Universities UK

SEPTEMBER 2023

Cyber Security and Universities

Managing the risk (2023 update)

in association with National Cyber Security Centre

Jisc

Contents

Foreword

The UK's universities are proudly dynamic, diverse and international institutions, bringing together staff, students and visitors from across the globe throughout the year. This type of engagement is a key strategic asset to the UK. Open access to campuses and their associated sites is an important aspect of academic life that is necessarily built on a foundation of safe and secure online environments.

Universities have made good progress in developing processes that manage security-related risks. However, there is more to be done, and cyber security has never been more important. Connectivity and digital technology now underpin almost all aspects of running a university or research centre. This makes the security of our networks, data and people crucial. As leaders, we are ultimately responsible.

This guidance demonstrates the criticality of cyber security. It reminds us that because of the work we do and the data we hold, our sector remains an attractive target for all kinds of cyber criminals, from have-a-go opportunists to state-sponsored, highly organised groups.

It will also help us understand what we ought to be doing to reduce risk; how to prevent as many attacks as possible and how to mitigate the impact of those we cannot.

There is a balance to be struck, though, between the need for collaboration and access to data, and working practices that maintain security. The Trusted Research Guidance for Academia, developed by the National Cyber Security Centre (NCSC) and the National Protective Security Authority (NPSA), outlines the importance of this balance.[1]

This should not mean anyone faces barriers in carrying out their job, but we must find new ways for people to operate that do not put themselves, their colleagues, their work, or their employer, at risk. We must be firm and prepared to change how we do things, fostering a positive culture of awareness where security is on everyone's radar.

[1] https://www.npsa.gov.uk/trusted-research-academia

In short, good cyber security hygiene is dependent upon robust processes and policies and requires a commitment to significant ongoing investment, both in technology and in people with the specialist skills to implement and operate it effectively.

Security failures can have potentially catastrophic consequences, as Jisc's cyber impact report outlines.[2] Serious cyber attacks on higher education providers have resulted in massive disruption to teaching and learning and to business-critical systems, sometimes for long periods of time. This has obvious implications for reputational damage and for the wellbeing of staff and students. Cyber attacks also often incur very significant financial costs.

So, prevention is better than cure. Yes, the task is significant and complex, but we are not alone; our critical friends at Jisc, NCSC and Universities UK (UUK) are here to support us.

Jisc offers a range of cyber security services and expertise, as well as its guidance, '16 questions you need to ask to assess your cyber security posture', designed for boards.[3] This complements the NCSC's newly revised board toolkit, which includes an introductory video specifically for the higher education sector.[4] UUK also has a dedicated programme of work on managing security-related issues and has developed guidelines on Managing Risks in Internationalisation, including a chapter on protecting university students, staff, visitors and campuses from cyber security threats.[5] You will find details of all these resources within this guide.

Cyber security will be high on every university's risk register. By collaborating with expert organisations which provide advice and solutions, we can minimise the risk and provide reassurance to our governors that, while it is impossible to be immune to attack, we can be as well prepared as possible.

---

[2] https://www.jisc.ac.uk/reports/cyber-impact
[3] https://repository.jisc.ac.uk/8549/1/cyber-security-16-questions-checklist.pdf
[4] https://repository.jisc.ac.uk/8549/1/cyber-security-16-questions-checklist.pdf and https://www.ncsc.gov.uk/section/education-skills/cyber-security-heis-feis
[5] https://www.universitiesuk.ac.uk/topics/funding-finance-and-operations/security-and-risk-how-universities-can and https://www.universitiesuk.ac.uk/topics/funding-finance-and-operations/security-and-risk-how-universities-can

Introduction

The purpose of this document is to demonstrate to vice-chancellors and other board-level university leaders the strategic significance of cyber security.

Drafted jointly by sector experts from UUK, Jisc and the NCSC, with support from UCISA, this guidance also outlines the main threats facing the sector and the impact of recent attacks against individual organisations across the UK research and education sector, and sets out leaders' responsibilities to understand and mitigate these risks.

It provides action points to consider and more detailed advice around our suggested approach to cyber security. We suggest that leaders pass on this more detailed section of guidance to senior technical colleagues, such as chief information security officers or IT directors.

