Higher Education Policy Institute

How safe is your data? Cyber-security in higher education

Dr John Chapman,
Head of Jisc's Security Operations Centre

HEPI Policy Note 12

April 2019

Introduction

It is exam time and students across a university are using the Virtual Learning Environment to help with their revision. Suddenly the page they are on stops responding. They try refreshing it. The page still will not load. They visit another web page – that does not load either. The institution has just suffered a complete network outage thanks to a Distributed Denial of Service (DDoS) attack targeted at disrupting teaching and learning.

A member of staff is browsing the internet on a university computer. They visit a website that has had malicious code inserted into it. This code downloads software to the university machine, which starts spreading through personal and shared access drives, preventing access to all files and folders. Infected machines display a message saying 'Attention! Price of software and your private key is 0.5 bitcoins. With this product you can decrypt all your files.' The university has suffered a ransomware infection.

Higher education regularly experiences these kind of scenarios and some institutions have been highly affected for days after cyber attacks. Organisations that do not adequately protect themselves risk the loss or exposure of personal student and staff data and also commercial, institutional and research data that are valuable to cyber criminals operating domestically and internationally. Such incidents are not going away, with 173 different higher education providers engaging with Jisc's Computer Security Incident Response Team during 2018 – a 12 per cent increase on the previous year. **It is critical university leaders consider whether their cyber protection governance is sufficiently robust.**

The growing risk of cyber threats is well reported. Distributed Denial of Service attacks targeting higher education institutions are on the rise and successful breaches can make headline news (as experienced by the University of Edinburgh in 2018).[1] State-sponsored attacks targeting research data and intellectual property have also been widely publicised.[2] It is clear that protecting networks and data should be a high priority for higher education leaders. But do institutions fully understand the scale of the risk?

We are not confident that all UK higher education providers are equipped with the adequate cyber-security related knowledge, skills and investment.

In order to assess the risks they face and to benchmark their position on security, there are a number of basic questions that higher education providers ought to be asking now:

- Where is data stored?
- Who has access to data?
- Are systems patched and up to date?
- Are regular vulnerability scans performed as part of a vulnerability management policy?
- Are staff and students trained in information security awareness, to help them spot fraudulent emails, to know how to look after their data and how to report when things go wrong?
- Is there an incident response plan in place?
- Who should be contacted when additional help or guidance in needed?
- Do attack monitoring and mitigation systems cover the right cyber risks?
- Is the network provider mitigating denial of service attacks, which could bring down the network?

This paper discusses:

- the current security landscape for UK higher education and research;
- the types of incidents higher education providers face that could lead to significant data breaches or loss of access to data;
- the types of questions governors and students should be asking their institutions' leadership teams; and
- the minimum requirements and tools providers should have in place as a framework for protecting themselves and the sector as a whole.

Current security landscape

When it comes to cyber-security, and unlike most sectors, UK higher education and research has the advantage of operating on its own bespoke network – the Janet Network. This has built-in cyber-security measures delivered by Jisc's Security Operations Centre. However, while Jisc provides protection over the Janet Network, universities are ultimately responsible for their own cyberspace and for safeguarding their massive datasets.

Universities are naturally open environments both physically and academically and it is important they retain that open culture. A careful balance must be struck between openness and safety. However, it appears that, in general, universities are not confident about their cyber-security protection.

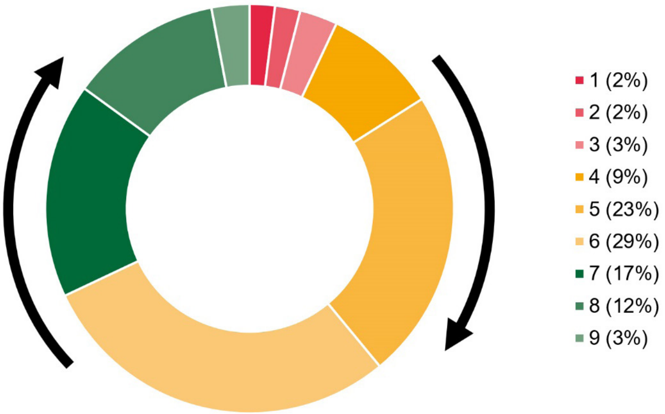
In the spring of 2018, Jisc surveyed university information technology and security staff to better understand their security position.[3] The results demonstrate that perceptions of cyber-security protection are fairly negative.

