SOPHOS
Cybersecurity delivered.

academia
the technology group

Cybersecurity for UK Further and Higher Education

A Sophos Whitepaper. June 2022

The changing face of cybersecurity in education

The value and the cost of post-secondary school education has never been more widely appreciated. The past 20 years have seen some major developments in the way education is financed in the UK. Maintenance grants were completely phased out in 2016 and today a bachelor degree student could be asked to pay up to £9,250[1] per year in tuition fees alone. This 'privatisation' process started with the creation of the Student Loan Company in 1989, and the introduction of tuition fees in 1998. Colleges and universities have become much more financially savvy during this period. Students have also become more aware of the investment they're making in their own future and demand more from their education providers.

Despite the rising cost of education, enrolment in further and higher education has never been higher. There was a 19% increase in enrolment from 2006 to 2010 though this did fall to 12% from 2010 to 2016, according to the National Center for Education Statistics[2]. In the fiscal year ending 31 July 2019, the University of Cambridge (the wealthiest in Europe), excluding colleges, had a total income of £2.2 billion[3]. The University of Bedfordshire, ranked as one of the least popular in the UK by the Complete University Guide[4], had a total income of £162.2 million in 2021 (and a surplus at year-end of £18 million) some 15.1% higher than in 2020[5].

All of these students and all of this money make higher and further education an attractive target for cyber-attackers.

1 *https://www.topuniversities.com/student-info/student-finance/how-much-does-it-cost-study-uk#:~:text=Now%2C%20UK%20and%20EU%20students,Survey%20of%20University%20Tuition%20Fees).*

2 *https://loyolaphoenix.com/2020/02/the-value-of-higher-education-has-changed-in-the-past-20-years/*

3 *https://en.wikipedia.org/wiki/University_of_Cambridge#:~:text=By%20endowment%20size%2C%20Cambridge%20is,from%20research%20grants%20and%20contracts.*

4 *https://www.bedfordshirelive.co.uk/news/bedfordshire-news/university-bedfordshire-ranked-worst-uk-5938865*

5 *https://www.beds.ac.uk/media/wuspromq/financial_statements_2021.pdf*

The changing face of technology in education

Education providers at all levels have a reputation for being digital laggards. Though further and higher education institutions are well ahead of the curve in comparison to their primary and secondary counterparts. The first "node-to-node" communication from one computer to another took place in 1969 between a machine located in a research lab at UCLA and at Stanford University in the US, and thus was born the internet. Fast forward to today and a record number of students (129,610) applied to study Computer Science in the UK in 2021[6]. Indeed, according to UCAS, Computer Science was the fourth most popular undergraduate degree course in 2020[7].

Technology underpins everything in education from both a teaching and operational perspective. This was highlighted during the COVID pandemic. When England entered lockdown in March 2020, education all but ground to a halt. Yet thanks to technology adoption and the herculean efforts of education professionals, many further and higher education facilities were offering online lectures in time for the summer term. If the pandemic had happened just 10 years ago, this ramping up of remote learning would have been implausible.

Moving forward, digital transformation is a top priority in education. Tertiary education may be further along the road than secondary, but it still has a long way to go. Many institutions are operating across multiple sites, with tens of thousands of students and staff working from anywhere on a wide variety of devices. They are doing so against a backdrop of fragmented legacy systems which can result in potential points of vulnerability for cyber-attacks.

6 *https://www.itproportal.com/news/computer-science-degrees-are-more-popular-than-ever/*

7 *https://www.thecompleteuniversityguide.co.uk/student-advice/what-to-study/top-ten-most-popular-courses-in-uk*

Compounding the problem, education providers typically have an IT skills shortage. Colleges and universities can't afford large teams of people to work in IT and they certainly don't have time for proactive threat hunting. Teaching staff often have responsibility for how technology is used. Oftentimes lecturers might not be particularly tech savvy, but they find themselves responsible for liaising with hundreds of students online. Even in our post-lockdown world, lecturers are increasingly delivering content using technology in person, in addition to setting and marking coursework remotely.

The use of technology is now, more than ever, critical for the delivery of education. But as educators race to roll out the latest hardware and software they are faced with an uphill cybersecurity battle. Faster technology adoption, tighter budgets, fewer skilled IT people all point to major challenges ahead. Educators would be mistaken to assume it will be business as usual when it comes to cybersecurity.

