted security measures that optimise the value of their digital information.

An institutional approach to risk assessment will have to identify and assess data assets and their risks. A cyber risk assessment process should take into account:

- What information is considered critical by the university
- What information might be of interest for criminal, political or economic purposes
- How and where information can be accessed legitimately and illegitimately
- The controls and policies that manage access to and usage of data

It is essential for this risk assessment process to be embedded in data and research governance to enable risk management decisions that establish an appropriate balance between:

- The cyber security risk, including the likelihood, nature and potential impact
- Data management priorities, including access, users and publishing lifecycle
- The costs of implementing controls, including resources and indirect costs

The process of assessing risk requires partnership between the corporate entity that bears some of the cost of security failures, and the researchers and administrators who have responsibility for collecting, managing and publishing data. In many instances assessment of risk may be driven by the holders of data, such as researchers or administrators who have to meet data management requirements set by funders or the law, or are in a position to identify potential economic benefits. However, as the corporate entity also carries legal, reputational and financial risks it is essential that it is an active partner in the assessment process.

A shared understanding of risk management priorities is necessary otherwise security controls risk being undermined by unintended effects on practice. In particular, if a risk threshold is set too low an institution runs the risk of overly restricting practice at substantial cost to the detriment of the research and use process. Overly restrictive processes may also encourage risky behaviours that minimise the perception of risks during assessments or encourage risky behaviour to work around restrictions to improve usability. As a result, assessments also need to take into account variations in data management priorities and risks across the institution's different functions.

Cyber security risk assessment

Institutional cyber security risk assessment should:

- establish a shared understanding of threats and risks across the institution
- identify and evaluate information assets for their potential cyber security risk
- enable proportionate targeting of security resources and practices
- account for different security and management needs of data and users
- be iterative throughout the evolution of data risks and management priorities

Identifying information assets

Identifying potential information assets is an essential first step in the process of developing proportionate responses. Critical information includes information that is considered essential by the university or researchers and would present a significant operational risk if it was lost or accessed and used without authorisation. Information comes in many different forms and may be collected in highly decentralised ways. Three processes for identifying information assets are:

- Data that has been subject to **ethical approval**: These risks are primarily linked to an institution's ability and reputation for maintaining appropriate standards of research practices and management. *The concordat to support research integrity* (UUK 2012a) recommends that research in institutions should be governed by clear policies, practices and procedures to support researchers and be implemented through robust management systems.
- Data that is subject to **legislative or contractual protections**: The principal legal framework for cyber security is the Data Protection Act (1998). All institutions are recognised as data controllers under the Act and should be fully aware of their responsibilities (Jisc 2008). The Act places legal requirements on organisations processing personal data with a variety of penalties for potential breaches. Data requirements may also be included through contracts, in some cases linked to the Act or where information is commercially sensitive.
- Information with potential **economic or political value**: Identifying this presents possibly the greatest challenge to institutions. Although many researchers will be aware of the potential commercial or political value of their work, institutions may not have established dedicated processes to identify these kinds of data. However, research data management and knowledge transfer policies provide potential avenues for identifying these types of assets.

Only certain types of data will be considered an asset by the institution for the purposes of cyber security and more in-depth risk assessment can reasonably be targeted at those areas that are most likely to be considered higher value and higher risk. There may be a base line of good handling practice applied for categories of digital research and enterprise information. Items that are covered by legislation or contractual arrangements may be reviewed for minimum handling and security standards. However, this process will likely need to identify information assets that are not directly covered by legislative, contractual or immediate operational risks, in order to evaluate the appropriate security and handling response.

Evaluating the external threat to assets

It is essential that risk assessment enables appropriate and proportionate targeting of security resources. As part of this, risk assessment should assess the likelihood that different data assets may be targeted by external threats, and the degree of sophistication that these threats represent. As the priorities and capabilities of external threats can and do evolve it is not possible to provide a comprehensive analysis of areas that may be targeted. In light of this, it is important that any risk assessment is informed by up-to-date information on evolving threats, through information sharing and advice services.

Nevertheless, when reflecting on the types of information that may be most at risk from targeted threats, a number of broad categories can be identified:

a. Research with potential economic value, such as:

- Energy technology, including nuclear, renewables and efficiency
- Biotechnology, including drugs, treatments and devices
- New materials, such as rare earths and semi-conductors
- Information technology, including security and infrastructure technologies
- Advanced engineering, such as aerospace and telecoms

b. Politically and commercially sensitive information, such as:

- Climate modelling
- Economic data and projections

The Centre for the Protection of National Infrastructure

As part of the National Cyber Security Programme, the Centre for the Protection of National Infrastructure (CPNI) is working with the UK's most economically important companies and a selection of academic institutions to improve awareness of the cyber threat and provide protective security advice to mitigate the associated risks.

