Cyber impact

The impact of cyber security incidents on the UK’s further and higher education and research sectors

Observations, advice and recommendations

November 2020
Who is this document for?

This document is for vice chancellors or principals, CIOs, board members and executives with responsibility for data protection, risk management and cyber security leadership.

Audit and risk committees, funders, sector membership organisations and insurance organisations will also find value in this report.

IT and security professionals may find this report useful when discussing cyber security with their institutional leaders. The report does not contain a set of instructions. Rather it focuses upon development topics and areas for further discussion within your institution.

Who authored this report?

This report is a collaboration between Jisc and Hadfield Consultants Ltd. Jisc protects all UK further and higher institutions through the management and development of the Janet network and associated cyber security services. Hadfield Consultants Ltd provide an independent lens to ensure the information and recommendations in this report reflect the needs and observations of the further education and skills (FES) and higher education (HE) sectors.

Please see this useful glossary of cyber security terminology ncsc.gov.uk/information/ncsc-glossary
4 Introduction

6 Report recommendations

8 Cyber security context
Janet CSIRT incident tickets breakdown
Sector lens
Institution lens
Personal lens
Timing lens

12 Cyber security impact

18 Reducing and managing cyber impact and risks
Leadership
Technical ‘basics’
Awareness and training
Certification
BS 31111
ISO 27001
Cyber Essentials and Cyber Essentials Plus
The role of cyber insurance

22 How Jisc supports and protects HE institutions and FES providers

24 Appendix - cyber security impact checklist
Recovery
Direct
Long term and strategic
Introduction

This report examines the impact of cyber security incidents and breaches across the UK FES, HE and research sector. We examine the range of incidents that can affect institutions and provide practical advice and guidance as to how institutions can reduce the risk and mitigate these impacts.

We draw upon relevant findings extracted from Jisc’s recent (2020) Cyber Posture survey but also from various other sources - including deep-dive interviews with 16 institutions (12 universities and 4 further education providers). We have avoided naming specific institutions and are acutely aware of the sensitive nature of cyber-attacks.

Covid-19 is challenging all aspects of our education ecosystem as both further and higher education institutions develop new ways to deliver learning and teaching. Personal data and information are being increasingly held on devices outside of institutional premises. Protecting that information, wherever it exists, has extended existing security challenges.

Every UK institution is working hard to reduce the likelihood of a breach occurring and of the impact should one occur, and the survey results show institutions are becoming more prepared. However, from the increase in high profile incidents affecting institutions and from Jisc’s wider security activities, our work has concluded that it is a case, for all institutions, of when an incident or a breach will occur and not if one will occur. Repeatedly we have heard of near misses with one university describing the scale of the challenge as “there’s a danger we’re preparing for a medium weight threat but we’re up against a heavy weight”.

The cyber security impact examples we present in this report highlight the breadth of breaches – IT and institutional priorities and projects disrupted, students and teaching and research staff impacted, leadership effort to manage major breaches and the financial impact of payroll losses, ransomware payments and IT recovery costs.

At the same time many institutions do not fully understand and are not systematically tracking all costs associated with a cyber security incident. In this regard our cyber impact checklist is designed to help.

Cyber security investment, we note, often follows some form of breach or incident – our collective challenge is to reflect on the nature of threats, breach likelihood, potential impact and proactively invest, despite financial constraints.

Leadership awareness of cyber security attacks has increased over the last two years and particularly since Covid-19. We ask institution leaders to read this report, note our recommendations and support cyber security colleagues’ requests for leadership support and financial investment.

We hope every UK FES provider and university will derive value from this report.
Further education and skills (FES) providers
FES providers, in the context of this document, refer to further education colleges across the four nations, sixth form colleges in England (including academies which were previously sixth form colleges) and Wales, specialist colleges and independent specialist colleges in England and Welsh government grant funded, adult and community learning providers and work based learning providers.
Report recommendations

The recommendations opposite, on page 7, reflect the observations throughout this report and crystallise action for institutions to consider. We also present a cyber impact checklist to help you consider the full monetary impact of cyber incidents and breaches (see appendix).
Institutions - cyber security

1. Ensure the governing body and executive are aware of cyber security risks to the institution

2. Achieve Cyber Essentials as a minimum to protect against a range of the most common cyber-attacks. Consider Cyber Essentials Plus and BS 31111 certification – see page 20 for more information

3. Ensure Multifactor Authentication is in place for all access to critical systems, and ideally for everyone to all systems