The four pillars of cyber security are governance, assurance, technology and culture:

- Governance relates to an organisation's overall approach to identifying and managing cyber security risks. A strategy should be in place, with policies, processes and resources to deliver it.
- Assurance activities include both internal and external review and audit. External review should be based on an appropriate framework, such as Cyber Essentials or ISO 27001, but compliance must be shaped by overall strategic goals, with external assurance providing confidence that processes, procedures, and controls are functioning as designed.
- Technology covers systems, services and infrastructure, including firewalls and two-step verification, also referred to as multi-factor authentication (MFA). Security should be embedded across all operations, working practices and configuration management.
- Culture describes an open, honest and transparent consideration and awareness of security across the entire organisation. With visible engagement and support and leadership from the top, all staff and students must receive training and feel supported to report, not hide, issues, incidents and concerns, so that everyone can benefit from the experience and support continual improvements.

This guidance complements Universities UK's 'Managing risks in Internationalisation: Security related issues', which sets out measures universities should take to guard against hostile interference and promote academic freedom, and the NCSC Board which facilitates discussions between boards and their technical experts.[6]

[6] https://www.universitiesuk.ac.uk/what-we-do/policy-and-research/publications/managing-risks-internationalisation and https://www.ncsc.gov.uk/section/board-toolkit/home

Executive summary

The UK's higher education sector is rightly regarded as one of the best in the world. A key contributor to that reputation is universities' open, collaborative approach to teaching and research activity. This activity is fundamental, but it also carries a degree of risk; universities and their data are valuable targets for cyber criminals. If data is not secured appropriately, there can be financial, reputational and personal consequences. 'Cyber security and resilience' is cited as a priority area in the UK government's overarching national security and international strategy, the 2023 Integrated Review Refresh.[7]

A robust cyber security posture is only possible with strong leadership. So, it is important that senior leaders understand the threat landscape and the potential impact of cyber attacks and must take ultimate responsibility for the digital resilience of the organisation, while also ensuring that all staff and students are aware of their roles in security.

Be aware of the threat landscape

Universities globally remain attractive targets. They operate large, complex and diverse digital infrastructures, with significant storage and processing capabilities.

The motivation of attackers falls into four main categories: those seeking to directly extort a payment through ransomware or other methods; theft of research data / knowledge; use of universities' digital infrastructure to directly monetise assets, through bitcoin mining for example; and those seeking to disrupt and destroy. These infrastructures must both resist attacks and be open and accessible in support of research and education. This balancing act leads to a set of trade-offs within cyber security. Universities' size and open culture create a very large attack surface of networks, devices and internet-facing services.

Half (50%) of higher education institutions, participating in the government's Cyber Security Breaches Survey 2023, reported experiencing breaches or attacks at least weekly, with three-quarters (75%) of higher education institutions reporting they were negatively impacted regardless of whether there was a material outcome or not.[8] Our sector must routinely defend against a high volume of relatively

[7] https://www.gov.uk/government/publications/integrated-review-refresh-2023-responding-to-a-more-contested-and-volatile-world
[8] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023-education-institutions-annex

unsophisticated but incessant speculative and opportunistic attacks alongside more serious attacks carried out by organised criminals, including state-sponsored groups.

For example, Jisc has identified a growing trend of destructive ransomware attacks against institutions, observing 15 major incidents in 2020, 18 during 2021, 19 during 2022 and 9 in the first half of 2023, impacting the organisation's ability to undertake core activities such as teaching or research.[9]

The increase in serious incidents in 2020 and 2021 resulted in the NCSC issuing an unprecedented three alerts to the UK research and education sector, highlighting targeted activity by hostile groups, during late 2020 and the first half of 2021.[10]

Understand the potential impact

Failure to invest properly in a robust cyber security strategy can have disastrous consequences, as Jisc's cyber impact report shows.[11] Impacts go beyond the direct costs of disruption to teaching and research activities and possible fines; students could lose coursework and the personal details of any staff member or student could be sold or traded online.

Some universities hit by ransomware over the last few years have lost control of their entire digital estates, with systems broken and data lost. This can halt all online functions, including communications and financial transactions. Some attacks have been deliberately timed to cause maximum disruption at critical points in the academic calendar, for example during enrolment, clearing and exams.

Serious attacks at any time can have huge implications for an organisation's reputation and finances. Significant monetary and human resources must be diverted to recover and rebuild, which could take weeks or months and cost millions. During this period, huge pressure is brought to bear on students and staff, with both short-term stress and longer-term burn-out presenting wellbeing and mental health risks.