For those institutions assessed to be most exposed to the threat, CPNI is assisting them to assess their risks including the types of research that are of particular economic or political interest, the methods that are being used to obtain information, and an institution's vulnerabilities. Further information and advice relevant to all universities is available on the CPNI website, www.cpni.gov.uk

- Live animal research
- Product development and testing data
- Information used for expert testimony

c. Sensitive enterprise data, such as:

- Staff data, especially when engaged in controversial or valuable research
- Student record data
- Financial data
- Recruitment and marketing data

The threats associated with the different types of data that an institution works with may vary in their frequency and sophistication. All data is at risk of loss through handling failures such as poor storage policies and practices. Enterprise data and processes may be targeted by criminal gangs or by 'hacktivists' and other political actors who may attempt to steal data or disrupt networks to the detriment of normal business functions. These types of attacks may be highly frequent and can be increasingly sophisticated. Highly advanced threats that are typically associated with corporate or state espionage may be less frequent but are increasing in volume, and can represent a more targeted and pervasive threat to commercially or politically valuable research.

Establishing management priorities

Risk management should be alert to the different ways in which information is vulnerable as it is stored, accessed and used. Risk assessments should then target measures at data that may be particularly sensitive. For example, some types of patient-identifiable data may be subject to relatively low active external threats. However, it may require high handling standards to avoid accidental loss and ensure the confidence of the third parties that own data, such as the NHS. Alternatively data with potential commercial value may be particularly valuable but as it has not been subject to external handling standards may be particularly vulnerable to external threats.

Risk assessment should enable proportionate targeting of security according to the use needs of the information. In cases where a high priority is placed on exchange and access to information there are greater opportunities for users to inadvertently, or even deliberately, compromise the integrity of systems or information. However, measures that seek to attain high levels of security to prevent even deliberate attempts to compromise networks and data incur both direct and indirect costs. In light of this, highest security should be targeted at those assets that are of greatest value to the institution, and where the vulnerability to external threats is high.

Evaluation of risk should also take into account any evolution of the data's vulnerabilities and how its handling priorities may evolve throughout the information lifecycle. A key consideration is the balance between the accessibility of data for the purposes of analysis whilst addressing security concerns. For example, during the creation and use phases, data may need to be secured against theft to protect potential commercial benefits, but in a way that balances the need for access across multiple sites. However, after publication the priority may be to archive data for future reuse. This may include assessing the security needs of specific elements, such as patient-identifiable data, or where licensing arrangements may require some usage restrictions (see Figure 1).