4. Business continuity plans should be in place with particular emphasis placed on key times of the academic year - for example, assessment, clearing, enrolment, induction. In addition, all FES providers and universities should review investment plans for specific services to defend critical systems and minimise the impact of any successful attack

5. Institutions must ensure all students and staff have good cyber security awareness and that training and awareness starts before students arrive and continues throughout their time at an institution

6. Implement segregated central logging of critical systems to assist in incident investigations and ideally implement a security information and event management solution – either internally or as a managed service

7. Increase effort to track the impact of cyber incidents – from a recovery, direct impact, and a long term/strategic point of view

8. Implement Domain Name System (DNS) protection to mitigate web requests being directed to compromised or dangerous websites

9. Implement network segmentation and consider moving towards a Zero Trust Environment - see page 19 for more information

10. Ensure Janet CSIRT is informed of any cyber security incident or concern, on: irt@csirt.ja.net or call 0300 999 2340

Institutions – cyber insurance

1. Review and implement the NCSC cyber insurance guidance: ncsc.gov.uk/guidance/cyber-insurance-guidance

2. Ensure your cyber insurer and their appointed incident response organisation is aware of Jisc, and Janet CSIRT is included in all incident response, management and Disaster Recovery processes

3. Ensure cover reflects the technical and compliance environment across your institution and your risk attitude
Cyber security context

We present the nature of the FE and HE cyber security threat through sector, institutional, personal and timing ‘lenses’ and explore the ways in which Covid-19 has changed the threat profile.

In September 2019, the National Cyber Security Centre (NCSC) published a paper that provided a short assessment of the cyber security threat to UK universities and academia. It highlighted cyber-crime as presenting “the most evident and disruptive difficulties for universities” and that state-sponsored espionage “is likely to cause greater long-term damage” to the value of research and to the UK’s knowledge advantage. Meanwhile, the variety of attack methods being deployed is increasing for all institutions right across the education and research sector.

State sponsored actors, cyber criminals, disgruntled students, and opportunists are all threats to institutions – potentially at the same time. General cyber-criminal activity is affecting the education sector in the same way other industries are impacted, but attacker reconnaissance can also lead to highly refined operations that reflect institution processes and systems, giving them a better chance of success.

Attack objectives include scamming individuals for money, accessing systems to defraud payroll, demanding ransom payments, identity theft, disruptive activity, and attacks designed to extract high value research Intellectual Property.

The breadth of incidents is illustrated in the chart on page 9. Over the past few years, Jisc’s computer security incident response team (Janet CSIRT), has handled between 5,000 and 6,000 incidents and queries a year. The graph shows a breakdown of the types of incidents affecting Jisc’s members.

These statistics help illustrate the breadth of incidents experienced across the education sector; the actual figures are heavily influenced by the activity of Janet CSIRT and the detection of events rather than their actual rates of occurrence. For example, a successful investigation into a botnet will cause that month’s malware figures to rise even though the malware may have been active, but undetected, in previous months.

The scale of the challenge is clear - between August 2019 and August 2020 Jisc saw more than 1,100 Denial of Service¹ attacks, on the Janet network, targeting 236 members.
Janet CSIRT incident tickets breakdown
September 2019 - August 2020

- A denial of service incident may contain multiple attacks. These 601 incidents contained more than 1,100 DDoS attacks.

<table>
<thead>
<tr>
<th>Category</th>
<th>12m total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware</td>
<td>1,817</td>
</tr>
<tr>
<td>Copyright</td>
<td>692</td>
</tr>
<tr>
<td>Denial of service</td>
<td>601</td>
</tr>
<tr>
<td>Compromise</td>
<td>549</td>
</tr>
<tr>
<td>Phishing</td>
<td>396</td>
</tr>
<tr>
<td>Net/security query</td>
<td>385</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Category</th>
<th>12m total</th>
</tr>
</thead>
<tbody>
<tr>
<td>General query</td>
<td>290</td>
</tr>
<tr>
<td>Misconfiguration</td>
<td>205</td>
</tr>
<tr>
<td>Scanning</td>
<td>151</td>
</tr>
<tr>
<td>Vulnerability</td>
<td>145</td>
</tr>
<tr>
<td>Unsolicited bulk email</td>
<td>45</td>
</tr>
<tr>
<td>LEA query</td>
<td>43</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Category</th>
<th>12m total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorised use</td>
<td>32</td>
</tr>
<tr>
<td>Legal/policy query</td>
<td>13</td>
</tr>
<tr>
<td>Social engineering</td>
<td>10</td>
</tr>
<tr>
<td>Undetermined</td>
<td>5</td>
</tr>
<tr>
<td>Other</td>
<td>66</td>
</tr>
</tbody>
</table>

1 A denial of service incident may contain multiple attacks. These 601 incidents contained more than 1,100 DDoS attacks.
We have observed the cyber security threat through four lenses.