Take responsibility for cyber security

Board-level leaders hold ultimate responsibility for the cyber security strategies that keep their people, data and systems safe from harm and misuse. While Jisc research

[9] Jisc Computer Security Incident Response Team (CSIRT) quarterly reports are published via Jisc's Cyber Security Community Group https://www.jisc.ac.uk/get-involved/cyber-security-community-group
[10] https://www.ncsc.gov.uk/news/alert-targeted-ransomware-attacks-on-uk-education-sector
[11] https://beta.jisc.ac.uk/reports/cyber-impact

shows cyber security is a priority for senior leaders at most universities, some institutions are better protected than others.[12]

Those organisations whose leaders are engaged with and take responsibility for cyber security are more likely to have effective defences and less likely to fall victim to a serious attack. Leaders must understand and oversee a number of key aspects, including policy and regulatory requirements, the risks their organisations face and how these are tackled. They must also engage with and empower technical leads, particularly chief information security officers and IT directors, and prioritise a continual investment programme that keeps up with the ever-evolving threat landscape.

Recommended actions for senior leaders

- Review security posture using the four-pillar security posture model described in the introduction above and in more detail below, along with:
    - Jisc's '16 questions you need to ask to assess your cyber security posture'
    - NCSC's 'Board Toolkit'
    - UUK's guidelines on 'Managing Risks in Internationalisation: Security-related Issues'
- Business continuity: make sure everyone in your organisation knows what to do in the event of a serious security incident. Regularly rehearse scenarios with a view to continual improvement, remembering to reflect changes in the threat landscape and technology. Again, tools and resources are available to assist with this.[13]
- Share and collaborate: Defending as one, higher education institutions should work together to share threat intelligence and expertise, which has a positive impact on the sector's preparedness and capability to respond, both tactically and strategically.

[12] https://beta.jisc.ac.uk/reports/cyber-security-posture-surveys
[13] For example, https://www.ncsc.gov.uk/information/exercise-in-a-box and https://beta.jisc.ac.uk/training/ransomware-incident-response-workshop

Risks and threats

Key points:

- The essential nature of universities, their extensive digital footprints and the important work they do, significantly increases their exposure to cyber risks.
- Cyber risks must be managed alongside all other areas of organisational risk (operational, financial, regulatory) as part of organisations' overall due diligence.

About the risks and threats

Universities are at risk from cyber attacks, and ransomware remains a key threat to all organisations. The NCSC 2022 Annual Review reported that 'Ransomware remains the most acute threat that businesses and organisations in the UK face'. During 2022, Jisc observed 19 highly disruptive major incidents impacting an organisation's ability to undertake core activities such as teaching or research. Many of these could have been prevented had basic security controls been in place and properly configured.

Phishing (obtaining user credentials or distributing malware via impersonation and deception) and business email compromise (BEC), abusing compromised accounts to make or receive fraudulent payments or share sensitive information are also serious risks and can cause significant damage, financially, operationally, and reputationally.

The use of compromised credentials (usernames and passwords) permits attackers unauthorised access to systems, services and data associated with the individual user account. Two-step verification provides a highly effective additional layer of defence against this risk. Systems and services designed, configured, and operated on a least privilege principle, helps reduce the initial impact of compromised accounts.

The sector is subject not only to opportunistic attacks from criminals, but also to specifically targeted attacks from highly skilled and determined threat actors, including those sponsored by nation states. In this context, universities must also consider how best to manage the threats created through their supply chain. Recent high-profile incidents, such as the 2020 attack against the software company SolarWinds, has highlighted the importance of identifying and managing supply chain security risks.[14]

[14] See https://www.ncsc.gov.uk/news/ncsc-statement-on-solarwinds-compromise

Universities globally remain attractive targets. They operate large, complex digital infrastructures, with significant storage and processing capabilities in support of their core mission. The motivation of attackers falls into four main categories: those seeking to directly extort a payment through ransomware or other methods; theft of research data/knowledge sets; use of universities' digital infrastructure to directly monetise assets; and those seeking to disrupt and destroy digital infrastructure.

These large and complex infrastructures must resist attacks, yet also be open and accessible in support of research and education. This balancing of open access, but secure storage, computational systems and services leads to a difficult set of trade-offs within cyber security. Combined with the culture of open access and collaboration to facilitate teaching, learning and research activities, this creates a very large attack surface of networks, devices and internet-facing services.

Risks specific to the sector:

- The nature and complexity of university environments creates a large attack surface with multiple potential points of entry. The complexity and breadth of organisations' digital estates mean new risks and threats are continually emerging.