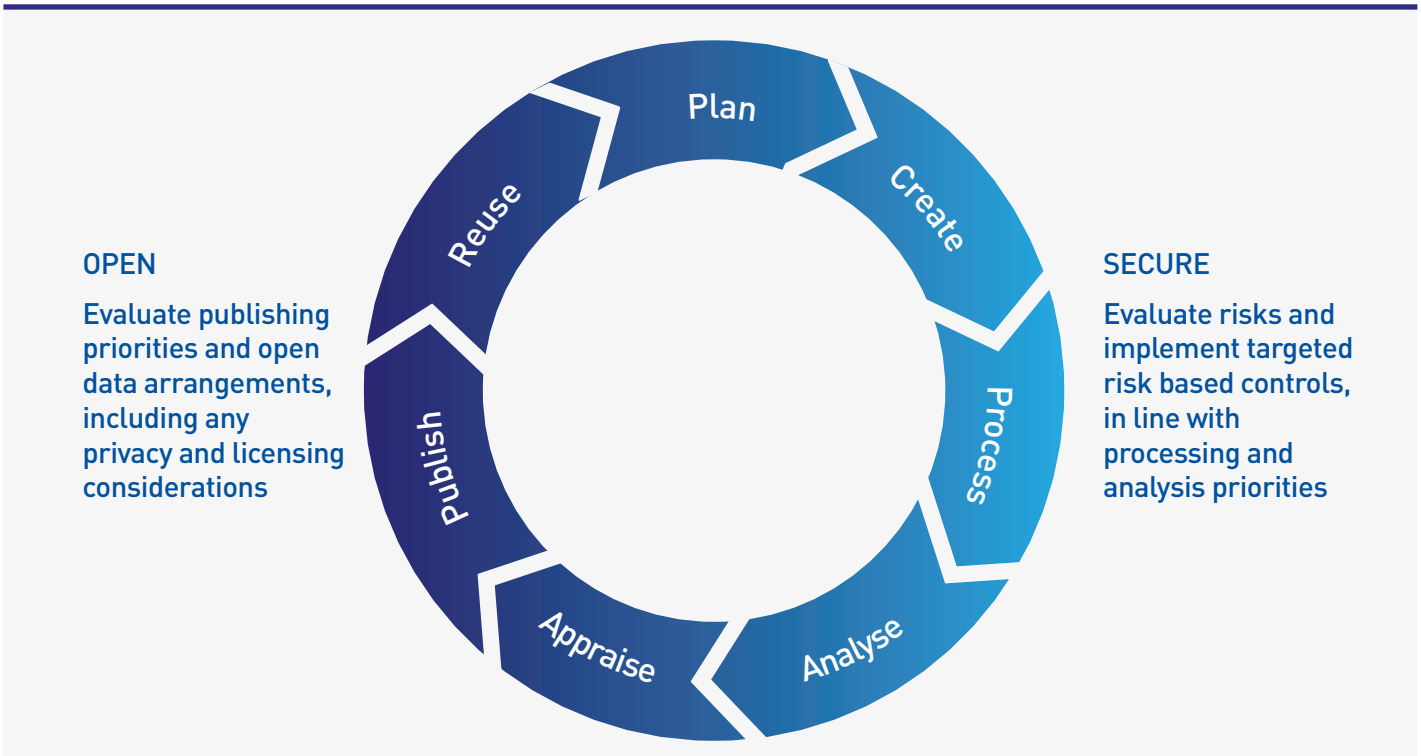
Balancing cyber security with openness

Security is about effective management that protects data from the threat of unauthorised access, loss and corruption. As the eventual goal of most research activity is publication, there would likely be fewer or different security measures needed after this point. Furthermore, the shift toward open data also indicates a trend where raw underlying data is made more openly available, with appropriate licensing, for reuse by third parties to increase its utility. The shift to open data illustrates the need for appropriate data management practices throughout the lifecycle so that data is effectively maintained and published in order to be reused by others. However, as illustrated earlier in this report, there will continue to be legal imperatives to secure certain types of data post publication.

Security and openness may be approached as two themes in the same data management and risk assessment process. Effective risk assessment should enable an institution to identify appropriate handling and security approaches throughout the lifecycle of the different types of information that are produced and used by an institution. The process should include assessment of management priorities, security risks, appropriate access controls, and publishing arrangements and storage infrastructure. An integrated approach could enable an institution to approach cyber security and open data, as well as knowledge transfer, with confidence, in the knowledge that the data is appropriate for reuse by third parties.

In some respects the shift toward open data illustrates a wider trend of value shifting away from ownership of information toward what is done with it. This shift may seem to negate some of the imperatives of cyber security by encouraging wider access to data. However, as open practices are typically applied at certain points during the production or completion of data sets, and sometimes in qualified ways, there remain opportunities for theft, appropriation or tampering that may subsequently damage the future value of the data. Furthermore, where an information lifecycle includes both secure and open elements, it may be increasingly important for institutions and researchers to appraise potential commercial opportunities earlier, during secure phases, and link with knowledge transfer policies.

Figure 1: Balancing management priorities through the data lifecycle



4. IMPLEMENTING CYBER SECURE INFORMATION GOVERNANCE

Higher education institutions should implement corporate approaches to managing their cyber security risks as part of existing governance structures. Institutional boards should take ownership of the cyber security risks facing institutions.

Institutions should consider who in an institution 'owns' or 'controls' data in order to establish clear lines of assessment, accountability and monitoring between the decentralised production and use of data and the institution that shares the costs of security failures. Institutions should also conduct internal and external audits of their risks, management priorities and systems.