**Sector lens**

There is evidence of attacks that have affected multiple institutions at the same time. Either through the infrastructure of one institution or through multiple attack points. Such attacks have also been international in nature. There is also evidence of institutional attacks leading to the compromise of suppliers and partners via a chain starting at a single institution.

**Institution lens**

According to Jisc’s 2020 Posture Survey, phishing/social engineering is still the top threat identified in HE and FE, with 72% of responding HE institutions and 74% of FES providers selecting this as their top ranked threat. Ransomware/malware and unpatched security vulnerabilities are ranked second and third by both HE and FE sectors. For those who indicate ‘other’ threats, human error and accidental data breaches by staff are most mentioned, reflecting the responses from 2019.

A separate (2020) IBM & Ponemon Institute Cost of a Data Breach Report states the education sector average cost of a data breach at £3.1m (a 18% reduction from 2019) with healthcare having the highest global industry average cost of £5.7m.

**Personal lens**

Students and staff members are victims too. Multiple and opportunistic scams are well known, with Amazon and Apple gift card scams common across the FE and HE sectors. Student tuition fee fraud attempts continue to impact those working and studying within UK institutions.

**Timing lens**

August 2020 has seen an increase in attacks leading to NCSC issuing a UK education cyber security alert in September. Successful attacks during key times, such as clearing, enrolment, or assessment "would be catastrophic" one university told us, reflecting the same sentiment as the FES providers we spoke to. Defending against and managing the impact of attacks, at critical times, is a priority for all institutions.
Although there has been a change in the types of incidents following the move to more remote working, FES providers and HE institutions require exemplary cyber security policies and controls irrespective of Covid-19.

Phishing attempts continue apace, and as reported by NCSC, threat actors have exploited the pandemic by using Covid-19 related scams and phishing emails.

Covid-19 has led FE and HE organisations to accelerate, for example, the deployment of Multifactor Authentication (MFA) and Virtual Private Network (VPN) roll outs. It has also parked or delayed IT/cyber projects dependent upon institution-based staff and contractors.

We have started to put in extra controls because of Covid-19 and home working, but predominantly on college devices. Updated our procedures on use of personal mobile devices. Increased investment in malware and phishing protection. A number of our projects have been delayed due to Covid-19 where external contractors are required onsite.

FES provider
We explore the impact of cyber-attacks on FES providers and HE institutions in terms of how they recover, the direct impact upon staff, students and researchers as well as the potential long term and strategic impact of some breaches.

An appendix, at the back of this document, provides a cyber security impact checklist to assist institutions in understanding and tracking impact.

The 2020 IBM & Ponemon Institute Cost of a Data Breach Report states the education sector average cost of a data breach at £3.1m (a 18% reduction from 2019) with healthcare having the highest global industry average cost of £5.7m.

Research (2020) by IDC found that education organisations suffered 8 DNS attacks (on average per annum) each costing $867,000. They also claimed education institutions as having the most instances of customer information or intellectual property stolen than any other sector.

These monetary impact numbers may seem unrealistic, but as this report shows, there are many ways an incident can affect an institution, not all of which may be accurately or holistically recorded. Responses to the Jisc Posture Survey show that responders from both HE institutions and FES providers estimate that cyber security breaches and attacks over the last 12 months have cost their organisation less than £100,000, with most responses in the £1,000 to £49,000 bracket. Over one third of FE responses (35%) indicated no incurred cost, while 36% of HE institutions do not know the financial costs.

The Jisc posture survey also suggests that many institutions rely on the goodwill of their staff to respond to incidents out of hours. Given the lengthy recovery periods experienced in the sector, it is likely that this goodwill extends beyond the initial incident and should be taken into account when assessing the financial impact of cyber security incidents. The emotional impact on staff handling the incident as well as the emotional experience of staff and students affected by an incident should also be captured.

These survey responses suggest that organisations do not see a significant financial cost to their organisations. However, we suspect the actual cost is not being captured across an institution. In-depth interviews undertaken June-August 2020, with 16 institutions, has illustrated how hard impact is to calculate and that there is a general lack of measuring impact.

To get a better understanding of the range of impact costs, associated with cyber security incidents, we present them in terms of recovery, direct and strategic impact - see the following pages.
Recovery impact

Jisc’s 2020 Posture Survey states staff time to deal with incidents as the biggest reported impact for both HE and FE.

