Cyber impact 2022

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

Observations, advice and questions to ask

April 2022
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.

How do I get help with cyber security?

If you are suffering from a cyber security attack, need assistance, or wish to share information about an incident contact Jisc CSIRT, on irt@jisc.ac.uk or call 0300 999 2340

To find out how to strengthen your security posture contact help@jisc.ac.uk or speak to your Account Manager jisc.ac.uk/contact/your-account-manager

Who authored this report?

Version 1 of this report was published in November 2020 and was 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 provided an independent lens to ensure the information and recommendations in this report reflect the needs and observations of the Further Educations and Skills (FES) and Higher Education (HE) sectors.

Version 2 published in April 2022 has been updated by Jisc to reflect more recent incidents and associated guidance.

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

6 Questions you need to ask to assess your cyber security posture

8 Cyber security context
   Jisc CSIRT incident tickets breakdown 2021
   Sector lens
   Institution lens
   Personal lens
   Timing lens

12 Cyber security impact

22 Reducing and managing cyber impact and risks
   Leadership
   Technical ‘basics’
   Awareness and training
   Certification
   The role of cyber insurance

26 How Jisc supports and protects HE institutions and FES providers

28 Appendix - cyber security impact checklist
   Recovery impact
   Direct impact
   Long term and strategic impact
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 2021 cyber posture survey and also from other sources - including deep-dive interviews with 16 institutions (12 universities and 4 further education and skills providers) undertaken for the 2020 cyber impact report. We have avoided naming specific institutions and are acutely aware of the sensitive nature of cyber attacks.

We noted in Version 1 that COVID-19 was challenging all aspects of our education ecosystem as both further and higher education institutions developed new ways to deliver learning and teaching. Personal data and information are increasingly held on devices outside of institutional premises. Protecting that information, wherever it exists, has extended existing security challenges and as we will show, some of the responses to these challenges over the past two years have inadvertently led to some major security incidents occurring.

Every UK institution is working hard to reduce the likelihood of a breach occurring and the impact should one occur, and the survey results show institutions are becoming more prepared. However, 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.

The cyber security impact examples we present in this report highlight the breadth of incidents – 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 tremendously over the last few 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, university and research organisation 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.
## Questions you need to ask to assess your cyber security posture

The following questions address areas covered in this report and provide a useful starting point for discussions between senior leaders and IT and security professionals. Combined with the impact checklist in the appendix, this report should allow for specific actions to be implemented that will increase security posture and mitigate against some of the disruptive and costly cyber security attacks illustrated here.

<table>
<thead>
<tr>
<th></th>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Do we have a data classification scheme to help identify sensitive information and ensure appropriate protections are in place?</td>
</tr>
<tr>
<td>2</td>
<td>Do we have effective mechanisms for controlling access to resources, such as how we handle new starters, movers or when staff leave our organisation?</td>
</tr>
<tr>
<td>3</td>
<td>Do we review user accounts and systems for unnecessary privileges on a regular basis?</td>
</tr>
<tr>
<td>4</td>
<td>Do we enforce multifactor authentication for all systems and users?</td>
</tr>
<tr>
<td>5</td>
<td>Do we have a tried and tested process for backing-up critical data in a manner resistant to disasters or cyber attacks?</td>
</tr>
<tr>
<td>6</td>
<td>How long will it take us to recover critical business functions, assuming a loss of all infrastructure? What's the business impact of a loss of all digital infrastructure? How will we lead and coordinate business recovery in this scenario?</td>
</tr>
<tr>
<td>Question</td>
<td></td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>7. Can the business tolerate a recovery period that could take several weeks or months? How is this affected by different critical time periods for our business?</td>
<td></td>
</tr>
<tr>
<td>8. Do we have regularly rehearsed plans to deal with the most likely cyber events or disasters?</td>
<td></td>
</tr>
<tr>
<td>9. Are all of our hardware and software products free from vulnerabilities, supported by the vendor and regularly patched?</td>
<td></td>
</tr>
<tr>
<td>10. Are our networks separated so that if an attacker gets access to one device, they will not have access to our entire estate?</td>
<td></td>
</tr>
<tr>
<td>11. How would our organisation identify an attacker’s presence on the network?</td>
<td></td>
</tr>
<tr>
<td>12. Do we regularly review our cyber risk management approach to ensure that the ways we have decided to manage risks remain effective and appropriate?</td>
<td></td>
</tr>
<tr>
<td>13. Are all staff aware of and participate in effective cyber risk management processes?</td>
<td></td>
</tr>
<tr>
<td>14. Are we doing everything necessary to support our staff, students and stakeholders to understand and be aware of cyber risk, via training advice and guidance?</td>
<td></td>
</tr>
<tr>
<td>15. Do we maintain an accurate record of our technology assets, including hardware, software, firmware, peripheral devices and removable media?</td>
<td></td>
</tr>
<tr>
<td>16. Do we adequately understand our business-critical services and functions and their associated data, technology and supply chain dependencies?</td>
<td></td>
</tr>
</tbody>
</table>
Cyber security context