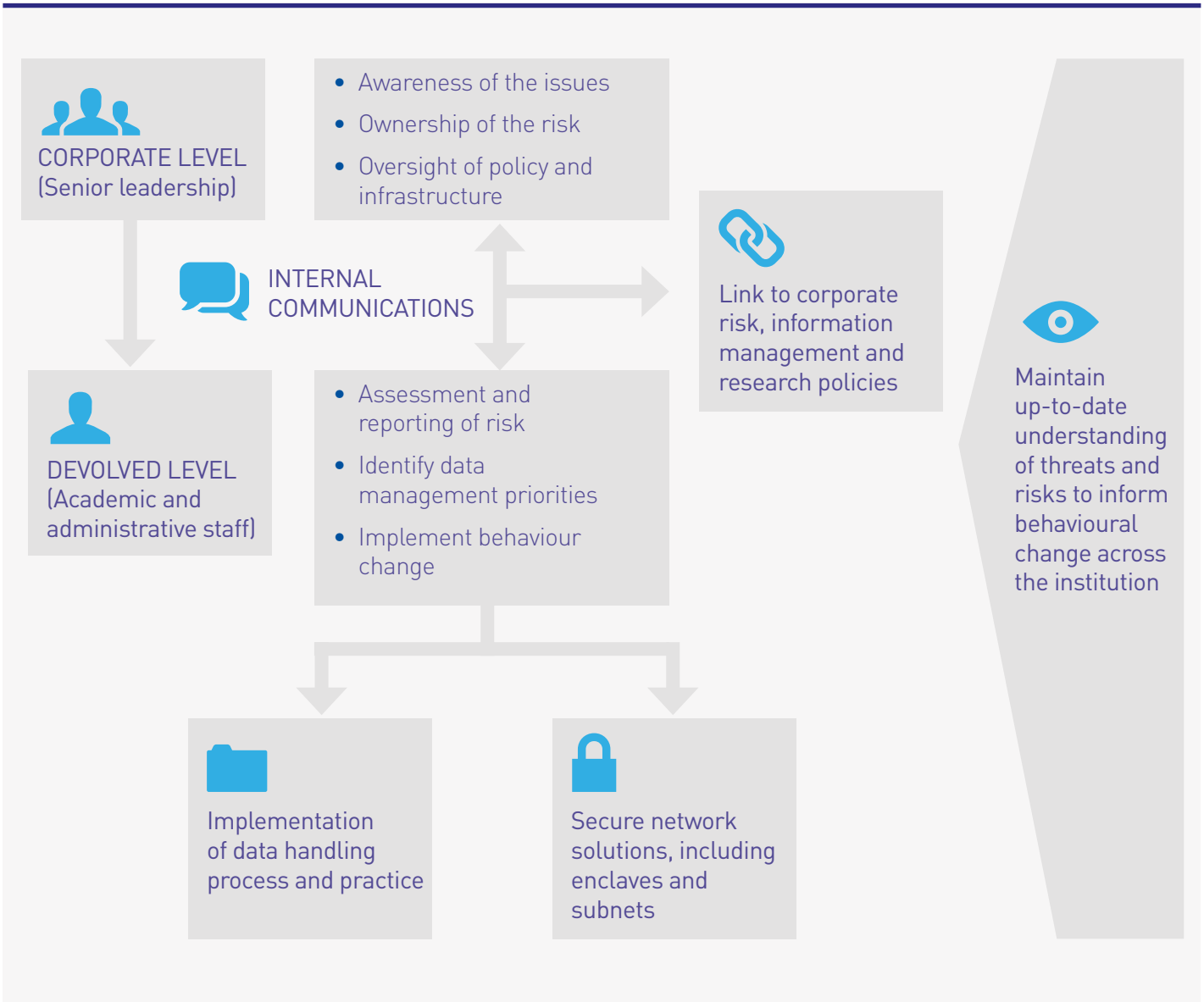
The identification and targeting of security controls at certain types of data can only be achieved with the active involvement of controllers of data. These groups are best placed to identify assets, assess which types of controls will be most appropriate, and will ultimately be responsible for maintaining the integrity of systems and data. The executive team reporting to the vice-chancellor typically owns much of an institution's corporate data, although data will also be held by academic schools and tutors. In the case of research, principal investigators and deans of schools may primarily be responsible for controlling data. As a result it is important that they play a central role in deciding an institution's appetite for risk and the identification and evaluation of information assets.

Ultimately, network security is a responsibility for the whole institution. Network administrators and defenders can maintain up-to-date knowledge of

Table 2: Implementing cyber security – overview of roles

Objectives	Function	Role	Target groups
Awareness	The whole institution	Need appropriate levels of understanding of the threats facing the university and the measures that have been put in place.	All staff, students, leaders and trustees
Oversight	Governing councils and executive groups	Include cyber security on risk rosters at an appropriate level so that a practical oversight at corporate level is maintained.	PVC research & enterprise, registrars and deans/ heads of schools
Assessment	The controllers of data and networks	Should own the day-to-day responsibility for assessing, managing and reporting risks appropriately.	Heads of schools, principal investigators, registrars, directors of IT
Securing	Data users & controllers, network controllers &	Should possess the up-to-date information on their responsibilities and the evolving threats and risks that they should be alert to.	Research groups, administrators, heads of network security
Implementation	All users	Should be in accordance with policies and procedures and given awareness and technical training where necessary.	All staff and students

Figure 2: Process model for managing cyber security threats in higher education institutions



threats and counter measures through exchange of information with peers and with government agencies. However, it is users who are crucial to the security of any network and information. They must play a central role in evaluating the risk facing information, setting management and security priorities and ultimately, as users, are responsible for the implementation of controls. In light of this it is essential that network users, from general users to those dealing with more sensitive assets, are aware of and act on their responsibilities.