Feedback also suggests that incident recovery is not always tracked in terms of IT and other staff effort. We also found that post-incident cyber security investment is often accelerated rather than newly justified because of an incident. Nonetheless specialists (e.g. database/system forensic) can cost more than £1,200 per day and could, for example, result in £36,000+ to recover just three systems. For incidents that result in a court case the impact on IT staff will extend over time and may also include legal costs (although this might be covered by insurance).

Critically, the effort to resolve cyber security breaches means that IT and other staff are halted from other priorities – the opportunity cost. Both FES providers and universities shared with us many examples of important transformational projects being affected because of a breach or incident.

University phishing breach
A university, in response to a 2019 data breach, deployed a response team of fifteen staff members for three weeks and a further five staff members for three more weeks equating to £65,000 worth of staff effort plus significant legal costs. Existing projects were delayed because of the breach.

University unauthorised hacking
A university suffered, in 2020, a password spraying attack affecting one university led to the onward phishing of other universities and organisations. Around 1,000 accounts were compromised within the originating university (almost all student accounts) resulting in 80 days of IT effort to resolve. The progress of IT transformation projects and response times for internal customers were affected. Impact on students was minimal but could have been severe if data/systems had been accessed.

University unauthorised hacking
In 2020, a password spraying attack affecting one university led to the onward phishing of other universities and organisations. Around 1,000 accounts were compromised within the originating university (almost all student accounts) resulting in 80 days of IT effort to resolve. The progress of IT transformation projects and response times for internal customers were affected. Impact on students was minimal but could have been severe if data/systems had been accessed.

FES provider phishing breach
One FES provider shared that they experienced, in 2020, a phishing campaign that affected 40 accounts, leading to recovery costs of £30,000 over 12 months. Two attacks took one member of staff a week to resolve. A Denial of Service attack, at the same FES provider, in 2019 resulted in system downtime that affected some online-based student exams - a direct impact.
Direct impact

Staff and student money has been lost, institution’s monies lost and connected institutions, suppliers and partners also defrauded.

The targeting of finance teams and senior staff in all organisations is commonplace and regularly successful. While finances might be recovered the effort is significant. Both FE and HE take the protection of personal data extremely seriously, but a six figure ICO fine has occurred within the sector. Moreover, FES providers and universities told us of the softer impacts an ICO investigation brings in terms of the intense nature of the experience, the potential longevity of that experience, the impact of the well-being of those involved, and the potential reputational impact incurred.

Phishing breach affecting university supply chain
In 2020 a university suffered from a phishing attack resulting in a full reset of all finance department accounts. For two weeks processing payments was hampered, but more significantly hackers tried to defraud university suppliers of c£250,000. One creditor did pay out monies, though it was in the end retrieved.

HE sector phishing campaign
In 2018 Stolen Pencil (thought to have originated from North Korea) spearphishing emails were targeted at academics with a view to compromising institutional systems and IP via fake websites, lure documents and the installation of malicious Google Chrome extensions.

State sponsored phishing attacks - Silent Librarian
The US Dept of Justice cited a cybercrime group for hacking, wire fraud and identity theft across 2018-2019. The indictment alleged c$3.4 billion worth of Intellectual Property due to unauthorised access, 31.5 terabytes of data, 7,998 compromised university accounts, 144 US and 176 non-US universities affected. This attack followed an earlier Iranian campaign between 2013 and 2017. There is also evidence of Silent Librarian credential phishing campaigns continuing throughout 2019 and 2020.

US University phishing attack
An American university paid, in 2017, $1.9m into a fraudster’s bank account. The payment was in response to an email-based invoice from a criminal posing as their contracted construction company.

University ransomware attack
A 2020 ransomware attack affected one university researcher who lost their research data - though it was backed up. Days of reformatting effort resulted, but the nature of the attack led to a further ten days of high-grade IT support due to a concern that the impact might broaden to other researchers. It did not due to their effort. Processes were tightened because of the incident.
FES provider ransomware attack
A FES provider suffered an attack, on results day in August 2020, resulting in the loss of IT infrastructure, staff and student email and the student portal. While the attack did not affect personal data, it significantly disrupted enrolment activities with results needing to be shared via personal email addresses. The FES provider said, “today has been among the most challenging days in College history”.

Indirect ransomware incident.
In May 2020 a third-party service provider with commercial relationships with many UK and international universities experienced a ransomware attack in which the criminal exfiltrated a subset of data from many of their clients including student, staff and alumni data. Although the incident occurred at the service provider, the impact on UK universities was considerable with time and money spent to investigate the incident, notifying affected individuals and informing the ICO as well as potential reputational damage.