We present the nature of the FES 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. This assessment is unfortunately still valid in 2022 and is evidenced by the ransomware incidents that have severely impacted institutions over the last couple of years.

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. Institutions need to understand and be ready to defend against both. 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 scale of the challenge is clear with the breadth of incidents seen on the Janet Network illustrated in the chart on the following page. Over the past few years, Jisc’s computer security incident response team (Jisc 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 Jisc 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 main development since our first cyber impact report has been the spate of ransomware attacks, with 15 FES and HE organisations impacted by ransomware in 2020, 18 universities and FES providers impacted in 2021 and at least 3 so far in 2022. Schools in the UK have also been affected by ransomware, with at least 13 school sector bodies hit with ransomware since March 2021 affecting more than 100 individual schools.

Ransomware attacks have also evolved over this time, with more threat actors applying ‘double extortion’ to their attacks, meaning not only are they demanding a ransom to provide a decryption key, but are also threatening to make sensitive data public if the ransom isn’t paid. There have also been instances where attackers have sought out backups in order to hamper recovery and apply further pressure on the victim organisation to give in to their demands.
A denial of service incident may contain multiple attacks. These 601 incidents contained more than 1,100 DDoS attacks.
We have observed four lenses through which the cyber security threat can be viewed.

**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.

Research-intensive universities are partially dependent upon private sector research partners for income and research integrity. Maintaining cyber security reputation and credentials matters to these partners. Universities cannot afford to allow cyber attacks to disrupt these relationships and the research intellectual property that they must protect.

**Institution lens**

In a change from the previous three years, according to Jisc’s 2021 cyber posture survey, ransomware/malware is the top threat identified in HE and FES. This is unsurprising given the unprecedented number of ransomware attacks in the past 2 years. Phishing/social engineering is the second most mentioned threat for both HE and FES sectors followed by unpatched security vulnerabilities (HE) and accidental data breaches (FES).

Cyber attack commoditisation does not help – a denial of service attack can be purchased online for as little as $5. Research-intensive universities tell us that they believe state-sponsored attackers are here for the foreseeable future and may possibly align with sophisticated cyber-criminal organisations, particularly within the context of an increasingly unstable geopolitical landscape.

There is evidence, too, of highly targeted FES and HE attacks where cyber criminals have researched institution staff and processes as the basis of specific attacks. This is all too easy as many institutions have full organograms, with names, job titles and direct email and phone contact details on their websites.

**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 FES and HE sectors. Student tuition fee fraud attempts continue to impact those working and studying within UK institutions.

**Timing lens**

August 2020’s series of ransomware attacks led to NCSC issuing a UK education cyber security alert in September, which was further updated in March and June 2021. 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. Threat actors also frequently launch attacks at times when staff are less likely to be ready to detect and respond, such as during evenings, weekends and holidays. This pattern has led to authorities in the UK, US and Australia issuing an alert, and is something Jisc CSIRT has been painfully aware of within the UK education sector too.
How has COVID-19 changed cyber security activities?

The change in the types of incidents following the move to more remote or hybrid working has continued, as have the challenges. Threat actors have always used news and current events in their attacks and we continue to see phishing attempts and smishing attacks (scam SMS text messages) using messaging about the pandemic.

COVID-19 has led FES and HE organisations to accelerate the deployment of multifactor authentication (MFA) roll outs and this has led to a sharp rise in the number of institutions reporting having MFA in place in the 2021 Jisc Cyber Security Posture Survey.

The mass migration to remote working inadvertently opened institutions to attack by implementing insecure remote access solutions. Insecure configuration of the Remote Desktop Protocol (RDP) for example, was a key factor in ransomware attackers gaining initial access to victims’ devices. This underlines the importance of basic security controls being in place, such as protections against brute force attacks (an attacker submitting many passwords with the hope of eventually guessing correctly). These protections can include having strong, unique passwords, limiting the number of login attempts, as well as implementing MFA.

