Cyber risks in the education sector

It's no coincidence that the education sector has quickly become a highly sought after target for cybercriminals. From student, employee and partners personal records, to sensitive financial information and valuable, confidential research data, schools and universities handle a treasure trove of data that can be illegally obtained by attackers.

The education sector is often also seen as an 'easy target' by cybercriminals, with a general lack of sufficient funding to ensure adequate security measures and regular cybersecurity awareness training. Most educational institutions have strictly limited budgets for IT staff and infrastructure, with a large proportion of their IT budgets typically focused on equipment for basic networking. As a result, educational IT departments cannot effectively address their existing cybersecurity concerns, leaving schools and universities extremely vulnerable to a wide range of online threats.

Business exposure and implications

The threat of Distributed-Denial-of-Service (DDoS) attacks

DDoS attacks – an attempt to crash a web server or online system by overwhelming it with traffic from multiple resources - are one of the most common threats to the IT infrastructures of educational institutions, and is growing in its frequency globally. With the onset of the pandemic, which has significantly accelerated network traffic due to virtual classroom requirements and VPN usage, DDoS attacks can now have an even greater effect on day-to-day operations of both the education and academic sector.

Access to schools' confidential information

In light of the recent global events forcing the digital transformation within the education sector, both teachers and students are now more reliant than ever on emails to send and receive important information. Combined with insufficient cyber security awareness and limited IT budgets – this makes the educational sector a particularly attractive niche for cybercriminals to take advantage of the situation to launch spear-phishing campaigns with the purpose to access schools' most sensitive and valuable data.

The legal implications and reputational damage

With educational organisations processing and storing a large amount of both personal and financial information, failure to adequately protect that data in case of a data breach can potentially cause devastating repercussions. Apart from directly associated GDPR fines and penalties, it can also result in significant damage to their hard-earned reputation that affects both the prestige of an institution and its valuable relationships.involved in the protection of vulnerable individuals or holding sensitive medical data could be particularly susceptible to this form of cybercrime.

Valuable research data and intellectual property

Vital in contributing to the economy, healthcare and innovation, universities handle a large quantity of sensitive research data, precious intellectual property and other assets, all of which have significant value. This, subsequently, makes universities prime targets for cybercriminals who are looking to commit fraud and monetise the stolen material through ransom demands, sale on the dark web, or to interested parties.

Key industry statistics

76%

of UK secondary schools surveyed experienced a cyber security breach or attack in the last 12 months[1]

69%

of surveyed UK primary schools admitted not being insured against their existing cyber risks[2]

£2.3m

the direct resulting loss for a US school district as a result of a phishing email scam[3]

300+

universities worldwide became victims of an organised cyber attack resulting in 31 terabytes of compromised data back in 2018[5]

What types of risks exist?

There is a variety of different threats that the education industry could be impacted by, but the most common include:

Phishing

Malicious emails designed to look like genuine emails which encourage employees to click – infecting their computers or stealing passwords in the process.

Viruses

Code which infects computer systems, corrupting or deleting data.

Hacking

An individual or group attempting to gain access to company systems with the intent to steal or destroy data.

Ransomware

A malicious programme which locks access to company files and data until a ransom payment is made, after which time access may be restored.

Case Study

Type

A university suffers a data breach through an initial cyber attack on its third-party services provider.

Scenario

Following the ransomware attack that targeted one of the university's third-party software providers and affected its systems and data, cybercriminals gained access to a large amount of the university's personal and sensitive information.

Sting

In the middle of summer, the university was notified that one of their software suppliers had been subject to a ransomware attack which was discovered earlier that year. As a result of the cyber incident, believed to have been carried out for a period of 3 months, a sub-set of data belonging to several different organisations - including the victim university - was stolen by the hackers.

Investigation

The victim institution was among a high number of other educational organisations around the world that have been affected by the attack on their software supplier. An investigation revealed that although cybercriminals couldn't access any financial information or password data, the information taken related to the Personally Identifiable Information (PII) for numerous university's alumni, employees and donors, and details of donations made.

Conclusion

When a third-party service provider is targeted with cyber attacks, the ripple effects may extend to other organisations lined up in the supply chain. A significant breach like this is also expected to have repercussions in the form of phishing attacks, identity theft, or other scams.

Regardless of its software providers, the educational institution remains the main body responsible for the data it handles and stores, therefore, it must ensure its third-party suppliers comply with the GDPR requirements to avoid potential legal action in the event of a data breach.

KYND

KYND's analysis of key cyber risks of the top* 200 UK independent schools

*by grades

Ransomware Risk

34% of schools had at least one external internet service exposed which would place them at a higher risk of a ransomware attack.

Email Spoofing

98.5% of schools were vulnerable to having their email addresses spoofed.

Vulnerable Services

59.6% of schools were running at least one service, such as an email server or web server, with a well-known vulnerability to cyber attack.

Out of Date Software

13.6% of schools had at least one service that was using software which was out of date, no longer supported and vulnerable to cyber attack.

Certificate Issues

32.3% of schools had at least one security certificate which had expired, been revoked or distrusted.

How KYND can help

- With just a website name, KYND reveals your organisation's cyber risks
- Instantly KYND lets you know if your emails are spoofable or if you're vulnerable to a ransomware attack
- KYND provides clear and easy recommendations without using technical jargon
- KYND continuously monitors and alerts you instantly if any new cyber risks are found

Get in touch

✉ broker@kynd.io

🌐 www.kynd.io

References:

[1] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/875574/Education_annex_-_Cyber_Security_Breaches_Survey_2020.pdf, 2020, Cyber Security Breaches Survey 2020

[2] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/875574/Education_annex_-_Cyber_Security_Breaches_Survey_2020.pdf, 2020, Cyber Security Breaches Survey 2020

[3] https://www.forbes.com/sites/leemathews/2020/01/13/phishing-scam-costs-texas-school-district-23-million/?sh=14db7dba41b3, 2020, Forbes

[4] https://axaxl.com/fast-fast-forward/articles/cyber-attacks-on-campus, 2019, Axa XL