Fraudulent email breaches
A FES provider described £10,000 being extracted, in 2020, from payroll via a fraudulent email sent to a vice principal. Another FES provider was tricked into paying £10,000 as a hacker had investigated and circumnavigated institutional processes. A university shared details of a phishing-based incident that resulted in 3 staff members’ salaries being diverted for one month, costing the university around £10,000.

University / research malware attack
In May 2020 over a dozen supercomputers across Europe were forced to shut down to resolve a security incident related to cryptocurrency mining malware. Research-intensive institutions were also affected with weeks of remedial work required to renew SSH keys and login credentials. The potential impact could have been greater had the cyber criminals motive revolved around research IP or corporate system hacks rather than using the processing power of supercomputers to process cryptocurrency programmes.

University ransomware attack
Maastricht University publicly shared their experience of an attack that occurred on the 24th December 2019. A successful ransomware attack led to c200 staff (central and faculty IT services, lectures, student advisors & psychologists, timetable schedulers, finance, HR, legal, library estates) working to address the impact of the attack and having all systems/processes ready for the start of term. Without a concerted cross university approach, it could have taken months to restore systems ready for students return. The university is thought to have paid a ransom of c£230,000. The attack was described in Dutch parliament as a “wake up call for the entire education sector” and illustrates the recovery effort as well as direct monetary impact.

Suppliers datacentre breach
One university reported a managed service provider’s datacentre being taken down, in 2019, by an attack meaning researchers could not log on to journals for a day. While not business critical in nature, the incident illustrates the dependence upon supplier cyber security infrastructure and protocols. It is important that FES providers and universities ensure their suppliers have robust cyber security.

Student records data breach
In 2019 a UK university suffered a malicious data breach resulting in c100 students’ records being breached and basic data on c4,000 students being downloaded.

University / research malware attack
In May 2020 over a dozen supercomputers across Europe were forced to shut down to resolve a security incident related to cryptocurrency mining malware. Research-intensive institutions were also affected with weeks of remedial work required to renew SSH keys and login credentials. The potential impact could have been greater had the cyber criminals motive revolved around research IP or corporate system hacks rather than using the processing power of supercomputers to process cryptocurrency programmes.
Long term and strategic impact

The exposure of personal data could affect reputation though there is little evidence of significant reputation impact from cyber-attacks/breaches to date despite national press headlines.

There is also little evidence that student related income has thus far been lost due to cyber-attacks – but security leaders are most worried about impacts during key time periods, such as clearing, enrolment and assessment periods. Consistent attacks would most likely have a significant impact – a previous FE Jisc ‘value study’ suggested that students might move FES provider if systems (and therefore student access) were impacted over a number of weeks.

2020’s ransomware incidents illustrate the impact of successful attacks during the critical month of August. Seven Jisc members, that we are aware of, were affected with one suffering results day systems losses. This compares to six successful ransomware attacks during the rest of 2020. Recovery from such attacks also highlight the innovation that exists across the FE and HE sectors with workarounds (e.g. new microsites built in 48 hours, new phone lines for enrolment) being put in place when attacks occur.

One of the affected universities expected it would take “a number of weeks” to resolve the cyber-attack with limited systems available at the start of the new 2020 academic year. Another university attack led to exams being cancelled and the clearing hotline being disrupted. Students were told there would be no access to the campus for a brief period and online platforms had been temporarily switched off. Assessment deadlines were extended, and students assured no one would be disadvantaged.

Clearing downtime is a risk where £10m of income could be lost if systems were down for a significant period.

University CISO regarding the potential impact of cyber-attack related downtime during clearing.
Students - spotlight

Critically, institutions told us that their students care about their data and expect institutions to protect it. As they re-join/join their FES provider or university it has never been so important to protect their accounts. A Jisc study – the 2018 Digital Experience Insights Survey conducted with more than 37,000 students – showed that, while more than half of students are confident their data are protected by their HE institution, only 39% feel they are told about how their data is stored and used by their university. Institutions therefore have more work to do raise awareness about potential threat as well as the measures they are taking to protect student’s data.

Interview feedback has also highlighted the potential increased vulnerability (to phishing attacks) of students emanating from outside of the UK. Cultural acceptance of authority and other factors make it more likely that some prospective or current international students might fall for student fee and other fraudulent email scams. However, all students are vulnerable to phishing scams with Student Loan Company phishing campaigns being a regular occurrence at the start of the academic year. Institutions must work hard to ensure all students have cyber security awareness before they arrive for study/research and continue thereafter.