Only 15 per cent of higher education IT and security staff scored their organisation as eight or more out of 10 on a scale where one means 'Not at all well protected' and 10 means 'Very well protected: comprehensive controls in place'. The mean score was 5.9.

The reasons given for this relatively low figure include a lack of dedicated staff and budgets and a lack of policies, suggesting senior leaders are not taking the issue seriously enough.

Another 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 higher education institution (52 per cent), only 39 per cent feel they are told about how their data is stored and used by their university.[4]

Cyber security protection perceptions



High-profile data breaches and cyber-attacks make headlines, but the barrage of such news may lead to complacency. Viewed in the abstract, it becomes almost background noise. Higher education institutions should think about the value of their data and their students' data. How damaging could it be to your institution if it were to suffer an information security breach?

Major data breaches in 2018:

- Marriott Hotels (500 million customer records)
- MyFitnessPal (150 million records)
- Quora (100 million user accounts)
- MyHeritage (over 90 million accounts)
- Facebook (up to 90 million accounts)

State-sponsored attacks

Despite the millions of data breaches reported from multinational companies, the theft or exposure of academic data is not widely publicised. This may change with greater awareness of General Data Protection Regulation (GDPR) and the responsibility it places on organisations to report breaches to the Information Commissioner. But in recent months the only public story featuring a UK higher education institution was about Greenwich University's fine of £120,000 for holding data on an unsecured server.[5]

Many such incidents at universities are not big enough to trigger national media interest, but any of them could still cause personal, financial and reputational harm.

The massive breaches that hit the headlines tend to be focussed on personal data, which higher education institutions also store, with millions of records for staff, students and alumni across the sector. But institutions also have incredibly valuable and commercially-sensitive research data of interest to organised criminals and some unscrupulous nation states.

There were two such large-scale incidents that affected higher education institutions in 2018.

1. Iranian hackers (affiliated to a criminal organisation called the Mabna Institute) targeted UK universities via the 'Silent Librarian' campaign.[6]
2. Stolen Pencil – a North Korean group – targeted individual academics with emails designed to trick them into downloading a malicious extension to the Chrome web browser.[7]

Criminal attacks

Organised criminals play a large part in cyber-attacks, particularly phishing attacks, which means using malicious emails to trick the recipient into clicking through to a fake website and entering a username and password.

Jisc sees a number of examples of such attacks against colleges, universities and research centres. During 2018, we noticed phishing attacks becoming more sophisticated and better targeted towards the education sector. For example, around the beginning of term, particularly at the start of the academic year, there has been an increase in student grant fraud. This is where students are sent phishing emails purporting to offer free grants or requesting bank details are updated so that loans can be paid.[8]

'Spear phishing' attacks, where specific individuals are targeted with requests for information, have also become increasingly common. One example includes 'CEO fraud' where criminals send urgent transfer requests via email to finance departments, impersonating senior members of staff in an attempt to trick them into transferring funds into the fraudster's bank account. Jisc's own Chief Executive and Finance Department have been targeted in this way.

The Jisc Security Operations Centre is aware of examples of this type of approach being targeted at higher education institutions. One case involved fraudsters using a senior staff member's name via a Gmail account in an attempt to convince a staff member to purchase a gift voucher on their behalf.

The fraudster stated it was needed for an urgent birthday present and that they were unable to buy the gift themselves due to being in a meeting all day. They requested images of the voucher, including the PIN code, be sent to them. In this instance, the spelling and grammar was noticeably poor so the event was recognisable as a fraud attempt by a third party.

A variant of this type of attack is where the email asks the recipient to review an attached document. The attachment then contains a link to 'unlock the document' which then leads to a web page that tries to get the victim to enter their institution's credentials.

In both cases, the criminal has used the name of a senior member of staff, sending emails to people who work closely with them. The institution's departmental structures were published on the university website, making this an easy thing to do for the attacker.