Ultimately, network security is a responsibility for the whole institution'

Corporate governance

All institutions should be aware of their duties regarding the protection of personal and financial administrative data and have appropriate measures in place to ensure that they are compliant with the Data Protection Act (1998). However, institutions will have different structures for the management of data and research, and appropriate levels of oversight. Furthermore, institutions and researchers are likely to have developed a variety of data management policies and plans, often with very little corporate oversight. These features present a challenge for corporate governance to understand both the issues and the approaches that can be employed to help develop cyber security practice in their institution.

Effective corporate cyber security needs to take into account the devolved structure of managing data whilst also accounting for the institution-wide risk that may be associated with any management failures. Corporate oversight of risks inevitably relies on communication from and management by those with responsibility for controlling data. An oversight function may be integrated into existing research approval processes; however, these may need to be adjusted to take into account potential economic risks in addition to ethical, legal and contractual requirements. When setting policy, corporate governance should seek to establish clear answers to the following questions:

- What information does your institution, the law, funders or partners consider sensitive?
- Who owns or controls data within the institution?
- How should the management priorities for data be established?
- What are the channels for monitoring and managing cyber security risks?

Recommendations for corporate governance

- ✓ Consider establishing a dedicated governance committee to maintain oversight of institutional data management and cyber security risks.
- ✓ Consider conducting an institutional assessment of cyber security risks and data management priorities covering existing and new assets.
- ✓ Ensure there are clear channels of communication and reporting between controllers of data and corporate governance on risks and management priorities.
- ✓ Consider the role of internal and independent audit to assess corporate governance and management of cyber security, including beyond legal responsibilities.

CASE STUDY

Information management committees

A number of institutions are exploring establishing dedicated governance committees with responsibility for oversight of data risk management.

These include oversight of data protection responsibilities, cyber security measures and research data management. For example, the University of Oxford's Oxford Digital Repositories Steering Group has held responsibility for oversight of the university's federated data management programme since 2007. The steering group comprises key stakeholders from across the university and is responsible for oversight of the institution's research data management strategy, including provision of support and guidance around research data management and security.

Research data management

Cyber security is one part of the wider agenda of improving digital data management and publishing practices in institutions. Research funders are increasingly stressing the importance of sound data management practice to improve the quality of research. All of the funding councils require data management plans from the outset of research programmes. The Higher Education Funding Council for England's proposals to include open data requirements as part of future research evaluation frameworks will also increase the need for effective data management throughout the data lifecycle. In response, many institutions are reviewing their approach to data management and the support that is provided to researchers to manage and maintain their digital data sets safely, securely and accessibly.

Measures to improve the security of data within institutions should aim to work within evolving data management policy and support structures. Policy should aim to enable researchers to effectively manage research data in such a way that it can be presented in open access repositories or have the appropriate security controls in place as the management priorities of data evolves. In particular, research funder requirements often refer to key security standards when setting conditions for handling their data. For example, data management checklists used as part of the design of project data management plans, such as the one set out by the Digital Curation Centre, can be used to feed into cyber security risk assessments for new projects.

Institutions will also need to consider audits of existing data to identify potentially sensitive data and assess their risks and management priorities. The objectives for the audit should be made explicit to all those involved in identifying and assessing risk and should cover security considerations as well as wider data management policy and practice priorities in order to support researchers in their work. The parameters of any audit would need to be carefully defined to ensure that only relevant data is included in the process. In light of this an audit may consider focusing on assessment of a range of significant research data sets and the nature of existing management practices, with a view to informing more comprehensive policy and practice.

Recommendations for research management

- ✓ Develop a light touch audit and assessment framework to evaluate risks and data management measures for existing data.
- ✓ Review data management plans as part of ethical review and ongoing research governance processes to assess potential security risks and management priorities.
- ✓ Require security considerations to be included in data management plans for all new research proposals.

CASE STUDY

Research data management policy

As part of the development of improved institutional approaches to digital data management the University of Edinburgh conducted an audit of its data to assess current management and storage needs.

This was the first step toward institutional data management planning and practice that is improving the infrastructure and support available to researchers across the university. The sampling approach that was adopted by the audit could be adapted to target those research areas that might be considered at most risk.

Network security

As universities are complex organisations without traditional enterprise and network parameters, security measures should be targeted according to their risk and management priorities. Segmented approaches to network security enable higher levels of security to be applied to data that has been identified as high risk and high value. Security practices may involve improved base line controls, dedicated network controls or in some cases physical control of access to certain locations. In all cases controls need to take into account the management priorities for data, including the security and protection requirements and the costs of measures, including impacts on the usability of data.