- The huge range of valuable data generated and stored by universities (staff and student personal information, research data and evidence) and their consequential reliance upon it makes them an attractive target:

    - Universities produce data that needs to be stored, accessed, backed up and used appropriately to fully realise its academic or commercial value. This might include data produced for contractors or commercial potential, through to politically sensitive data.
    - Universities access sensitive data from third-party organisations, such as medical institutions that provide patient-identifiable or other clinical data. Universities may also access data that is considered commercially, operationally or personally sensitive.
    - Universities collect data associated with their enterprise, such as information about students, staff and finances. Data might be considered sensitive under law, by the data provider, or in cases where it informs decision making.

- How the sector operates – flexible/remote access to teaching and learning, national and international collaboration – contributes to a large attack surface of accessible, internet-facing services and infrastructure.

- Attacks may lead to a loss of control to digital infrastructure, and interruption/disruption of key services and activities. This may affect a university's ability to maintain high-quality teaching and research provision and affect its ability to uphold contractual or regulatory obligations.

In light of these risks, it is essential to identify and adopt new approaches that ensure security while preserving the aspects, such as open campuses and open research, that are fundamental to the sector's success.

Assessing risks and threats

The process of assessing risk requires open and transparent dialogue between all interested parties, including organisations' governance and technology teams and the researchers and administrators who have responsibility for collecting, managing and publishing data. 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. Technical and security teams can advise regarding the implementation of security controls and ensuring that working practices appropriately balance ease of use, functionality and security.

A shared understanding of risk management priorities is essential for success and must be driven by the highest levels of governance.

Organisations must also strike the right balance between the cost of implementing security controls and the costs that will be incurred following an attack or other security incident. However, it is essential that all potential costs are fully considered in such calculations – for example, the cost of service unavailability must be considered alongside the cost of recovering or rebuilding systems affected by an attack. The risk landscape is constantly changing, sometimes very quickly, so organisations must frequently review and be ready to adapt their risk management strategy accordingly. [15]

Confidentiality – Integrity – Availability (CIA) triad

The CIA triad is an established part of the security body of knowledge. It illustrates how information security management is a dynamic process, about finding the balance between three interrelated aspects in tension with each other. Universities must balance both the confidentiality and availability of their information with facility access, collaboration and sharing, while also maintaining its integrity (such as the veracity/accuracy of research findings and other data).

[15] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/a-guide-to-data-security/

The NCSC provides comprehensive risk management guidance for non-technical staff, for those who conduct cyber risk assessments, and for those making decisions that are informed by risk assessments.[16] Risk management guidance is also included in the NCSC's Cyber Security Toolkit for Boards.[17]

The toolkit notes that boards 'should have an awareness of the wider threat landscape through a regular threat briefing. This should include current threats which could affect all organisations and those that are specific to the business. Changes in the threat position should be included in the management information that the board receives at its board meeting'. NCSC produces threat reports on cyber security matters affecting the UK that universities can sign up to.

[16] https://www.ncsc.gov.uk/collection/risk-management-collection
[17] https://www.ncsc.gov.uk/section/board-toolkit/home

Strengthening security posture

Key points:

- The essential nature of universities, their extensive digital footprints and the important work they do significantly increases their exposure to cyber risks.
- Cyber risks must be managed alongside all areas of organisational risk (operational, financial, regulatory) as part of organisations' overall due diligence.
- Cyber security is complex and challenging, so it is important for universities to review their approach. Is basic digital hygiene in place? Is security managed in the way that it should be? Does the programme have a focus on continual improvement?
- Compliance frameworks are valuable tools for assessing organisational security posture, but are a means to an end, not an end in itself.
- Security must be embedded across all elements of an organisation's digital infrastructure, culture and working practices.
- Attacker tactics and techniques are continually evolving, so all organisations must keep their defensive approaches under review.
- Universities must actively monitor and manage supply chain related security risks such that the potential impacts of supply chain vulnerabilities or compromises can be quickly understood and mitigation actions taken.
- Senior leaders must demonstrate a strong commitment to training, building awareness and supporting staff, who are a key part of the defence.
- Encouraging a security culture and mindset is fundamental to a strong security posture.

A strong security posture is dependent upon four closely interrelated pillars – governance, assurance, technology and culture.

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. Like financial risks, cyber risks should be considered as organisational risks and included in corporate risk registers.

Institutions should consider who in the organisation 'owns' or 'controls' data to establish clear lines of assessment, accountability and monitoring between the decentralised production and use of data and the overarching shared organisational

responsibility for security. Institutions should also conduct internal and external audits of their risks, management priorities and systems.

