The cyber threat to Universities

Assessing the cyber security threat to UK Universities

Introduction

This paper aims to provide a short assessment of the current cyber security threat to UK universities and academia.

This information will be of interest to all academic and non-academic staff. It will be particularly relevant to senior leaders in universities and research institutions, members of university councils and those engaged in research.

In the paper, we consider who is targeting the sector and why their attacks may be successful. We also provide a forward look on the threat.

The threat posed to the university sector sits within the broader context of the threat to the UK as a whole. Over the past two years, the UK government has attributed state-sponsored malicious cyber activity against the UK to Russia, China, North Korea and Iran. There is also a serious and sustained threat to the UK from organised cyber crime.

Key judgements

1. **The key cyber threats to UK universities** are highly likely to be:

- Criminals seeking financial gain
- Nation states looking to steal personal data and intellectual property, for strategic advantage

2. **Cyber crime** will probably present the most evident and disruptive difficulties for universities. However, **State-sponsored espionage** is likely cause greater

long-term damage.

3. **Likely effects of state espionage** include:

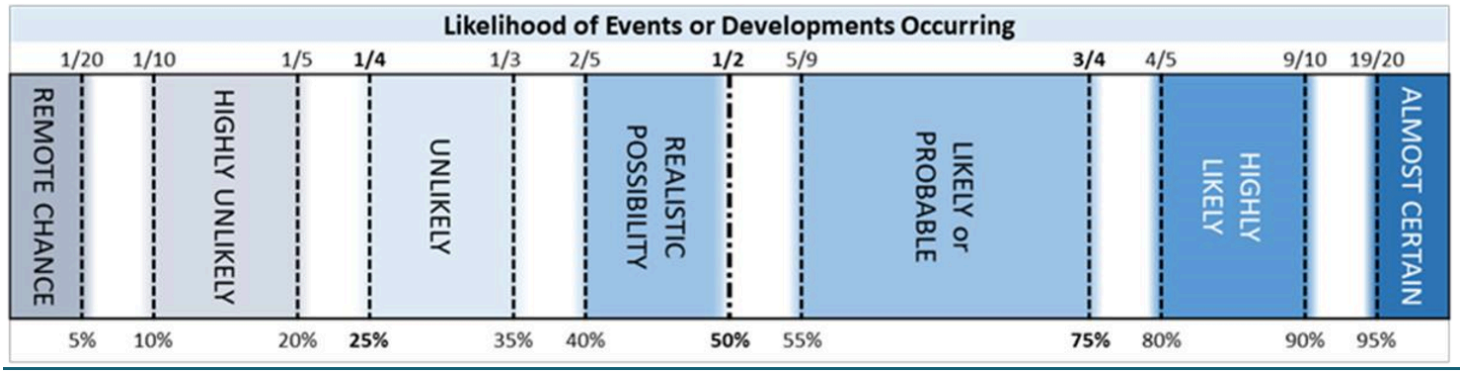
- Damage to the value of research, notably in STEM subjects
- A fall in investment by public or private sector in affected universities
- Damage to the UK's knowledge advantage

4. **If foreign direct investment were to come under greater scrutiny or restriction**, it is a realistic possibility that the cyber threat to universities would increase, as nation states sought alternative ways to gain access to sensitive research and intellectual property.

How likely is a 'realistic possibility' ?

This Assessment uses the PHIA probability yardstick, pictured below.

Every time we make an assessment, judgement or prediction, the terms used correspond to these likelihood ranges.



Why are universities targeted, and by whom?

Universities are key contributors to the economy, skills development and innovation in the UK. In doing this, they handle personal and research data,

intellectual property and other assets, each of which has significant value to others.

It is almost certain that state-sponsored actors are looking to steal data and information for strategic gain. Meanwhile, cyber criminals seek to commit fraud, or monetise stolen material through sale or ransom.

Once access is gained, it is highly likely that both types of attacker will exploit facilities such as compromised email accounts, to further penetrate university systems.

State-sponsored actors

While it is highly likely that cyber crime will present the most evident difficulties for universities, state-sponsored espionage will likely cause greater long-term damage. This is particularly true for those universities which prize innovation and research partnerships. This damage will extend to the UK's larger national interest and to those researchers whose work may give others the chance to 'publish first'.

Nation states almost certainly target universities for the data and information they hold. Cyber offers a deniable route to obtain information that is otherwise unavailable to them. It is likely exploited instead of, or in conjunction with, traditional routes to gain access to research, such as partnering, 'seconded students', or direct investment.

Awareness of the risks associated with international collaboration and overseas funding are variable between universities, as is the level of scrutiny applied to investment opportunities.

Types of data targeted

The kinds of data and information of interest to a nation state may be:

- emails
- bulk personal information on staff and students
- technical resources (e.g. documentation and standards)
- sensitive research and intellectual property

The use of this data is varied, but will meet a wide range of state requirements. Examples include commercial advantage for the nation's companies, advancing equivalent research efforts, military or security apparatus.

Sensitive research may be targeted for its defence or commercial value, and its loss is likely the most detrimental of all to both the affected university and to the UK as a whole. Likely effects include damage to the value of impacted research and intellectual property for both individual researchers and the institution. The attractiveness, relevance and value of an impacted university as an investment partner will also be negatively affected. And at a wider scale, the knowledge advantage of the UK will suffer.