A model is developing whereby network security teams establish a centralised secure data store with associated policies and technologies that meet information handling and security standards. To date examples have primarily focused on providing safe storage for patient-identifiable data and census data, but they may transfer to other high-risk, high-value areas. These initiatives provide services to researchers that raise security standards and streamline practice. Where data management has to meet external requirements these services can facilitate access to sensitive data and research funding. However, these practices also have downside costs, including resource and accessibility issues that will require careful assessment when protecting other types of data.

Institutions also need to design measures in accordance with rapidly evolving cyber security threats. This process of continual review and updating of practice should feed into wider institutional risk assessment and governance processes. In addition to support from higher education organisations such as Janet and the Universities and Colleges Information Systems Association (UCISA), government agencies offer services to help institutions. In particular the government has established the Cyber Security Information Sharing Partnership (CISP) to improve the exchange and monitoring of information about evolving cyber security threats and targets across industry and higher education. Where an institution has concerns about the risks it faces and effective methods of protecting data it should stay up to date with information from CPNI on appropriate security controls.

Recommendations for targeted controls

- ✓ Ensure that network and information services are in a position to provide support and develop policies and controls for sensitive information.
- ✓ Segment and focus controls proportionately through techniques such as secure network areas or enclaves and virtual private networks.
- ✓ Join the CISP and regularly review the Centre for the Protection of Critical Infrastructure's 20 critical controls to stay up to date with evolving threats, targets and security standards.
- ✓ Work with sector groups such as Janet and UCISA to stay up to date with evolving network security issues and practice in the sector.

CASE STUDY

Secure network enclaves

University College London has implemented a dedicated system for securing patient-identifiable data.

The Identifiable Data Handling Solution (IDHS) is a centralised data store that provides researchers with a validated location to store data rather than relying on individual teams to set up their own systems. It is primarily targeted at life sciences and is designed to secure data and facilitate access of data held by external partners, namely hospital and other medical partners. In light of this it meets International Organization for Standardization (ISO) standards and the NHS toolkit as well as a number of other major funder requirements.

The system has been set up in close conjunction with heads of schools to ensure that there is awareness and cultural change around the use and storage of data and is run in conjunction with advisory and training services on data management and security. The model is targeted at patient-identifiable data given the clear need for high levels of data safety but could be transferred to other areas where data management priorities and risks require higher levels of security. Alternatively, high-risk data may be held off conventional networks, in secure physical locations.

The Cyber Security Information Sharing Partnership

The Cyber Security Information Sharing Partnership (CISP) is a joint, collaborative initiative between industry and government to share cyber threat and vulnerability information in order to increase overall awareness of the cyber threat and therefore reduce the impact on UK business.

The CISP uses a dedicated online collaboration environment to allow government and industry members to share cyber threat and vulnerability information at pace whilst operating within a framework that both protects and respects the confidentiality of any shared information. UK universities are eligible to join the CISP collaboration environment. Further guidance for universities on joining and using the CISP can be obtained via Universities UK (UUK 2013) or directly from the CISP team via their website, www.cisp.org.uk

Culture and behaviour change

The security of systems is dependent on the people that use them. Effective institutional assessment of risks and implementation of secure practices rely on a shared understanding of the threats and challenges facing the institutions. All networks should have use policies that should be understood and implemented by all users. UCISA and Janet have various policies and guidance documents on good practice that can be referred to and adopted. In addition, institutions need to consider how to develop the culture and awareness of staff, particularly those with responsibility for handling and managing potentially risky data. These initiatives can be built into wider staff and researcher development, including alongside more general data management skills and practices.

Recommendations for for developing cyber secure cultures

- ✓ Ensure close liaison between heads of schools, principal researchers and network services to ensure shared understanding of risk and solutions.
- ✓ Establish data champions in schools and departments to encourage understanding of the potential threats facing data.
- ✓ Consider rolling out communications and training programmes with research staff, including integrating data management practice into doctoral training programmes.

CASE STUDY

Cyber security training and development

Universities should consider how they embed knowledge of cyber security practice and responsibilities across their institution.

This ranges from requiring annual active confirmation of acceptance of terms and conditions of using the network or certain parts of it, through to training and education programmes. The 2011 UCISA Award for Excellence went to the University of Leicester, which led a consortium of universities that developed an Online Information Security Training for higher education institutions. Janet also provides a number of security-related courses for IT staff.