One university shared that, in one year, around 200 student and staff members had fallen for voucher scams resulting in £100’s of pounds lost for each of them (£50,000 - £100,000 collectively) – this only represents those they were aware of.
Reducing and managing cyber impact and risks

In this section we explore the solutions required to defend against would be attackers, improve recovery times and we explore the nature and role of cyber security insurance.

The Jisc Posture Survey suggests that perceptions of cyber security protection are not high with only 10% scoring their (HE) organisation as 8+ and a mean score of 6.4/10. Perceptions in FE are more positive with 36% scoring their organisation as 8+ and a mean score of 7/10. For both sectors this shows that more measures and processes may be needed for institutions to improve protection levels – particularly to respond to the different threats related to increased remote working that Covid-19 brings.

Through the recent Jisc Posture Survey and follow up interviews we have noticed four equally important aspects to reduce and manage cyber security threats.

**Leadership**

The vast majority of HE institutions and FES providers show priority is given to cyber security within their institution while even greater percentages now have cyber security on their corporate risk registers (Jisc Posture Survey 2020). This supplies a solid foundation to build upon. Continued leadership awareness, knowledge, and support of the nature of cyber threat, the likelihood and potential impact is a critical success factor for UK FES providers and HE institutions to optimise their threat defence, detection, and management strategy. Cyber security is not simply an IT issue and targeted investment must ensure a coordinated and strategic approach to technology, processes, and awareness/training. Board level involvement is crucial with risk and audit committees taking a proactive role as well as effective cyber dashboards and regular reporting. Visible leadership support for cyber security campaigns will also help.

In addition, systems are often decentralised which increases the complexity and effort in protecting them. Support to implement necessary changes, across all departments, is therefore critical. At the same time this compartmentalisation makes it hard for universities to track the true impact, for students and staff, across an institution. Our cyber security impact checklist should help leaders consider all aspects.

**Technical ‘basics’**

Institutions must ensure the technical basics are in place or at least scheduled with sufficient investment. These basics cover how staff and students access systems, data, and research from campus and from home, the corporate systems that underpin all aspects of an institution and the network that allows access to those systems. Institutions must invest in skilled cyber security staff – either internally or via managed services – to plan and implement solutions across the institution’s systems estate.

NCSC’s recent education sector alert provides useful mitigation and recovery advice and guidance.
Access control - Multifactor Authentication (MFA) spotlight

HE institutions and FES providers tell us how important MFA has been in reducing the likelihood of cyber breaches and in particular phishing and fraudulent emails scams. The Jisc Posture Survey (2020) shows us that both HE and FE sectors are more likely to deploy MFA to staff. 72% of HE and 64% of FE indicate some form of MFA deployment for staff, dropping to 22% (HE) and 10% (FE) for students. Reasons for non-deployment include disruption to users, time/resource, platform integration issues and prioritisation of other work. Despite these barriers we recommend MFA for all critical systems and services and preferably for all staff and students to all systems.

Certification

Certification provides an assessment of the effectiveness of institutional defences, information and security management practices and risk awareness and management. They are an important vehicle to ensure institution wide progress and, based upon feedback from universities, unlock research and training opportunities.

Jisc's Posture Survey (2020) shows an increase in the proportion of HE organisations achieving Cyber Essentials (CE), CE Plus and ISO27001, showing their continued importance. But there is some way to go – 31% of universities have not yet achieved CE, 69% CE Plus and 86% ISO27001 but positively 31% are working towards CE Plus. Certification penetration is currently lower in FE than HE but has increased substantially over the past few years. 49% FE providers have achieved CE and a further 34% are working towards CE and 36% towards CE Plus.

This increase is likely linked to government and funding requirements, for example, the Education and Skills Funding Agency requires FES providers to progress to Cyber Essentials Plus for the 2021/22 funding year and achieving the certification was a Key Action in the Scottish Cyber Resilience public sector action plan 2017-2018.

Zero Trust Model

Zero Trust is centred around not automatically believing everything inside your firewall can be trusted. Instead, it uses identity and device verification, MFA, least privileged access and network segmentation to reduce the number of opportunities for threat actors to gain access. NCSC has published a set of Zero Trust principles that should be considered if deciding to migrate to a Zero Trust architecture.
What are the important cyber security related standards and certifications that FE and HE leaders should be aware of?