The changing face of cybersecurity

More technology and greater fragmentation mean more points of weakness, and therefore more potential for successful cyberattacks. Education is seen as an easy target and 2020 was a tough year, with the sector experiencing the highest level of ransomware attacks of all industries (tied with retail) according to the Sophos State of Ransomware in Education 2021 report[8]. At the same time, the rapid shift from lecture theatre to online learning in many countries piled additional work and pressures on IT teams: nearly three quarters (74%) of respondents said cybersecurity workloads increased over 2020, the second highest rate of all sectors. Meanwhile, attacks have continued on into 2022. For example, in March 2022, Edinburgh's Heriot-Watt University[9] suffered a massive attack that ground some of its systems to a standstill. The attack followed similar breaches in 2021 at the University of Hertfordshire[10] and Newcastle University in 2020[11].

8 *https://assets.sophos.com/X24WTUEQ/at/g523b3nmgcfk5r5hc5sns6q/sophos-state-of-ransomware-in-education-2021-wp.pdf*

9 *https://www.theregister.com/2022/03/24/heriot_watt_outage/*

10 *https://www.itpro.co.uk/security/cyber-attacks/359222/university-of-hertfordshire-hit-by-cyber-attack*

11 *https://www.itgovernance.co.uk/blog/newcastle-university-becomes-latest-ransomware-victim-as-education-sector-fails-to-heed-warnings*

In the face of these challenges, many education organisations that were hit by ransomware paid the ransom to get their data back. In fact, the education sector has the third-highest rate of ransom payment (35%), behind energy, oil/gas and utilities (43%), and local governments (42%). However, those who paid, on average, only got back 68% of their data, leaving almost a third inaccessible. Just 11% got all their encrypted data back. In other words, paying the ransom doesn't really pay off[12].

In recent years, ransomware groups have become more professional, with well organised company-style structures and ransomware as a service (RAAS) affiliate schemes. It is not the case that threat actors only encrypt data and demand payments for decryption keys, but they increasingly exfiltrate valuable data and threaten to publish or sell it on the dark web.

Cybersecurity is a multi-layered threat

The threat posed by ransomware attacks is particularly damaging for educators who handle student data and are financially responsible for the clean-up. The overall financial impact of ransomware is crippling for education organisations. The average bill for recovering from a ransomware attack is $2.73 million, the highest by far of all sectors and 48% above the global average[13]. This is likely due to many education organisations running outdated and fragmented IT infrastructures supported by understaffed IT teams. As a result, in the wake of an attack they are often forced to totally rebuild from the ground up, incurring major financial cost.

Risky online student behaviour, such as downloading unpermitted software or visiting certain websites also increases exposure to attack. The pandemic has further exacerbated the challenge. Many education establishments switched, with short notice, from brick-and-mortar classrooms to virtual/remote learning environments, leaving IT teams little time to plan security strategies or invest in new IT infrastructure. The rapid switch also limited opportunities for cybersecurity training for staff and students, while overloaded IT staff had limited availability to provide technical/security support.

12 *https://assets.sophos.com/X24WTUEQ/at/g523b3nmgcfk5r5hc5sns6q/sophos-state-of-ransomware-in-education-2021-wp.pdf*

13 *https://assets.sophos.com/X24WTUEQ/at/g523b3nmgcfk5r5hc5sns6q/sophos-state-of-ransomware-in-education-2021-wp.pdf*

In today's world, it is no longer enough to simply deploy antivirus software across networks and expect to be protected. Malware and hacking used to be two different threat landscapes; however, they have merged over the last five years. Attackers are stealthy – if IT teams don't play an active part in looking for signs of a breach, then cybercriminals can use (often legitimate) tools to enter and move around a network undetected, simply waiting for the right opportunity to strike. 'Hands-on attacks', where the adversary goes interactive within an IT estate, are becoming increasingly common and can unfold at lightning speed, quickly, overwhelming staff. If this happens, it's crucial that an organisation has the expertise to respond rapidly at any time of day or night, or bring in incident response services to assist.

Barriers to transformative security

As colleges and universities accelerate with their digital transformation plans, it will result in more data being shared across sites and greater commonality of systems. This will result in more points of weakness and more cybersecurity risk.

Management teams are faced with three key immediate, challenges in terms of digital transformation. First is the complexity of the existing or legacy platforms and software across a fragmented landscape. Second is the requirement to address security and compliance - the immediacy of this requirement can lead to quick fix solutions, which does not help with long term challenges. The third challenge is a lack of skills with new technologies such as cloud, AI and cybersecurity.