5. CONCLUSION

The cyber security threat is a complex and significant challenge that is likely to continue to grow. Institutions need appropriate governance and management systems in order to develop proportionate measures that protect sensitive information.

To achieve this aim, institutions should consider developing a devolved cyber security risk management model that enables them to come to a corporate understanding of risk that relies on assessment and management by those who have ownership of the data. These systems should ensure that an institution:

- Is able to identify, evaluate and monitor cyber security risks
- Inculcates effective and secure data management practices and attitudes
- Implements and maintains appropriate network controls, including general and targeted security measures
- Works with the CISP, CPNI and Janet to understand and manage the cyber security risks it faces

Ultimately, effective security is the responsibility of the whole institution. Effective security measures rely on active collaboration between governing bodies, data controllers, network defenders and network users. Furthermore, active collaboration between institutions, government and industry will help all to keep abreast of the rapidly evolving threat and enable institutions to prepare and protect themselves. By achieving an effective and proportionate approach to managing cyber security, institutions will be able to maintain internal and external confidence and continue to develop their core research and teaching missions safely and securely in the digital age.

Active collaboration between institutions, government and industry will help all to keep abreast of the rapidly evolving threat and enable institutions to prepare and protect themselves.'

ANNEXE A: BIBLIOGRAPHY

Department for Business, Innovation and Skills (2013)
Information security breaches survey, technical report
https://www.gov.uk/government/publications/information-security-breaches-survey-2013-technical-report (accessed 7 November 2013)

Context Information Security (2012)
Crouching Tiger, Hidden Dragon, Stolen Data
http://www.contextis.com/files/Targeted_Attacks_Whitepaper.pdf

HM Government (2011)
The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world
https://www.gov.uk/government/policies/keeping-the-uk-safe-in-cyberspace#background

Jisc (2008) Code of Practice for the Further and Higher Education Sectors on the Data Protection Act 1998
http://www.jisclegal.ac.uk/Portals/12/Documents/PDFs/DPACodeofpractice.pdf

Mandiant (2013)
APT1: Exposing One of China's Cyber Espionage Units
http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

Universities UK (2012a)
The concordat to support research integrity
http://www.universitiesuk.ac.uk/highereducation/Documents/2012/TheConcordatToSupportResearchIntegrity.pdf

Universities UK (2012b)
Policy briefing P-2012-10: 'Cyber security – protecting universities from the cyber threat'
http://extranet.universitiesuk.ac.uk/Publications/PolicyAnalyticalBriefings
(access for UUK members only)

Universities UK (2013)
Policy briefing P-2013-08: 'Cyber Security Information Sharing Partnership (CISP)'
http://extranet.universitiesuk.ac.uk/Publications/PolicyAnalyticalBriefings
(access for UUK members only)

ANNEXE B: ORGANISATIONAL STANDARDS FOR CYBER SECURITY

There are a variety of organisational standards and guidance for boards on implementing cyber security. The government has published a series of guidance documents, including *10 Steps to Cyber Security* and its executive companion. These documents clearly set out the need for corporate governance to prioritise the issue and the steps that they can take to ensure that their organisations are protected. The government also plans to identify a preferred cyber security standard to clarify basic organisational standards and expectations around cyber security.

Although the 10 steps are designed as generic guidance to cover a variety of organisations, the vast majority of it is transferable to higher education institutions. However, there are features of higher education institutions, including their devolved structures and the wide range of education and research missions, which require careful consideration when implementing any security standards or models. Boards are advised to consider this guidance, alongside their existing responsibilities, under the Data Protection Act (1998).

Organisational standards for information security provide frameworks for assessing organisations' governance and information handling measures. In order to bring greater clarity for organisations the government is to identify a preferred organisational standard. The selected standard will primarily be a basic security standard for the protection of enterprise data that is often comparable across different industries, although it will also be applicable to research data protection. BIS is scheduled to announce the preferred standard at the end of November 2013, when further details will be made available on its website.

The Centre for the Protection of Critical Infrastructure (CPNI) publishes 20 critical controls that can be used as a base line for high-priority information security measures. The controls focus on various technical measures and activities, with the primary goal of helping organisations prioritise their efforts to defend against the current most common and damaging computer and network attacks. Further details of the critical controls can be found at:
http://www.cpni.gov.uk/advice/cyber/Critical-controls/

An adapted version for universities has been developed by the Russell Universities Group IT Directors forum (RUGIT). This version looks at the different controls and how they may need to be amended for the different types of risks and data management priorities that are found across institutions. In particular, as university networks support a variety of activities, such as bring-your-own devices for students, or programming in computer science departments, it is essential that controls are applied appropriately to different parts of the network.