Although espionage can cause long-term damage, it's highly likely that UK universities are targeted to advantage the nation states themselves, rather than to harm the UK.

Stealing from libraries

In August 2018, researchers discovered over 300 fake websites and login pages for 76 universities across 14 countries, including the UK. Victims were likely directed to the fake websites by email. After entering their credentials into the fake login page, their credentials were stolen, and the victims redirected to the legitimate university website. This was likely to limit suspicion over what had taken place.

Many of the fake pages were linked to university library systems, indicating the actors' appetite for this type of material. The researchers attributed this activity to Iranian actors who had previously targeted universities in order to steal intellectual property, including from library systems.

This attack followed a previous Iranian campaign between 2013 and 2017, which saw the Mabna Institute target the accounts of more than 100,000 professors worldwide, and led to the loss of more than 30 terabytes of academic data and intellectual property.

Cyber crime

Cyber criminals are likely to impact universities most often through untargeted attacks.

An example of this is widely-distributed ransomware, which locks systems and data until a ransom has been paid. Such attacks brought significant loss-of-service to multiple UK universities in June 2018.

While rarer, targeted attacks by cyber criminals have the potential for greater financial impact. The use of spoofed or compromised email accounts to impersonate a university's partners or suppliers is rising, and has led to the passing of sensitive information or funds to criminals.

> **Business email compromise**
> In June 2017, an American university paid $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.
>
> The FBI estimates that similar schemes have resulted in global losses of £9bn, between 2013 and 2018.
>
> UK Finance estimate that UK losses for the first half of 2018 were £145m.

Why are attacks against universities successful?

In both culture and technology, universities are one of the most open and outward facing sectors. This enables and eases collaboration between academics across borders, and is likely a key component of their success. Unfortunately, this also eases the task of an attacker.

Phishing
Using sources such as a university's website, it is straightforward to identify who to target, how to reach them, and to establish a credible story with which to

approach them. This information is often key in enabling phishing attacks, where a well-tailored message is used to trick a member of staff or student is into doing something which aids an attacker. This is one of the most common of attacks to affect universities, with one survey from 2017 finding that seven out of ten universities had been affected.

Phishing attacks may result in payments to a fraudulent recipient, the loss of a victim's login credentials, or nefarious malware spreading throughout the university network.

Malware

Malware, or malicious software, is a powerful tool for both state-sponsored groups and cyber criminals.

Malware may be designed to enable the theft of information, provide the attacker with long-term access to a system, or render machines and data inaccessible, until a payment is made.

> **2018 Cyber Security Posture Survey**
>
> JISC is a not-for-profit organisation which provides digital services, including the Janet Network, to UK education and research bodies. The impact of both phishing attacks and malware can be seen in their 2018 Cyber Security Posture Survey.
>
> They found that phishing attacks and malware were present in the top three concerns of security professionals in both Further and Higher Education. Security accidents by staff and students also present amongst the top three concerns.
>
> The report also highlighted a lack of concern for the threat arising from nation states, with only a single response highlighting state activity as a worry.

Defending against attacks

People first

Phishing attacks exploit human tendencies, so the first line of defence is good security awareness among staff and students. Maintaining this security awareness will be a challenge for universities, due to the rapid turnover of both staff and students.

Access and authentication

This frequently changing population of users also makes it difficult to ensure that network access is provided only while appropriate and necessary. This is a key component of security, as many cyber attackers will seek to use authentic user credentials to navigate a network, once an initial foothold is gained.

Security-conscious policies, strict access controls and partitioning of high-value research all contribute to making it more difficult for an attacker to find and steal sensitive data and information.

Network design

A further challenge for universities is in establishing good security without impacting the ease with which information can be shared, or the diversity of what information can be accessed. Within this context, the design of a university's computer network is key.

Many university networks contain a collection of smaller, private networks, providing close-knit services for faculties, laboratories and other functions. The freedom this offers is balanced by the challenge it presents to protecting the data and information within.

When maintained with minimal central oversight or adherence to security policy, private networks are likely more vulnerable to persistent infection or unauthorised access. However, this same segregation offers an opportunity to separate high-value or sensitive data and information, and apply a higher level of protection, without impacting the openness of the wider network.

The future

While UK universities continue to conduct high-end research and generate high value intellectual property, they will almost certainly remain a target for state-sponsored espionage.

State-sponsored activity will continue whilst it remains successful and the repercussions are limited. This is demonstrated by the string of incidents that have been widely attributed to Iran.

We believe that state espionage will continue to pose the most significant threat to the long-term health of both universities and the UK itself. There's a realistic possibility that the threat will increase in-line with increased scrutiny of foreign direct investment and the minimising of other avenues to gain insight and advantage.

Cyber crime too will almost certainly continue to impact universities, either as a direct target or as collateral, regardless of the reputation and success of those universities targeted.

While the methods employed by cyber criminals are constantly evolving, we assess that spear-phishing and social engineering are highly likely to remain the main attack vectors. Ransomware is likely to be the greatest single cause of disruption to staff, students and the universities themselves.

Many of these acts are likely to incur additional damage to any university affected, whether reputationally or through fines levied under data protection legislation.

PUBLISHED

18 September 2019

WRITTEN FOR

Small & medium sized organisations

Large organisations

Public sector

Cyber security professionals