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, they play a central role in determining an institution's appetite for risk and the identification and evaluation of information assets.

Ultimately, security is a responsibility for the whole institution. Institutional boards are strongly advised to make use of Jisc's 16 Questions you need to ask to assess your cyber security posture.[18] NCSC's Board Toolkit notes that that the assessment of cyber skills might be an activity within the overall people/talent-planning part of the business, and the board should have sight of this. The toolkit also notes that setting a risk appetite for cyber issues will help define the 'level' of risk an organisation will manage when pursuing its objectives, thereby aiding effective decision making.

Assurance

Governance arrangements should be informed by internal audits and reviews, while assurance frameworks provide mechanisms for organisations to assess and benchmark, through independent assessment, their current arrangements and identify areas for improvement.

Assurance or compliance, defined as configuring security to an accepted baseline and verifying whether it remains at or above that baseline, should be regarded as a starting point, not an end state. All organisations should understand the extent to which the risks they face are (and are not) mitigated by their compliance with an assurance framework, putting additional measures in place to address any gaps.

It is a condition of the Janet Security Policy[19] that any organisation connected to the Janet Network must undertake an annual self-assessment of the organisation's security posture. This can be to whatever framework, maturity model or certification that the organisation finds most useful or appropriate. Many universities have achieved Cyber Essentials, Cyber Essentials Plus or ISO 27001. These and the NCSC's Cyber Assessment Framework (CAF) are all useful and effective tools for demonstrating assurance in relation to a cyber security baseline.

[18] https://repository.jisc.ac.uk/8549/1/cyber-security-16-questions-checklist.pdf
[19] https://community.jisc.ac.uk/library/janet-policies/security-policy

Technology

In the context of security posture, technology should be considered as encompassing the broad range of systems and infrastructure all large organisations now depend upon. It relates not only to specific security components and services, such as firewalls and two-step verification, but also to making sure that security is embedded across all configurations, operations and working practices.

Technologies and working practices must appropriately balance ease of use, functionality and security. If security controls are perceived as too onerous and time-consuming, or if their importance is not properly communicated, people will at best ignore them and at worst seek to circumvent them.

Security must be considered as part of the landscape of day-to-day IT operations, some of which are set out in NCSC's 10 Steps to Cyber Security.[20] These include activities such as asset and vulnerability management, engagement and training, and data security. Fundamental to an organisation's digital resilience and its ability to quickly and effectivity recover from security incidents is an effective backup strategy, ideally including immutable, offline, backups ideally at a separate physical location.

A strong security posture is dependent upon a range of technical controls being in place and operating effectively together, as part of a defence-in-depth approach. It is important to move away from legacy technologies and network architectures which have been found to be increasingly insecure. At the same time, many services and tools widely used across the sector include built-in security controls, but these must be turned on, configured and managed correctly: assuming technologies are secure by default can be a costly mistake. Remote access services and end point detection and response tools are examples of technologies where maintaining secure configuration and operation is often challenging.

Culture

If staff and students are not properly advised and supported, they are very unlikely to exhibit the desired or required security behaviours. Worse, if the context and rationale for security controls are not clearly communicated and understood, controls may be perceived as simply getting in the way, rather than as an important aspect of business operations, resulting in them being circumvented or simply ignored.

Changes and improvements in security behaviours and mindsets will not happen overnight, and security awareness and training programmes must be driven from the

[20] https://www.ncsc.gov.uk/collection/10-steps

highest levels of the organisation to be credible. While mandatory induction and annual security refresher training have a role to play, regular updates, reinforcement and encouragement are essential if key messages are to become embedded in day-to-day working practices and habits.

People should be encouraged and praised for reporting any security issues and concerns. A positive, no-blame security culture needs to be engendered from the top down within organisations, balanced by clearly communicated and understood expectations around behaviour, acceptable use and negligence.