**BS 31111**
The BS 31111:2018 standard and assessment is a governing body led approach to cyber security. It helps institutions to find cyber risks, understand them and ensure that right processes are in place – to help build resilience to cyber-attacks and other disruptive events, while improving operational performance. In turn, this helps you to show the steps you are taking to stakeholders and regulators. In 2018/2019 Jisc undertook an assessment of CERN’s ability to protect information and data processing infrastructure against BS31111.

**ISO 27001**
The international ISO 2700:2013 is a widely recognised standard for information security management systems (ISMS) and likely to become a mandatory standard for education institutions in the future. It is designed to help organisations of all types and sizes manage information security processes while optimising costs.

**Cyber Essentials and Cyber Essentials Plus**
The self-certified (government led and UK focused) Cyber Essentials certification provides institutions with reassurance that your defences are protected against many of the most common cyber-attacks. The process ensures that you understand where you stand and the areas where you may need to improve. Certification means your organisation can bid for government contracts involving sensitive or personal information. Cyber Essentials Plus includes additional external hands-on technical verification.
The role of cyber insurance

Jisc’s (2020) Posture Survey for the first time explored the nature and extent of cyber-related insurance across the FE and HE sectors. It discovered that 41% of HE institutions indicate they have some form of cyber security cover and are more likely to have specific cyber security insurance (27%) than FES providers (15%). However, more FES providers indicate having some form of cyber security insurance overall (60%) and are more likely to have this as part of a broader insurance policy. Interestingly, cyber insurance take-up levels in the FE and HE sectors are greater than for other sectors, with only 11% of businesses and 6% of charities reporting in the 2019 DCMS Cyber Security Breaches Survey that they had a specific cyber security insurance policy.

Insurance claims for cyber security breaches do not appear to be common, although more are reported in HE than in FE. Only 3 HE institutions (out of 21 that stated they had such insurance cover) reported making cyber insurance claims in the current or previous academic years. None of the 28 FES providers that stated they had cover had made a claim.

FES providers and HE institutions told us that there is a need for cyber-specific policies to reflect the reality of protection in place. Moreover, the reasons stated for not having insurance included that cyber security-related fines (e.g. ICO) were not covered by UK insurers (they stated this was not the case in the US) and that generally speaking they were not convinced an insurer would pay out - there is no evidence as to whether this is or is not the case. Those that do not have specific cyber insurance are living with the incumbent risk.

For some, cyber-specific insurance supplies comfort and specialist support and guidance – especially when incident response services are provided. Institutions should ensure their insurance companies and any insurance-provided incident response services are aware of Janet CSIRT and the help that can be provided for no additional cost as part of Jisc membership. The sooner Janet CSIRT is notified of an incident, the quicker it can be resolved and if necessary other institutions can be alerted to protect them and the sector.

In August 2020, a useful guide to cyber insurance was published by NCSC.
How Jisc supports and protects HE institutions and FES providers

Jisc has a wide range of cyber security services to protect the Janet Network; protect FES providers and HE institutions connected to the network; and help organisations to protect themselves.

The cyber security services and intelligence we provide focuses upon protecting the Janet Network and helping to protect all those connected to Janet.

Our services align with the needs and demands of IT and cyber security teams within education and research institutions as well as the strategic needs of institution leaders.

We also provide cyber security related advice and guidance, procurement frameworks, training, and JiscMail lists to help cyber security professionals stay in touch with the latest developments.

