Cyber Threats and Opportunities in the Education Sector - A Boardroom Agenda

EDUCATION

By **Anu Khurmi**, Managing Director, Global Services, Templar Executives

"From the Board to the frontline, it has never been more critical for educational institutions, responsible for a treasure trove of valuable data, to safeguard against the growing threats from indiscriminate and targeted Cyber attacks and data breaches."

Ensuring students are at the heart of the learning experience is an ongoing exercise for educational institutions, government bodies and teaching staff in an age of innovation and change. The opportunities opening up to the education sector are exciting and ambitious; the ideals of the 4th educational revolution advocate for a more personalised, mixed reality learning approach. The growing adoption of technology solutions, digital tools innovations based on Artificial Intelligence (AI) and Virtual Reality (VR), are integral to this evolution, enabling a blended learning approach from the physical classroom presence to increasingly virtual means, such as remote learning.

Whilst this has immense and far reaching benefits, it also has its fair share of challenges and none more so than the huge disruption and controversy caused by the COVID-19 lockdown and the impacts on school children, students, staff and learning faculties. What this means for the future of education and our society is another intense and ongoing debate.

As teachers and students head back to the classroom, a fundamental part of the safety and security agenda relies on implementing hybrid working environments encompassing home and remote working. Not surprisingly, this has triggered an acceleration in the adoption of digital technologies such as social media apps, cloud solutions, virtual reality tools and personal devices. It has also brought into sharp focus growing concerns about exploitation of the sector through its increasing vulnerability to Cyber attacks and data breaches.

Although colleges can fall victim to widespread attacks affecting the community at large or suffer an attack by a Cyber-capable student, there are also a multitude of reasons why Cyber criminals view education as an attractive sector. It is seen as an easy target teeming with a veritable treasure trove of valuable data. The multitude of users make it possible to easily harvest user credentials for future scams and phishing attacks. Unfortunately, board engagement has traditionally referred Cyber security to the IT function.

As teachers and students head back to the classroom, a fundamental part of the safety and security agenda relies on implementing hybrid working environments encompassing home and remote working. Not surprisingly, this has triggered an acceleration in the adoption of digital technologies such as social media apps, cloud solutions, virtual reality tools and personal devices. It has also brought into sharp focus growing concerns about exploitation of the sector through its increasing vulnerability to Cyber attacks and data breaches.

Although colleges can fall victim to widespread attacks affecting the community at large or suffer an attack by a Cyber-capable student, there are also a multitude of reasons why Cyber criminals view education as an attractive sector.

Unfortunately, board engagement has traditionally referred Cyber security to the IT function. As a result, the investment in Cyber Security is not properly put in context or prioritised as a business risk at the leadership level, whether it is risk that affects personal data, assessment data or digital services supporting learning and administration. Today more than ever, the benefits of technological innovation must be accompanied by greater Board awareness of the evolving trends and increasingly sophisticated threats; this in turn will enable enlightened leaders to prioritise and deploy proportionate proactive measures within their organisation to manage risk, compliance and enhance business resilience.

EDUCATION

In recent years legislation and new data protection laws, such as the General Data Protection Regulation (GDPR), have mandated much greater responsibility for protecting the confidentiality integrity and availability of data by organisations collecting, using and storing personal information; there are now substantial financial penalties for non-compliance.

Higher education institutions, in particular, face unique threats to their data security with state sponsored and criminal Cyber actors specifically targeting universities for the sensitive research and intellectual property stored in their systems. A recent example in July, saw a state-sponsored Cyber attack by Russia's APT29 hacking group steal COVID-19 vaccine research undertaken by UK, US and Canadian pharmaceutical companies and academic institutions.

Cloud computing technology has helped school and university learning to flourish in virtual classrooms and lecture theatres, whilst also presenting cost effective opportunities to bridge the digital divide.

It is important however, that organisations review their chosen cloud and managed service providers (MSPs), ensuring that all stages of the information lifecycle have appropriate protection, and that they have oversight and manage where their organisation's intellectual property and sensitive information resides. In May this year, US cloud computing provider Blackbaud suffered from a ransomware attack during which personal data was stolen from over 40 UK universities, 11 UK-based not-for-profit organisations and 50 international organisations.

Technological innovations by third parties are also fuelling exciting developments in the provision of creative new educational offerings; even before the current crisis, the Digital Economy Council estimated the UK EdTech sector to be worth £3.4bn by next year. Whether it be the drive for home learning, sitting exams remotely online, monitoring student behaviours, running virtual classes, Edtechs are helping shape the future of education in the UK and across the world.

Again, the use of third party suppliers needs to be properly assessed and managed; Boards should be aware that accountability for organisational risks cannot be passed on to a third party; this was recently highlighted in the ProctorU data breach incident when thousands of students' personal details were hacked and leaked onto the internet.
There is no doubt that the education sector continues to be a prime target for Cyber attacks and the victim of breaches. The DCMS Cyber Breaches Survey in 2020 found that 54% of further education institutions identified breaches or attacks at least once a week. A similar proportion (57%) had a material outcome from these breaches, such as a loss of money or data. The most common impacts cited by further and higher education institutions involved a temporary loss of network access, and the loss or destruction of personal data. Ransomware attacks have been brought into particular focus over recent years with Northumbria University one of the latest casualties.

Ominously NCSC continue to warn of the heightened threats targeting the sector and their latest alert warns that ransomware attacks could disrupt the start of term.
It is increasingly apparent that without greater Cyber Security awareness, further and higher education institutions will continue to be vulnerable to exploitation from threat actors and their own staff and students inadvertently contributing to incidents. The requirement for a holistic approach to Cyber Security, placing an importance on people, processes and culture alongside technical solutions needs to be driven by the Board. It is crucial that there is effective leadership in fostering a culture which values investment in staff and protects business critical information. This will enable informed decision making that advocates a proportionate and proactive approach to implementing Cyber Security best practices and capitalising on lessons learned.

"Survey in 2020 found that 54% of further education institutions identified breaches or attacks at least once a week. A similar proportion (57%) had a material outcome from these breaches, such as a loss of money or data"

The DCMS Cyber Breaches Survey 2020

Contact Us

+44 020 3542 9075

https://www.templarexecs.com

@templarexecs

Templar Executives