Frontline security staff often face considerable challenges, particularly when dealing with security incidents where the consequences may be severe. Staff welfare is a critical component of an organisation's security and resilience. The NCSC provides a range of advice and guidance to help organisations maintain staff wellbeing and avoid burnout.[21]

The joint NCSC and National Protective Security Agency (NPSA) Trusted Research campaign, with associated Effective Practice Principles, provides guidance on securing international research collaboration, which is essential to the continuing success of the UK's research and innovation sector.[22] UUK's guidance on Managing risks in Internationalisation: Security related issues also outlines a need to develop a developing a positive, risk informed culture, underpinned by robust governance, reporting and risk-management structures.[23]

[21] https://www.ncsc.gov.uk/blog-post/preparing-the-long-haul-the-cyber-threat-from-russia
[22] https://www.npsa.gov.uk/trusted-research-academia
[23] https://www.universitiesuk.ac.uk/sites/default/files/field/downloads/2021-07/managing-risks-in-internationalisation.pdf

Defence in depth

Key points:

- Basic security controls can deter and defend against the high volume of routine, speculative and opportunistic cyber attacks.
- Basic controls, in combination with other types of controls, increase the likelihood of successful detection and defence against more persistent, sophisticated attacks.
- The essential nature of universities, their extensive digital footprints and the important work they do, significantly increases their exposure to cyber risks.
- Organisations must establish and maintain a wide range of security controls to ensure defence in depth.
- A strong security posture relies upon closely interrelated technical and non-technical security controls.

Basic controls include making sure hardware and software are patched and up to date, and making sure internet-facing systems and services are protected with strong unique passwords and two-step verification. These controls alone block access to many avenues frequently exploited by attackers to compromise networks and initiate malicious activity, such as scanning for unpatched, vulnerable systems and employing brute-force techniques such as lists of commonly used or re-used passwords as 'routes in' to networks and systems. NCSC's Cyber Essentials is a UK government backed certification scheme, enabling organisations of all sizes to demonstrate that they have the recommended basic security controls in place.[24]

While it is important to prioritise basic controls, these are by no means the end of the story. Establishing a range of controls of different types helps organisations pivot from a primarily reactive to a proactive security stance, where controls designed to prevent and detect can reduce the impact of and resources required to address incidents and issues. Universities are eligible to sign up for a wide range of active cyber defence tools, available free of charge from the NCSC. [25]

[24] https://www.ncsc.gov.uk/cyberessentials
[25] https://www.ncsc.gov.uk/section/active-cyber-defence/services

The security body of knowledge identifies the following types of security control:

- Preventative – stops or minimises impact (for example, a firewall default deny rule for inbound traffic; segregation of account privileges within a finance system to prevent fraud).
- Detective – monitors and sounds alerts about incidents and issues (scanning for vulnerabilities and unpatched systems; security information and event management (SIEM); regularly auditing the allocation of administrative permissions and firewall rules).
- Corrective – remediates and reverses adverse impacts (restoring lost or stolen data from backups; incident response policies and procedures; security awareness training for staff involved in or affected by a security incident).
- Compensating – makes up for a weakness in another control (two-step verification strengthens account authentication and mitigates password security issues; detailed monitoring and alerting for a particularly vulnerable server).
- Deterrent – warns and discourages malicious or inappropriate activity (warning about attempted access to malicious websites; CCTV monitoring of secure areas; IT acceptable use policies; disciplinary procedures).

Each type of control has strengths and limitations, so a strong security posture must incorporate an interrelated set of all control types, managed and resourced appropriately. As the examples given above demonstrate, not all controls are technical (security awareness training is a very effective preventative control if done well) and recognising what a particular control does not do is just as important as understanding what it does.

Detection should be a primary objective for implementing security controls, not only for individual organisations but for the entire sector. As in any other context, prevention is always better than cure: gathering, sharing and analysing information about attack types and techniques gleaned from detective controls provides valuable intelligence that can inform both immediate tactical and longer-term strategic responses to issues and incidents.

The importance and effectiveness of a defence-in-depth approach is exemplified in the NCSC's guidance on protecting against phishing attacks,[26] which sets out multiple defensive layers:

[26] https://www.ncsc.gov.uk/guidance/phishing

- Layer 1: Make it difficult for attackers to reach your users with phishing emails by, for example, putting technical measures in place to filter or block incoming messages that could be malicious.
- Layer 2: Help users identify potential phishing emails via regular awareness training, encouraging them to seek help and report suspicious messages via easily accessible routes.
- Layer 3: Put measures in place to protect against the effects of undetected messages, such as two-step verification, which prevents an attacker from gaining access even if they manage to obtain a user's password, and malware protection on all devices.
- Layer 4: Respond quickly to incidents and reports, supported by a regularly tested and updated incident response plan.