Cyber security guidance for boards:
https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility

20 critical controls for cyber security:
http://www.cpni.gov.uk/advice/cyber/Critical-controls/

ANNEXE C: RESEARCH DATA MANAGEMENT PRACTICE

Research councils and other funders typically set standards of information management and security as a condition of funding.

The Digital Curation Centre provides an overview of different policies and standards of research councils. Details can be accessed at: **http://www.dcc.ac.uk/resources/policy-and-legal/overview-funders-data-policies**

Standards commonly referenced by significant funders and other research partners include:

- **ISO/IEC 27001 requirements for information security management systems**. This is a high level standard for identification and control of information risks but it does not specify particular risks or measures. The Universities and Colleges Information Systems Association (UCISA) has produced a toolkit containing sample policies for each of the standard's areas, which has been used by a number of institutions (see **www.ucisa.ac.uk/IST**).
- **NHS Information Governance Toolkit**. This is typically referred to when handling patient-identifiable data, and meeting standards is an important requirement for institutions that want to work with patient-identifiable and other clinical data. Further details on information governance for the NHS and partner organisations can be found at **http://systems.hscic.gov.uk/infogov**.

There are also a number of tools and resources to help institutions and researchers assess if adequate infrastructure, staff skills and resources, and senior management support are in place to ensure that data is effectively managed for validation, reuse and evidential purposes.

CARDIO self-assessment tool

CARDIO is a benchmarking tool for data management strategy development, typically applied at the departmental or research group level. It allows groups to:

- collaboratively assess data management requirements, activity and capacity
- build consensus between data creators, information managers and service providers
- identify practical goals for improving data management provision and support
- identify operational inefficiencies and opportunities for cost saving
- make a compelling case to senior managers for investment in data management support

Data Asset Framework

The Digital Curation Centre (DCC) has developed the Data Asset Framework (DAF; formerly the Data Audit Framework), which enables organisations to identify, locate, describe and assess how they are managing their research data assets. The DAF combines a set of methods with an online tool to enable data auditors to gather this information. It will help ensure that research data produced in UK higher education institutions is preserved and remains accessible in the long term. Further information about the DCC's Data Asset Framework can be accessed at: **http://www.dcc.ac.uk/resources/repository-audit-and-assessment/data-asset-framework**

DCC data management plan

The DCC also sets out a checklist for developing data management plans that includes security considerations from the outset. It asks:

- What are the risks to data security and how will these be managed?
- How will you control access to keep the data secure?
- How will you ensure that collaborators can access your data securely?
- If creating or collecting data in the field, how will you ensure its safe transfer into your main secure system?
- What information standards do you need to meet?

Some institutions are also providing data management training to researchers that covers data security elements. For example, the MANTRA research data management training programme is a free, non-assessed course with guidelines that is aimed at improving data management awareness and skills for researchers and includes some basic components on storage and security practices. The course is particularly appropriate for those who work with digital data. Further details are available at: **http://datalib.edina.ac.uk/mantra/**

JISC infoNet also has a number of resources relating to information management, available at: **http://www.jiscinfonet.ac.uk/topics/information-records-management/**

ANNEXE D: CASE STUDY INFORMATION

University of Edinburgh research data audit and policy
http://www.ed.ac.uk/schools-departments/information-services/research-support/data-library/research-data-mgmt/overview

University College London Identifiable Data Handling Service
http://www.ucl.ac.uk/isd/itforslms/services/handling-sens-data/tech-soln

Janet workshop report on secure network enclaves
https://community.ja.net/library/janet-services-documentation/protecting-sensitive-information-workshop-report

University of Oxford federated data management committee
http://www.ict.ox.ac.uk/odit/projects/datamanagement/

University of Leicester information security training
http://www.ucisa.ac.uk/~/media/Files/members/awards/excellence/2011/Leicester and **http://www2.le.ac.uk/offices/ias/is**

Janet cyber security training
www.ja.net/training

Universities UK

recycle
When you have finished with this please recycle it

This publication has been produced by Universities UK, the representative organisation for the UK's universities. Founded in 1918, its mission is to be the definitive voice for all universities in the UK, providing high quality leadership and support to its members to promote a successful and diverse higher education sector. With 132 members and offices in London, Cardiff and Edinburgh, it promotes the strength and success of UK universities nationally and internationally.

Woburn House 20 Tavistock Square London WC1H 9HQ

Tel: +44 (0)20 7419 4111

Email: info@universitiesuk.ac.uk
Website: www.universitiesuk.ac.uk
Twitter: @UniversitiesUK

ISBN: 978-1-84036-300-5

November 2013

To download this publication, or for the full list of Universities UK publications, visit **www.universitiesuk.ac.uk**