"We are doing our best, but all areas of IT support seem to be growing and requiring more attention and it’s one part of a larger role (where its importance should be far greater). The pandemic has only stretched us further."

FES provider
Cyber security impact

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 2021 IBM and Ponemon Institute Cost of a Data Breach Report puts the education sector average cost of a data breach at $3.79m (a very slight decrease from the 2020 figure of $3.9m). Healthcare continues to have the highest global industry average of $9.23m.

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. From Jisc CSIRT’s work in helping HE institutions and FES providers recover from ransomware incidents, we are aware of impact costs exceeding £2m.

Interestingly, the IBM and Ponemon report found that organisations that had both an incident response team and that had tested their incident response plans experienced data breach costs of almost half of those without either.

Jisc’s posture survey 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.

For other types of cyber security incident, previous Jisc cyber security posture 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 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 in the following pages.
From the Jisc cyber security posture survey findings it is clear that few institutions have so far appointed a chief information security officer (CISO) role – 24% of HE (though this rises to 50% of large HE institutions) and just 8% of FES providers have a formal CISO position, however anecdotally we are aware of many more individuals performing a CISO-like role, taking on responsibility for strategic leadership of cyber security in their institution. When appointing a CISO, there needs to be a recognition for and understanding of the CISO role and its position within the institution to ensure that person has the authority to make the required big decisions. However, care must also be taken to not overburden the role – there have been many stories in the press about ‘CISO burnout’ - so there is a need to ensure that there is accountability without blame; that there is understanding that cyber security is a whole organisation responsibility; and the acceptance that security will never be ‘done’. These dimensions make the CISO role challenging day-to-day, even in the absence of any incidents.
Recovery impact

In a previous posture survey (2020) staff time to deal with incidents was the biggest reported impact for both HE and FES.

Feedback also suggested that incident recovery is not always tracked in terms of IT and other staff effort. The findings also showed that post-incident, cyber security investment was often accelerated rather than newly justified because of that incident. Nonetheless, specialists (e.g. database/system forensic) can cost more than £1,200 per day and could result in costs of tens of thousand pounds to recover key 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 delayed or cancelled because of a security breach or incident.

**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 around 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 about 40 accounts, leading to recovery costs of ~£30,000 over 12 months. Two attacks took one member of staff a week to resolve.

**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.

**Phishing breach affecting university supply chain**
In 2020, a university suffered 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 retrieved.
**FES Data breach**
In early 2022, a FES provider was subject to an attack that led to college systems being accessed and data stolen. Due to the security controls in place, the attack was recognised quickly, but to mitigate against further data exfiltration, access to systems was restricted, which caused disruption for staff and students for a number of days while the incident was investigated and remediated.

**FES malware outbreak**
March 2021 saw a college experience a security incident when malware was detected across its network. Third party assistance was required to investigate and remove the malware as well as to provide advice and guidance on hardening infrastructure to minimise the risk of a similar incidents occurring.

**School revenge attack**
A ‘bored’ ex-employee accessed a school’s IT systems in January 2021 erasing school and personal data, causing a 10-day outage, impacting remote learning. Data on 125 devices was erased, including personal devices belonging to 39 families, leading to loss of GCSE course work and personal photos.

**University ransomware attack**
A 2020 ransomware attack affected one university researcher who lost research data – although it was backed up. Days of reformatting effort resulted, but the nature of the attack led to a further 10 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.
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 FES and HE take the protection of personal data extremely seriously, and although only one six figure ICO fine has occurred within the sector, other institutions have been subject to ICO investigations. FES providers and universities have told us of that the impact 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 is substantial.

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”.

University / research malware attack
In May 2020, more than 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 crypto currency programmes.

Fraudulent email breaches
A FES provider described in 2020 how £10,000 was extracted from payroll via a fraudulent email sent to a vice principal. Another FES provider paid a hacker £10,000 – the hacker had investigated and circumvented institutional processes. A university shared details of a phishing-based incident that resulted in three staff members’ salaries being diverted for one month, costing the university around £10,000.
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 200 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 £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.

US university ransomware attack
The University of California paid, in 2020, $1.14m to regain control of data. According to an IBM/Ponemon ‘2021 Cost of a Data Breach’ report, the average cost, across all sectors, of a ransomware attack is $4.62m.