Key to this approach is the overlapping of defensive layers, recognising that no layer can ever be 100% effective. A combination of preventative, detective and corrective controls must be in place to ensure a strong defence. Incidents will always occur, regardless of an organisation's level of readiness, so procedures for handling and responding to incidents are just as important as preventative measures to reduce the possibility of their occurrence. All organisations need a comprehensive combination of different controls to ensure a robust defence in-depth approach.

Maintaining momentum

Key points:

- The dynamic security landscape necessitates a culture of continual improvement.
- The complexity and difficulty of establishing and maintaining a strong security posture should not be underestimated in terms of resources and effort required.
- Regular rehearsals and testing are an essential part of security preparedness.
- Sharing services, experience and expertise strengthens the whole community.

Rapid technological developments and the dynamic threat landscape mean that the defender can never afford to be complacent. A strong security posture is dependent upon a culture of continuous review and improvement, and preparedness to adapt accordingly as circumstances change, sometimes at pace.

Rehearsals, exercises and tests

Regular rehearsals, exercises and tests are key to a strong security posture and institutions' capability and capacity to respond to cyber security threats and incidents. All institutions should regularly test all aspects of their preparedness, ensuring changes in the threat landscape and technology are reflected appropriately.[27] Numerous tools and resources are available to assist with this.[28]

Collaboration and sharing

While the sharing of information on cyber security incidents and data breaches can be a sensitive issue, sharing information about risks, threats, remediation approaches and lessons learned among the community is an essential component of an effective security ecosystem.

Sharing cyber security data, expertise and capabilities across the sector, facilitated by Jisc, the NCSC and other agencies, contributes to the establishment of a defensive

[27] https://www.ucisa.ac.uk/Resources
[28] For example, https://www.ncsc.gov.uk/information/exercise-in-a-box and https://beta.jisc.ac.uk/training/ransomware-incident-response-workshop

force more powerful than the sum of its parts, supporting both tactical and strategic responses to what is observed 'in the wild' and how risks and threats change over time.

Jisc provides a key point of focus in this area, via its Cyber Threat Intelligence Service,[29] its Cyber Security Community[30] and its Cyber Threat Monitoring Service.[31] The NCSC has established the Cyber Security Information Sharing Partnership (CiSP) to improve the exchange and monitoring of information about evolving cyber threats and targets across industry and higher education.[32] The Universities and Colleges Information Systems Association (UCISA) also maintains a security community group.[33]

[29] https://beta.jisc.ac.uk/cyber-threat-intelligence
[30] https://beta.jisc.ac.uk/get-involved/cyber-security-community-group
[31] https://beta.jisc.ac.uk/cyber-security-threat-monitoring
[32] https://www.ncsc.gov.uk/information/cyber-security-information-sharing-partnership--cisp-
[33] https://www.ucisa.ac.uk/Groups/Security-Group

Conclusion: Defend as one

Universities are large, complex, and collaborative organisations that hold lots of valuable and sensitive data. By incorporating cyber security as a strategic, ongoing priority, senior leaders can help prevent disruptions to key services and activities, including teaching and learning provision. It is important to:

- Understand the risks and threats your university faces, including who is targeting you.
- Strengthen your cyber security posture through strong governance, assurances, technology and a positive security culture, underpinned by open and transparent dialogue.
- Start with basic controls which can detect, defer and defend against a range of cyber attacks.
- Create defence in depth by establishing and maintaining a wide range of security controls, with closely interrelated technical and non-technical security controls.
- Maintain momentum by creating a culture of continual improvement and by rehearsing, testing and sharing services, experiences and expertise with the community.

In a connected community like the UK higher education sector, every institution has a part to play. The interdependence and interconnectedness of the sector means a failing at one organisation can have implications for many others, so it is imperative that all individual organisations account for the risks they face and the criticality of the functions they are responsible for. It also requires universities, industry and government working in partnership.

Recommended actions

- **Review security posture using the four-pillar security posture model described in the guidance, along with:**
  - Jisc's '16 questions you need to ask to assess your cyber security posture'
  - NCSC's Board Toolkit
  - UUK's guidelines on 'Managing Risks in Internationalisation: Security-Related Issues'.
- Business continuity: Make sure everyone in your organisation knows what to do in the event of a serious security incident. Regularly rehearse scenarios with a view to continual improvement, remembering to reflect changes in the threat landscape and technology. Tools and resources are available to assist with this.
- Share and collaborate: Defending as one, higher education institutions should work together to share threat intelligence and expertise, which has a positive impact on the sector's preparedness and capability to respond, both tactically and strategically.