Educators are increasingly looking towards managed service providers to help with these challenges. As the strategic importance of technology increases in line with its complexity, the role of the IT professional in education is moving up the value chain from implementation expert responsible for building, deploying and maintaining solutions to technology orchestrator responsible for long term goals and strategy.

Taking a long-term approach

Security, like insurance, is something you hope you never need, but absolutely must have in place from a compliance perspective and to manage risks. In fact, colleges and universities would be well placed to work on the assumption that an attack will happen and ensure they have a tried and tested incident response plan that can be implemented immediately, to reduce the impact of the attack. Complicating matters, threats are constantly evolving as criminals try new avenues of attack against the latest security. For instance, phishing is become ever more sophisticated and difficult to spot, especially in environments with high footfall, such as student intakes, using fragmented IT architecture.

Too many cyber breaches are caused by the inadvertent actions of users. Therefore, it is important that users are educated about the cyber risks they face and the safeguards in place to protect them. They should also understand their individual cyber security responsibilities, be aware of the consequences of negligent or malicious actions, and work with stakeholders to identify ways to work in a safe and secure manner.

As individual staff members' machines are often the gateways for cybercriminals, all employees should complete data security awareness training, and participate in regular phishing simulations to raise awareness. At the very least you should check out the advice targeted at educators on the National Cyber Security Centre website[14].

Avoiding breaches – the cybersecurity solutions

Taking a proactive approach to cybersecurity is vital. Educators are faced with the choice to either manage IT themselves or outsource. Most do not have the right expertise, tools, people, and processes in-house to effectively manage their security programme around-the-clock while proactively defending against new and emerging threats. Furthermore, colleges and universities who do invest in cyber security solutions often fail to deploy them fully or use them to their full potential – significantly reducing their effectiveness and increasing the likelihood of a successful, but preventable breach.

For an organisation to mount an effective defence against cybercriminals, IT teams often use Endpoint Detection and Response (EDR) or Extended Detection and Response (XDR) tools. These monitor and scour the network for suspicious behaviour and Sophos XDR is one such solution. However, it takes expertise and time to use these tools effectively, burdening already overstretched IT staff.

14 https://www.ncsc.gov.uk/section/education-skills/higher-education

In these circumstances, buying in a Managed Detection and Response (MDR) service is an ideal solution. At Sophos, a human-led threat hunting team works together with AI technology to hunt, detect and respond to suspicious activity 24/7/365, maintaining an ongoing dialogue with IT staff. More than just a notification service, the team's level of involvement is entirely within an organisation's control – from validating threats and removing all the 'noise' of false positives, to carrying out targeted actions on an IT team's behalf. Because these threat hunters are so familiar with malicious behaviour, once detected, the issue is often resolved within the hour.

How Inspire Education Group worked with Sophos

In 2021 Inspire Education Group extended its IT security to include Sophos MDR[15]. When the time came to move both of its colleges to MDR a complication arose. At the Peterborough site, when the team removed the incumbent solution, ransomware attackers managed to compromise the college before MDR was installed. The attackers failed to access Stamford systems because MDR already in place there, as well as the other Sophos solutions the college had installed. Nothing was lost or damaged at Stamford yet in Peterborough, 80 servers were compromised. Thankfully, recent backups meant that the college did not lose everything[16].

15 https://assets.sophos.com/X24WTUEQ/at/8m2h964r7ghj779v6wknfx8/sophos-inspire-education-cs.pdf

16 https://assets.sophos.com/X24WTUEQ/at/8m2h964r7ghj779v6wknfx8/sophos-inspire-education-cs.pdf

Conclusion

With a continually changing threat landscape, securing further and higher education facilities requires a collaborative team effort. By working together, we will have the best opportunity to minimise security incidents and keep data safe as digitalisation continues apace.

Having a specialist MDR team in your corner at all times – whether it is in the middle of the night, at a weekend or on a bank holiday – ultimately provides you with peace of mind, knowing that you're doing all you can to keep your core services running and your teaching staff and students safe.

To learn more about the Sophos MDR service visit our website or read our case studies and research.

Sophos delivers industry leading cybersecurity solutions to businesses of all sizes, protecting them in real time from advanced threats such as malware, ransomware, and phishing. With proven next-gen capabilities your business data is secured effectively by products that are powered by artificial intelligence and machine learning.

2022-09-07 (WP-PC)

SOPHOS