Microsoft Exchange Server vulnerabilities
In March 2021, organisations were alerted that vulnerabilities in Microsoft Exchange Servers were being exploited by the Hafnium Group – a threat actor known to have targeted a variety of sectors, including universities and colleges. Institutions were strongly advised to patch systems as a matter of urgency, causing staff to react quickly and diverting them from other activities.

State-sponsored phishing attacks - Silent Librarian
The US Dept of Justice cited a cyber crime 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 that the Silent Librarian credential phishing campaigns have continued over subsequent years.

Research ransomware attempt
The NCSC’s 2021 report highlighted how the UK’s lead agency for cyber security helped the University of Oxford’s COVID-19 vaccine researchers protect themselves from attempted ransomware attack. If successful, the attack could have caused significant disruption to the UK’s pandemic response.

State-sponsored phishing attacks - Silent Librarian
The US Dept of Justice cited a cyber crime 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 that the Silent Librarian credential phishing campaigns have continued over subsequent years.

UK FES and HE ransomware attacks
March 2022 saw one FES provider and two universities impacted by separate ransomware attacks. Each incident has caused significant impact to parts of the organisation as systems were taken down to prevent further spread of the malware and to safely recover and restore data. In one case third party data recovery services were required.

Ransomware during clearing
Eight institutions were hit by ransomware during the 2020 clearing and enrolment period leading to a significant direct impact for those organisations and a knock-on effect for the entire sector as proactive work to mitigate similar attacks was launched across education and research in the UK.

Dutch research funding agency
February 2021 saw reports of internal documents from the Netherlands Organisation for Scientific Research being published after the agency refused to pay a ransom. Following the attack meetings were disrupted for a month and the ability to pay or receive bills was affected.

Microsoft Exchange Server vulnerabilities
In March 2021, organisations were alerted that vulnerabilities in Microsoft Exchange Servers were being exploited by the Hafnium Group – a threat actor known to have targeted a variety of sectors, including universities and colleges. Institutions were strongly advised to patch systems as a matter of urgency, causing staff to react quickly and diverting them from other activities.

Research ransomware attempt
The NCSC’s 2021 report highlighted how the UK’s lead agency for cyber security helped the University of Oxford’s COVID-19 vaccine researchers protect themselves from attempted ransomware attack. If successful, the attack could have caused significant disruption to the UK’s pandemic response.

State-sponsored phishing attacks - Silent Librarian
The US Dept of Justice cited a cyber crime 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 that the Silent Librarian credential phishing campaigns have continued over subsequent years.

UK FES and HE ransomware attacks
March 2022 saw one FES provider and two universities impacted by separate ransomware attacks. Each incident has caused significant impact to parts of the organisation as systems were taken down to prevent further spread of the malware and to safely recover and restore data. In one case third party data recovery services were required.

Ransomware during clearing
Eight institutions were hit by ransomware during the 2020 clearing and enrolment period leading to a significant direct impact for those organisations and a knock-on effect for the entire sector as proactive work to mitigate similar attacks was launched across education and research in the UK.

Dutch research funding agency
February 2021 saw reports of internal documents from the Netherlands Organisation for Scientific Research being published after the agency refused to pay a ransom. Following the attack meetings were disrupted for a month and the ability to pay or receive bills was affected.
Microsoft Print Spooler Zero Day
IT and security teams within HE and FES providers were impacted by the seemingly endless vulnerability alerts issued by Microsoft in July 2021 related to the Windows Print Spooler. Dubbed Print Nightmare, a series of vulnerabilities that were being actively exploited were discovered. Due to the potential severity of an attack, many institutions took the decision to disable all printing across the organisation until the vulnerabilities were fixed. This also impacted any systems that used the Print Spooler to generate PDFs and other documents - not just physical documents.

University ransomware attack
Maastricht University publicly shared its experience of an attack that occurred on 24 December 2019. A successful ransomware attack led to c200 staff (central and faculty IT services, lectures, student advisors and psychologists, timetable schedulers, finance, HR, legal, library estates) working to address the impact of the attack and to ensure all systems and processes were 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 the Dutch parliament as a “wake up call for the entire education sector” and illustrates the recovery effort as well as direct monetary impact. In the UK, the Government, NCSC and Jisc have all advised that ransoms should not be paid. Organisations known to pay ransoms can become targets for further attacks and, in the case of education providers, paying could be a breach of funding agreements. There is also no guarantee that payment will lead to recovery.

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 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.

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 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.