Resource list

Cabinet Office (2023). Integrated Review Refresh 2023: Responding to a more contested and volatile world. Available at: https://www.gov.uk/government/publications/integrated-review-refresh-2023-responding-to-a-more-contested-and-volatile-world

DSIT (2023). Cyber security breaches survey 2023: education institutions annex. Available at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023-education-institutions-annex

DSIT, DCMS (2022). Exploring organisational experiences of cyber security breaches. Available at: https://www.gov.uk/government/publications/exploring-organisational-experiences-of-cyber-security-breaches

Jisc (2022). Cyber impact. Available at: https://beta.jisc.ac.uk/reports/cyber-impact

Jisc (2022). Cyber security posture surveys. Available at: https://beta.jisc.ac.uk/reports/cyber-security-posture-surveys

Jisc. 16 questions you need to ask to assess your cyber security posture. Available at: https://repository.jisc.ac.uk/8549/1/cyber-security-16-questions-checklist.pdf

Jisc. Janet security policy. Available at: https://community.jisc.ac.uk/library/janet-policies/security-policy

Jisc. Ransomware incident response workshop. Available at: https://beta.jisc.ac.uk/training/ransomware-incident-response-workshop

Jisc. Cyber threat intelligence. Available at: https://beta.jisc.ac.uk/cyber-threat-intelligence

Jisc. Cyber security community group. Available at: https://beta.jisc.ac.uk/get-involved/cyber-security-community-group

Jisc. Cyber security threat monitoring. Available at: https://beta.jisc.ac.uk/cyber-security-threat-monitoring

NCSC. Alert: Further ransomware attacks on the UK education sector by cyber criminals. Available at: https://www.ncsc.gov.uk/news/alert-targeted-ransomware-attacks-on-uk-education-sector

NCSC. Security and usability: you CAN have it all! Available at: https://www.ncsc.gov.uk/blog-post/security-and-usability--you-can-have-it-all-

NCSC. Risk Management. Available at: https://www.ncsc.gov.uk/collection/risk-management-collection

NCSC. UK joins international cyber agency partners to release supply chain guidance. Available at: https://www.ncsc.gov.uk/news/uk-joins-international-cyber-agency-partners-to-release-supply-chain-guidance

NCSC. Cyber Aware. Available at: https://www.ncsc.gov.uk/cyberaware/home

NCSC. Actions to take when the cyber threat is heightened. Available at: https://www.ncsc.gov.uk/guidance/actions-to-take-when-the-cyber-threat-is-heightened

NCSC. Cyber Security Toolkit for Boards. Available at: https://www.ncsc.gov.uk/section/board-toolkit/home

NCSC. 10 Steps to Cyber Security. Available at: https://www.ncsc.gov.uk/collection/10-steps

NCSC. Preparing for the long haul: the cyber threat from Russia. Available at: https://www.ncsc.gov.uk/blog-post/preparing-the-long-haul-the-cyber-threat-from-russia

NCSC. Cyber Essentials. Available at: https://www.ncsc.gov.uk/cyberessentials

NCSC. Phishing attacks: defending your organisation. Available at: https://www.ncsc.gov.uk/guidance/phishing

NCSC. Exercise in a Box. Available at: https://www.ncsc.gov.uk/information/exercise-in-a-box

NCSC. Connect Inform Share Protect (CISP). Available at: https://www.ncsc.gov.uk/information/cyber-security-information-sharing-partnership--cisp-

NCSC and NPSA. Trusted Research Guidance for Academia. Available at: https://www.npsa.gov.uk/trusted-research-academia

UCISA. Cyber resources. Available at: https://www.ucisa.ac.uk/Resources

UCISA. UCISA Security Group. Available at: https://www.ucisa.ac.uk/Groups/Security-Group

UUK (2020). Managing risks in internationalisation. Available at: https://www.universitiesuk.ac.uk/sites/default/files/field/downloads/2021-07/managing-risks-in-internationalisation.pdf

Universities UK is the collective voice of 142 universities in England, Scotland, Wales and Northern Ireland.

Our mission is to create the conditions for UK universities to be the best in the world; maximising their positive impact locally, nationally and globally.

Universities UK acts on behalf of universities, represented by their heads of institution.

Universities UK

Woburn House
20 Tavistock Square
London, WC1H 9HQ

+44 (0)20 7419 4111
info@universitiesuk.ac.uk
universitiesuk.ac.uk
@UniversitiesUK

July 2021

ISBN: 978-1-84036-421-7