- Core service included in Jisc subscription
- Optional Jisc service

Further information on Jisc’s services can be found here.
<table>
<thead>
<tr>
<th>Jisc service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Incident response</strong></td>
<td>Janet CSIRT: Jisc’s team of security analysts who work closely with the education and research community to detect, report and investigate incidents that pose a threat to the security of our members’ information systems and to help you recover from serious incidents, such as ransomware. All underpinned by our cyber threat intelligence.</td>
</tr>
<tr>
<td><strong>Protecting staff, students and assets</strong></td>
<td>Janet Network resolver: This service can mitigate the risk of a user’s web requests being directed to compromised or dangerous websites, such as those used in phishing attacks.</td>
</tr>
<tr>
<td><strong>Network defence</strong></td>
<td>Foundation DDoS mitigation: Jisc detects and filters DDoS attack traffic across the Janet Network before it reaches you – mitigating the effects of attacks on your Janet connection, and reducing disruption and cost.</td>
</tr>
<tr>
<td></td>
<td>Critical services protection: Extra protection for business-critical services, offering out-of-hours coverage, customisable protection of externally-facing services and fast DDoS mitigation response times including the option of permanent mitigation.</td>
</tr>
<tr>
<td><strong>Resilience</strong></td>
<td>Primary / secondary nameserver service: Secure management of DNS records. Adds additional resilience to an organisation’s DNS infrastructure.</td>
</tr>
<tr>
<td></td>
<td>Network time service (NTP): Delivering a reliable and accurate time reference across your network.</td>
</tr>
<tr>
<td><strong>Identify threats</strong></td>
<td>Managed SIEM: A Security Information and Event Management (SIEM) solution makes it easier to spot security-related anomalies on your network by aggregating data from various systems and turning data logs into actionable insights either as a managed service or run by you. SIEMs help to spot incidents quickly, minimising their impact.</td>
</tr>
<tr>
<td></td>
<td>Splunk:</td>
</tr>
<tr>
<td><strong>Certifications, audits and assessments</strong></td>
<td>Cyber Essentials: A trusted way to gain and renew Cyber Essentials certification, helping to make sure vital security precautions are in place.</td>
</tr>
<tr>
<td></td>
<td>Cyber Essentials Plus:</td>
</tr>
<tr>
<td></td>
<td>BS 31111 audit and assessment: A top-down approach to managing cyber risk – helping leaders to understand risks, mitigate them and stay resilient.</td>
</tr>
<tr>
<td></td>
<td>Cyber security financial X-ray: A transparent overview of cyber security costs, with peer benchmarking included – to help assess levels of protection and identify vulnerabilities.</td>
</tr>
<tr>
<td><strong>Evaluate and improve the security of your institution</strong></td>
<td>Cyber security assessment: A tailored, cost-effective service that helps you to evaluate, analyse and improve your security posture and to help meet audit and compliance needs.</td>
</tr>
<tr>
<td></td>
<td>Penetration testing: A CREST-accredited team who will help you identify vulnerabilities, assess risks, and take corrective action by testing systems and networks against real-world cyber attack scenarios.</td>
</tr>
</tbody>
</table>
Appendix - cyber security impact checklist

Our research has highlighted different types of cyber security impact. The checklist is designed to raise awareness of different impact elements and to help leadership-based discussions to highlight the true impact of cyber security incidents and breaches.

**Recovery**
This report has highlighted that the involvement of senior management, teaching and research staff often supplements cyber security / IT effort and direct costs involved in recovery from a breach.

**Direct**
Our interviews suggest that few institutions track and calculate the impact of a cyber related breach beyond the recovery aspects.

**Long term and strategic**
Feedback suggests few institutions and providers have lost student income, but the truth is they are unlikely to know whether a clearing related breach, for example, has led to a loss of income and to what extent. Strategic impact can also relate to the knock-on effects of a breach for partners, suppliers, and the local economy. It is also important to track and calculate reputational damage associated with press coverage and ICO fines.

Impact should be considered in financial and non-financial terms. For example, the effort to recover from a cyber security breach can be calculated in financial terms (number of FTE x duration x average salary including on-costs) but it may also be insightful to track the hours and working days lost and the impact of losing those days on other projects or work on teaching and non-teaching staff.
<table>
<thead>
<tr>
<th>Type / scale of impact</th>
<th>No impact</th>
<th>Some impact</th>
<th>High impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recovery</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security staff effort</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT staff effort</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Teaching / research staff effort</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Senior management effort</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hardware replacement</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>External subject matter experts (e.g. forensic/database consultants)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Direct</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Students – learning, exams, well-being/distress</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Staff – well-being / distress and knock-on impact</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Students / staff – lost monies</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Teaching staff – teaching</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Research / researchers - research projects, collaborations, or partners</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Professional services / support staff – unable to work</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Senior management – deflection from priorities</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Opportunity cost / impact - what activity stopped because of a breach and how important was that activity</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Priority activities – assessment, enrolment, clearing, on-boarding</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Value of lost, damaged, or stolen outputs, data, assets, or intellectual property</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Legal costs</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Type / scale of impact</td>
<td>No impact</td>
<td>Some impact</td>
<td>High impact</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------</td>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Longer term and strategic</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Loss of students and student income</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Loss of other forms of income and / or research funding</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Loss of productivity</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reputational damage – IT and / or institutional</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cost of investigation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cost of fines e.g. ICO penalties</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Onward impact on connected organisations (suppliers, partners, on campus businesses – e.g. loss of earning from shops and cafes)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Contact us

Find your Jisc account manager [jisc.ac.uk/contact/your-account-manager](http://jisc.ac.uk/contact/your-account-manager) – we are ready to discuss any, or all aspects contained within this document.