US school sector insider breach
Student grade information, as well as confidential sensitive information of employees, students and their parents enrolled or employed since 2010 were accessed and downloaded from servers of the Dallas Independent School District by two students.

Schools impacted by ransomware
In March 2021, more than 90 schools were affected by five different ransomware incidents. One of the academy trusts impacted was reported to have received a demand for $15m.
Long term and strategic impact

The exposure of personal data could affect reputation, though there is little evidence of significant reputational 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. Sustained attacks would most likely have a significant impact – a previous FES Jisc ‘value study’ suggested that students might move FES provider if systems (and therefore student access) were impacted over a number of weeks.

Serious cyber security incidents can have a long-lasting impact, both positive and negative. Remediation and recovery may take weeks or even months in some cases, but the emotional impact on staff and students can last much longer. 2020’s ransomware incidents illustrate the impact of successful attacks during the critical clearing and enrolment period of August and September, with eight Jisc members affected, with one suffering results day systems losses. The steps taken to recover from such attacks also highlight the innovation that exists across the FES 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. 2020 saw 15 FES and HE organisations directly affected by ransomware and 2021 saw even more with 18 organisations affected. These attacks have led to the entire sector operating at a heightened level of awareness and putting in place controls to mitigate any future attacks.

A number of the affected institutions spent months to resolve cyber attacks, with some having to cancel exams and periods of learning and teaching were disrupted due to key systems being unavailable. Students were told there would be no access to the campus for a brief period and online platforms were 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.
Supply chain security incidents
Late 2021 saw two international partners of multiple universities experience cyber security incidents. Bad practice at each company led to multiple credentials being exposed. Although there has been no direct proof that credentials had been exploited in any way, the investigation, rectification and ensuing delays with recruitment and payments led to cost and time impacts for institutions, students and the suppliers. Rectifying the situation and endeavouring to obtain assurances that good practice was subsequently being followed has led to a commitment to develop a coherent approach to responding to such incidents in the future.

Widespread critical vulnerabilities
In December 2021, a vulnerability in the widely used Log4j logging tool was disclosed. Affecting millions of computers worldwide, the timing was particularly concerning for universities and FES providers due to the proximity to the Christmas holidays. Staff across institutions from IT, security, procurement and other roles spent many days assessing their own exposure and checking with supply chains. Given the widespread usage of Log4j, it is likely that this vulnerability will continue to have an impact for years to come and underlining the importance of taking both supply chain security and vulnerability management seriously.

Students - spotlight
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 to raise collective awareness of the tactics and techniques criminals employ. Institutions need to:

- publicise how criminals exploit current events;
- help people to anticipate and expect scams;
- demystify and de-sensationalise criminal activity;
- explain the signs of a scam;
- encourage people to report scams and make it easy to do so;
- ensure victims are supported and not penalised.

One university shared that, in one year, around 200 student and staff members had fallen for voucher scams resulting in hundreds 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 2021 Jisc posture survey suggested that perceptions of cyber security protection are not high with only 17% scoring their (HE) organisation as 8+, although this is an increase of 7% on the previous year. Perceptions in FES were more positive at 31%, however this was a 5% decline from 2020. Comments suggested that organisations exercised caution when scoring and felt there is always more that can be done, particularly considering threats to the sector. Even for those who scored 8-10, the need to introduce new products and systems and importance of increasing awareness and training were key themes.

Through the Jisc posture survey, 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 2021). This supplies a solid foundation to build upon. Continued leadership awareness, knowledge, and understanding of the nature of cyber threat, and 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 ease of protecting them. Support to implement necessary changes across all departments is, therefore, critical. At the same time, this compartmentalisation makes it hard for institutions 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 properly resourced and skilled cyber security staff – either internally or via managed services – to plan and implement solutions across the institution’s systems estate.

NCSC’s 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 (2021) shows us that both HE and FES sectors are more likely to deploy MFA to staff than students. 87% of HE and 87% of FES indicate some form of MFA deployment for staff, dropping to 49% (HE) and 13% (FES) for students. Reasons given for non-deployment included 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.

One FES provider that has implemented MFA for all students – more than 40,000 of them across seven colleges – has blogged about their experience, highlighting the following advice:

- This has to be led from the top with Exec/Principal support
- Students are more than likely already using MFA and if they aren't then you are providing them with not only life skills but skills they can take to the workplace, as most organisations will now use MFA.