Alarmingly, when using spear phishing as part of its penetration testing service, Jisc has a 100 per cent track record of gaining access to a higher education institution's high value data within two hours.

Security on the Janet Network

Jisc's Security Operations Centre handles more than 6,000 incidents or queries a year. Not all of them are related to data breaches, but some are and higher education institutions need to plan how to react when a breach does occur.

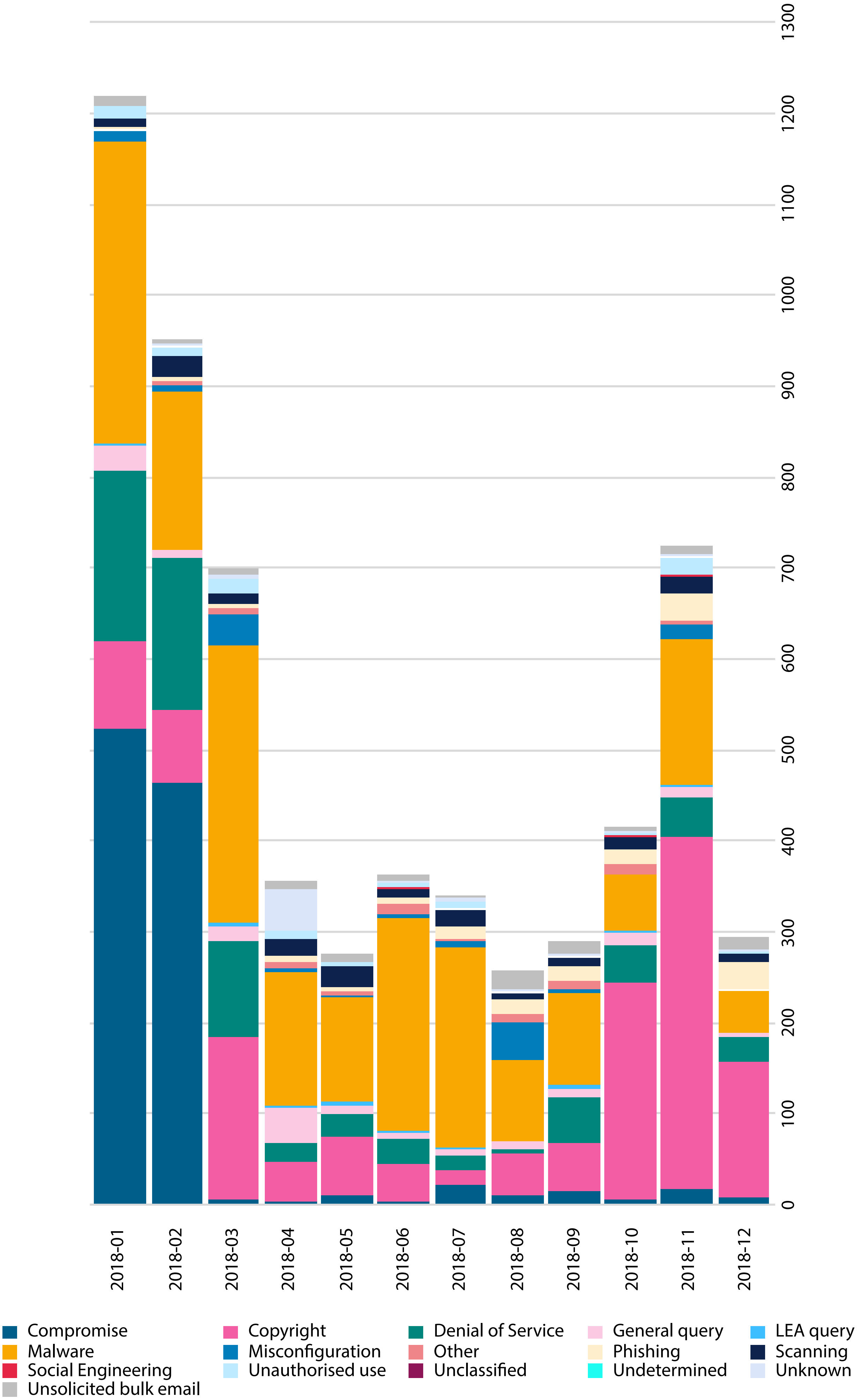
What would happen if a well-meaning administrator accidently emailed a sensitive file to a mailing list rather than an individual because they had not been trained on safe and secure methods of data handling? What if there were no vulnerability management policy in place so a security weakness on the institution's website went undetected, allowing access to the network by a criminal who can then siphon off commercially sensitive research data?

