Browne Jacobson

Cyber-attacks in UK universities: Why failing to prepare is no longer an option

02 April 2024

As UK universities increasingly rely on technology to conduct their operations, the threat of cyber-attacks looms large. With the rise of sophisticated cyber criminals and the rising value of research and personal data, it is no longer a question of if a cyber breach will occur, but when. Nathalie Jacoby-Danesh, Partner, and Heather McKay, Senior Associate at UK and Ireland law firm Browne Jacobson, explore the challenges faced by universities in responding to cyber threats.

Universities must take a proactive stance in anticipating cyber-attacks and implementing comprehensive cyber security measures to protect against them. The adage of "*failing to prepare is preparing to fail*" stands true now more than ever, and UK universities must be prepared to face the challenge of cyber threats head-on.

They are facing increasingly complex cyber threats, as cyber criminals and threat actors become more sophisticated in their tactics and as geopolitical actors may be looking for new targets.

Cyber threats can cause significant disruptions to a university's operations as well as substantial damages, including data breaches, financial loss and reputational damage.

In this article, we explore what steps UK universities can take to protect against these threats, exploring how the compliance lifecycle model can play a key part in preparing for and managing incidents. Taking these steps, they can reduce their risk of cyber-attacks and protect the sensitive data they hold.

Types of cyber threats in UK universities

UK universities face a variety of cyber threats, including phishing attacks, malware, ransomware, and distributed denial of service (DDoS) attacks.

Indeed, cyber criminals have become more sophisticated in their tactics, moving away from employing just one type of attack to combining multiple tactics. For instance, attackers may use ransomware to encrypt a university's data and then threaten to release sensitive information on the dark web if the ransom is not paid.

This type of attack can paralyse a university's research and other operations, causing significant financial damage including financial loss and reputational damage. As a result, universities must be vigilant in their cyber security efforts and implement a comprehensive cyber security program that includes employee training, IT security measures, and regular back-ups of critical data.

By taking these steps, universities can reduce their risk of falling victim to these types of attacks and protect the sensitive data they hold.

Phishing attacks are one of the most common types of cyber threats. They involve the use of fraudulent emails or links to websites to trick users into providing sensitive information, such as log-in credentials or financial information.

Malware is another common type of cyber threat that can infect a university's computer systems and steal sensitive information. Ransomware is a type of malware that encrypts a university's data and demands payment in exchange for the decryption key. DDoS attacks involve overwhelming a university's computer systems with traffic, making them inaccessible to users.

Case studies of cyber-attacks on UK universities

The 2020 Blackbaud Hack saw more than 20 universities and charities in the UK and abroad fall victim to a cyber-attack. It compromised a supplier of education administration, fundraising and financial management software, with affected data including personal information.

Another public sector body, the British Library, was the subject of an attack in October 2023 that resulted in the exfiltration and publication on the dark web of around 600GB of files, including personal data of library users and staff. No ransom was paid. The British Library published a very informative report in March 2024, which we would highly recommend to universities.

Across the channel, it has been reported that the University of Maastricht paid a ransom of nearly €200,000 to regain access to their computer systems following a cyber-attack in 2019.

It is the position of UK authorities that no ransom payments will be made to cyber criminals.

Prevention and mitigation strategies

To protect against cyber threats, UK universities can implement a variety of prevention and mitigation strategies. Employee training and awareness are critical components of any cyber security programme.

Universities should provide regular training to employees on how to identify and avoid phishing attacks, how to create strong passwords, and how to report suspicious activity. IT departments should also implement security measures such as firewalls, antivirus software, and intrusion detection systems. Regular back-ups of critical data should be performed to ensure that data can be restored in the event of a ransomware attack.

The compliance lifecycle

The compliance lifecycle is a three-stage process including preparation, incident management and learning lessons.

1. The preparation phase

This involves anticipating a cyber incident or data breach, implementing policies and procedures, and identifying a response team that will act promptly in the event of an incident.

2. Incident management

When an incident or potential incident has been identified, the response processes are triggered. The National Cyber Security Centre should be notified of the incident. The centre works 24/7 and it can support universities with advice and guidance in the case of an attack.

It works closely with partners from UK law enforcement, including the National Crime Agency, to ensure a joined-up response and it can also help co-ordinate a cross-government response if necessary. If the preparation phase is implemented well, the incident management phase should be like a well-oiled machine kicking into action.

The response team is mobilised with different sub-teams starting their work, including IT security, legal, regulatory compliance, finance and PR. This is understandably a stressful and time-critical phase, which is why good preparation is key.

3. Learning lessons

Finally, once the incident has been contained and remedied, reports must be written and digested, leading to the third stage of the compliance lifecycle, learning lessons. This phase feeds back into the preparation stage, allowing the university to return to business as usual with improved cyber security measures.

Legal implications of cyber-attacks in UK universities

Cyber-attacks on UK universities can have significant and wide-reaching legal implications, depending on the nature and scope of the attack and its impact on the university's operations. Possible implications include:

- **Personal data**: Universities have a legal obligation to protect the personal information of their students and employees under the UK General Data Protection Regulation (GDPR). In the event of a data breach, universities may be liable for damages and face legal action. Additionally, universities have an ethical obligation to protect the privacy of their students and employees. Cyber-attacks that

compromise sensitive data can cause significant harm to individuals, including identity theft and financial loss. Universities should handle any student complaints about the impact of a cyber-attack on their privacy and personal data in accordance with its Complaints procedure. If a significant number of students complain about the same incident, universities should consider dealing with them as a group complaint.