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 (2021) showed a slight decrease in the proportion of HE organisations achieving Cyber Essentials (CE), CE Plus and ISO27001. Again, this is likely to do with the increased sample size for the latest survey, however comments from the sector suggest that home working, reduced priority, bring your own device and changes to the Cyber Essentials scheme may all have been a factor. The survey recorded that 60% of universities have achieved CE, 29% CE Plus and 6% ISO27001. Certification penetration in FES has continued to grow, with 67% FES providers having achieved CE, 31% achieving CE Plus and for the first time in five years of running the cyber security posture survey, six colleges reported having achieved ISO27001 certification.
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.

The role of cyber insurance
Jisc’s (2021) posture survey showed an increase in the number of organisations with cyber insurance compared to the 2020 results. It discovered that 47% of HE institutions indicate they had some form of cyber security cover, with FES providers exceeding this – 72% have either a specific cyber policy or cover as part of a broader policy.

As with the 2020 survey, the 2021 results showed that insurance claims for cyber security breaches remain uncommon. Only seven HE institutions (out of 44 that stated they had such insurance cover) reported making cyber insurance claims in the current or previous academic years. And only five out of the 44 FES providers that stated they had cover had made a claim.

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.

The past two years has both shown the benefit of cyber insurance and raised a number of issues with it. Some institutions who have been impacted by ransomware have been grateful for the support provided in having insurance cover, but due to the huge increase in attacks globally, the insurance market has changed dramatically. Anecdotally we are aware of institutions seeing large increases in their premiums or being unable to renew their insurance. One university reported that at renewal their premium had a zero added to it and their cover had a zero removed. We are also aware that cyber insurance providers are imposing requirements on technical controls before providing cover.

We know that on occasion, insurance companies have instructed institutions to not share details of their particular incident with any third party. Institutions are encouraged to ensure that their insurers appreciate the need to advise Jisc and exempt Jisc CSIRT from that policy requirement so that help can be provided for no additional cost as part of Jisc membership. The sooner Jisc 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.
Reducing and managing cyber impact and risks
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 procurement frameworks, training, and JiscMail lists to help cyber security professionals stay in touch with the latest developments. Security professionals working in education or research sector roles can join the cyber security community group - a trusted community that helps Jisc members increase their security posture by providing helpful peer-to-peer support and meaningful content.

Further information on Jisc’s cyber security services can be found at https://www.jisc.ac.uk/cyber-security

Core service included in Jisc subscription

Optional Jisc service
<table>
<thead>
<tr>
<th>Jisc service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Incident response</strong></td>
<td>Jisc CSIRT</td>
</tr>
<tr>
<td><strong>Protecting staff, students and assets</strong></td>
<td>Janet Network resolver</td>
</tr>
<tr>
<td><strong>Network defence</strong></td>
<td>Foundation DDoS mitigation</td>
</tr>
<tr>
<td></td>
<td>Critical services protection</td>
</tr>
<tr>
<td><strong>Resilience</strong></td>
<td>Primary / secondary nameserver service</td>
</tr>
<tr>
<td></td>
<td>Network time service (NTP)</td>
</tr>
<tr>
<td><strong>Identify threats</strong></td>
<td>Managed SIEM</td>
</tr>
<tr>
<td></td>
<td>Splunk</td>
</tr>
<tr>
<td><strong>Certifications, audits and assessments</strong></td>
<td>Cyber Essentials</td>
</tr>
<tr>
<td></td>
<td>Cyber Essentials Plus</td>
</tr>
<tr>
<td></td>
<td>Cyber security financial X-ray</td>
</tr>
<tr>
<td><strong>Evaluate and improve the security of your institution</strong></td>
<td>Cyber security assessment</td>
</tr>
<tr>
<td></td>
<td>Penetration testing</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 impact**
This report has highlighted that the involvement of senior management, teaching and research staff often supplements cyber security/IT effort adding to direct costs involved in recovery from a breach.

**Direct impact**
Our interviews suggest that few institutions track and calculate the impact of a cyber related breach beyond the recovery aspects. 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 be more 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. The impact on staff and student mental health and wellbeing must also not be underestimated.

**Long term and strategic impact**
Feedback suggests few institutions 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 fines issued by the Information Commissioner’s Office.
<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><strong>Recovery</strong></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><strong>Direct</strong></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 an incident and how important was that activity</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Priority activities – assessment, enrolment, clearing, onboarding</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>Longer term and strategic</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
- we are ready to discuss any, or all aspects contained within this document.