Denying learning and research

Security experts often talk about the 'CIA triad'.

- **Confidentiality** – preventing people that should not see data from having access.
- **Integrity** – ensuring data is not changed and remains accurate.
- **Availability** – being able to access data that you are authorised to see.

Most breaches are a failure of the 'C' and the 'I', but in academia the inability to access data or



Number and type of cyber-security incidents and queries handled by the Jisc Security Operations Centre January – December 2018 networks (Availability) due to a cyber-attack, such as a Distributed Denial of Service (DDoS) attack (designed to bring down a network) is a real threat. Being unable to access an online resource due to an attack may be just an inconvenience for a specific lecture or tutorial, but if the attack persisted or occurred at a particular time of the year – such as during Clearing – it could cause severe reputational and financial damage.

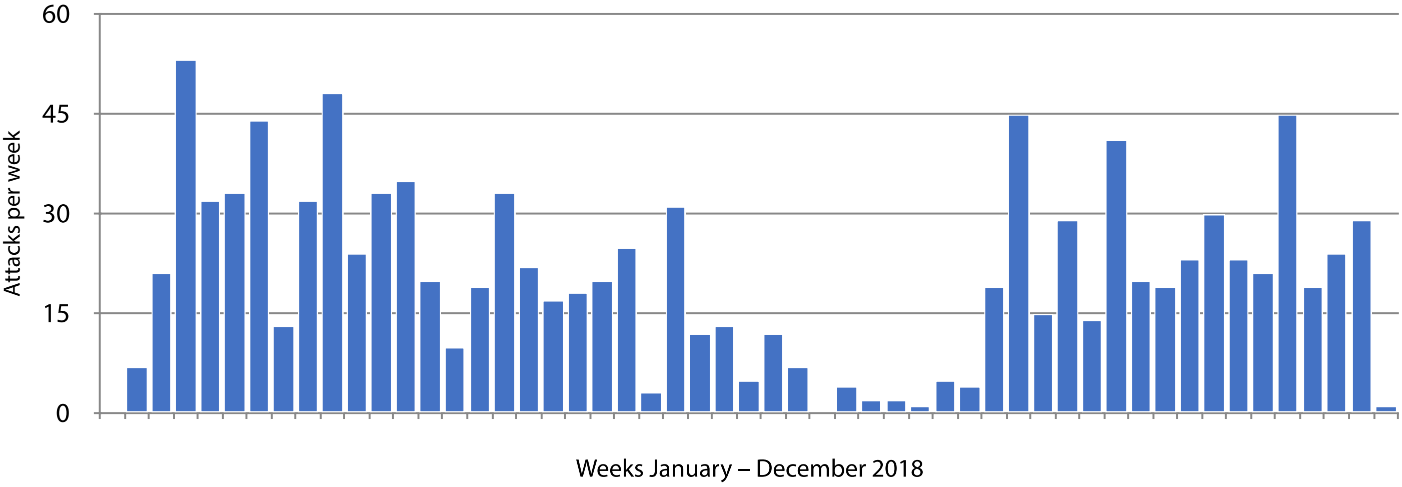
During 2018, more than 1,000 DDoS attacks were detected against 241 different UK education and research institutions. Analysing the timings of these attacks has led Jisc to surmise that many of them are 'insider' attacks launched by disgruntled students or staff.[9]

and processes are protected. A new British Standard – BS31111:2018 – has been developed to help governing bodies and executive management better understand the risks associated with IT activities and support decision making that ensures good cyber resilience. BS31111:2018 provides a framework to help board members identify, assess, and mitigate cyber-security risks within institutions' overall risk management framework.