- **Breach of the student contract:** An attack can compromise the education provided to students, for instance if teaching cannot proceed as planned or if a research project can't be completed as intended. The university will need to carefully handle any resulting disruptions to the students' experience in order to avoid student complaints. Universities should handle any student complaints about the impact of a cyber-attack on their learning or research in accordance with its Complaints procedure. If a significant number of students complain about the same incident, universities should consider dealing with them as a group complaint.
- **Breach of collaboration agreements**: The university may be precluded from abiding by its obligations under collaboration agreements with academic or industry partners, and will have to mitigate as much as possible negative consequences for itself and its partners. Contract amendments may need to be agreed at short notice in order to avoid liability for breach of contract.
- **Breach of funding conditions**: The disruption caused by an attack may prevent the university from complying with grant funding conditions (for instance by making it impossible to complete certain projects within the proposed timeframe). Funders may need approaching on a confidential basis, at short notice, in order to agree exceptional extensions or changes to the terms of funding.
- **Regulatory implications**: A threatened or actual attack may need to be reported to the university's regulators, including the Office for Students as a 'reportable event' and/or to the Information Commissioner's Office. The National Cyber Security Centre will not liaise with the university's regulators.
- **National security implications**: The introduction of the National Security and Investment Act 2021 highlighted the need for universities to gain a better understanding on whether their research activities fall within the sensitive areas of the economy that are of interest to national security. Where a cyber-attack could lead to a third party gaining access to, or control over, any assets or IP rights in those areas, the authorities will take a particular interest in the resolution of the threat. The National Cyber Security Centre should be notified in the first instance. It will then involve other relevant law enforcement agencies as required.

Our top 10 tips for universities

1. Familiarise yourself with the National Cyber Security Centre

It makes available on its website a large amount of free advice and guidance which universities can use as part of their training and preparation activities. The centre also offers a free early threat-notification service that can help alert a university to potentially suspicious activity on their networks. Moreover, it can support victims of attacks with identifying specialist cyber security advisers if necessary.

2. Engage with the compliance lifecycle

The governing body of the university should assume responsibility for engaging with the compliance lifecycle, and in particular the preparation phase. The organisation needs to understand the strength and limitations of its IT systems, the variety of threats to which it may be exposed and their potential impact on its operations.

This knowledge must not be confined to IT professionals but considered at a strategic level. Under the supervision of the governing body, an executive team comprising at representatives of all the major central services of the university (including the IT, HR, finance, compliance and risk, internal and external communications, student, regulatory and legal teams) should be assembled to be available at very short notice in order to deal with any actual or threatened attack. This incident management team needs to be contactable at all times.

3. Adopt protocols that will automatically kick in when the university comes under attack

This should involve pre-agreed lines of communication with student, staff and third parties. In case of data breaches or disruption to the university's operations, communications with staff and students are key in order to manage the incident, and reassure individuals as much as possible without granting undue publicity to the threat actors.

4. Speak to your insurers upfront

Insurance providers may need to be contacted in the event of an attack and they will have their own protocols in place. The better you understand their approach, the better they can support your response team in case of crisis.

5. Speak to your lawyers upfront

Familiarise yourself with the crisis support services that your legal advisors can provide to you at short notice, such as helping with contract amendments, liaising with regulators, assisting with communications to staff and students and boosting the capacity of the legal team at short notice. Make sure you know who to contact when the institution is under attack.

6. Update your policies

Ensure your internal policies, regulations, handbooks and protocols align with your crisis management preparation measures, and that they are brought to the attention of your staff and students.

7. Review your contracts

Just like Covid-19 triggered a review and (where possible) re-drafting of force majeure and liability clauses, we would advise universities to consider whether any ongoing or template contractual clauses may need revisiting to limit the university's potential liability in case of a breach of contract due to a cyber-attack.

Universities should also check what constitutes a material event of default in any loan agreements with banks as cross-default provisions could potentially trigger repayment obligations under various banking arrangements. If in doubt, seek legal advice early or try to clarify the situation with your bankers.

8. Mitigating practical impact of potential attacks

While it may be difficult to 'retrofit' back-ups on all existing systems of the university, the IT infrastructure of any new projects should be designed with back-ups when possible.

For instance, any scientific projects that rely on sample and data collection should be conceived whenever possible in a way allowing for data bases to be reconstructed if the university was to lose access to the primary data base (for instance by storing parts of specimen or samples with a third party whose security systems are not directly connected to those of the university). Cost implications may need to be brought to the attention of grant funders.

9. Train your people

Most attacks could be avoided if all individuals within an organisation complied with all IT best practice and training at all times. Remind your staff and students regularly of the importance of compliance and make training mandatory. Ensure that staff and students are aware of your efforts on an institutional level, know who to contact in case of threat and how to behave in case of an attack.

For instance, if staff or students were to get locked out of personal or research data bases and became unable to conduct their research or complete their course work, there is a risk that frustrated members of staff or the student body may publicise their frustrations.

You would want staff and students to understand that publicity is the oxygen to the fire of ransom demands and play to the advantage of threat actors. These messages are better conveyed during the preparation phase then in the heat of an attack.

10. Update your risk register

In the light of the above, it's imperative to update risk management documents.

Key contacts

Nathalie Jacoby-Danesh

Partner

nathalie.jacoby-danesh@brownejacobson.com

+44 (0)330 045 2833

Heather McKay

Senior Associate

heather.mckay@brownejacobson.com

+44 (0)330 045 2232

Related expertise

Criminal compliance and regulatory

Data protection and higher education

Data protection and privacy

Employment

Financial services and insurance advisory

Intellectual property

Regulatory