As stated in the British Standard, executive management should be capable of providing evidence of:

a) what and where the value of digital investment is and what the cyber risks are, including negative and positive outcomes;

DDoS attacks against UK education and research organisations



b) the suitability of the level of preparation and the prevention and response capabilities available to manage a cyber incident;

c) how the organisation manages and understands change across the cyber landscape; and

d) the availability of adequate resources (for example financial, human, information, technology) to meet the principles and objectives defined in the cyber risk management and resilience policy.

Guidance for governing bodies and executive management

Cyber-security is the responsibility of all individuals, with every user having to make informed decisions about how they access and store their own data and how they behave when interacting with computer systems and networks.

This can be best achieved when there is a culture of working within their institution that best supports cyber-security. This means that the institution's governing body and executive need to provide the leadership that best ensures staff, students and researchers can protect themselves, the institution and their stakeholders from the consequences of accidental information security breaches and malicious cyber attacks.

Institutions must demonstrate that their operations

Too often, we are seeing cyber risk being managed solely by the information technology function, but this approach is a big mistake as cyber risks affect all operations and need to be included and addressed by the wider governance and management processes across the organisation. Cyber risk cannot be delegated away from the governing body and the executive management needs to be held accountable for ensuring that informed and appropriate decisions are being made which meet or exceed the expectations of any organisation's stakeholders – and the law.

Looking at cyber-security from a risk management perspective is often familiar for board members who should be used to making risk-based decisions. However, they may not be familiar with cyber-security or information technology. By using the framework provided by BS31111:2018, governing bodies will be able to determine how cyber-security risks are assessed, whether the appropriate policies are in place to manage cyber risks and whether there is appropriate capability and accountability within the institution.

Sector protection in a data-driven world

All students have a right to expect a basic level of IT and network infrastructure to be in place that meets robust, requisite security standards. This is even more important when their personal data can actually make a positive difference to their learning journey through the proliferation of learning analytics and other big data-driven innovations in higher education.

While UK higher education institutions in receipt of public funding benefit from connection to Jisc's Janet Network and the dedicated support of its Security Operations Centre, private providers are required to make their own cyber and data security arrangements.

This means there is a divergence in institutional approaches to cyber-security across the sector and some providers may not be providing students and staff with the robust and secure protection they should expect.

This needs to change. It is time for sector regulators to discuss what minimum cyber-security and network requirements higher education providers should have in place to maintain a robust, well-protected sector and keep students and staff safe.

Conclusion

The security landscape has been evolving over many years and will continue to evolve as the arms race between attackers and defenders continues.

It is imperative that those in higher education continually assess and improve their security capability and for higher education leaders to take the lead in managing cyber risk to protect students, staff and valuable research data from the growing threat of attack.

This paper also highlights how a national conversation between those with a vested interest in the protection of universities from cyber attack, including Government, should explore further steps to enhance resilience across this critically valuable sector.

Useful links

NCSC article highlighting relevant guidance for universities	https://www.ncsc.gov.uk/blog-post/defending-your-university-against-top-3-cyber-threats
BS 31111:2018 Cyber risk and resilience — Guidance for the governing body and executive management	https://shop.bsigroup.com/ProductDetail?pid=000000000030342527
Jisc	https://www.jisc.ac.uk/network/security

Endnotes

[1] https://www.thetimes.co.uk/article/edinburgh-university-hit-by-freshers-week-cyberattack-0m2xzl0p8

[2] https://www.independent.co.uk/life-style/gadgets-and-tech/news/iran-hackers-uk-university-cyber-attack-security-cobalt-dickens-a8506406.html;

[3] https://community.jisc.ac.uk/groups/security-products-and-services/article/cyber-security-posture-survey-2018-how-secure-are-you

[4] Jisc, Digital experience insights survey 2018: findings from students in UK further and higher education, 2018, p.10.

[5] https://ico.org.uk/action-weve-taken/enforcement/the-university-of-greenwich/

[6] https://www.fbi.gov/wanted/cyber/iranian-mabna-hackers

[7] https://asert.arbornetworks.com/stolen-pencil-campaign-targets-academia/

[8] https://www.moneywise.co.uk/news/2018-11-19/fake-tax-refund-scam-targeting-university-students-reaching-unprecedented-numbers

[9] https://www.jisc.ac.uk/blog/cyber-attacks-on-colleges-and-universities-who-when-and-why-14-sep-2018