

Schools Are Getting Slammed By Cyberattacks and Student Data Is No Longer Safe. Here's How to Navigate Cybersecurity in the New, Digital Classroom



Opinions expressed by Entrepreneur contributors are their own.

Education has always been at the forefront of societal progress, shaping the minds of future generations. In recent years, as we further delve into the modern age, the traditional classroom is undergoing a profound transformation. This digital shift in education has completely changed how we teach and learn, from tablets and interactive whiteboards to

online learning environments and virtual reality. This shift, however, is not without difficulties.

The proliferation of mobile devices and cloud workspaces broadens the attack surface, making it easier for bad actors to access your network. Schools, universities and other educational institutions hold vast amounts of sensitive data, like academic records, student and parent addresses, phone numbers etc.

This makes them an enticing target for cyber attackers. Reports show that, from June 2022 to May 2023, there have been 190 known ransomware attacks against educational institutes. This is an 84% increase in attacks in the 6 months.

Apart from the monetary repercussions of such attacks, the danger to a student's privacy, the damage to these institutes, and their impact on society is genuinely troublesome. For instance, last year, Lincoln College, Illinois, a 157-year-old institution that had survived two great wars, the Spanish flu, the great depression, and the Covid pandemic, became a victim of multiple ransomware attacks and was finally forced to shut down.

So, the seriousness of cybersecurity in education cannot be understated. Fortunately, cybersecurity training in schools has been gaining steam recently. In March, the governor of North Dakota signed a bill that makes cybersecurity training a mandatory part of the curriculum for K-12 students. However, safeguarding the privacy and securing endpoints and networks while providing an unhindered learning experience is tricky.

Related: Will Colleges Survive in the Age of AI?

The balancing act between security,

privacy and productivity

In an increasingly interconnected world, where technology is deeply integrated into education, protecting students, institutions and their data is a prime concern.

The backbone of any institution's security lies in its network infrastructure. The network infrastructure of every organization serves as the foundation for its cybersecurity. Strong firewalls, intrusion detection systems, secure network access controls and threat prevention systems are essential components of a secure network. Furthermore, to avoid unauthorized access and data breaches, monitoring the network and fixing any vulnerabilities regularly is essential.

Along with the network, securing the endpoints is also pivotal as more and more schools provide computers, tablets, or mobile devices in the classroom. Instituting policies that require the use of strong, periodically updated passwords and regularly applying security patches and updates to operating systems are essential to keeping these devices secure. Alternatively, utilizing a Unified Endpoint Management (UEM) solution will provide endpoint security features such as enforcing strict password policies remotely pushing app and OS updates or patches etc.

Related: Google Is Getting Sued for Collecting Data From Kids' Educational Chromebooks

Apart from securing endpoints, when the number of devices keeps increasing, managing them and ensuring they are not misused creates another hurdle. Provisioning all school-owned devices with a UEM allows administrators to hone these devices into focused learning tools. Its app management capabilities help push essential applications to the devices directly from the UEM console without any external user intervention.

Moreover, any undesirable apps could be blocked or restricted

from being installed on the devices. The web content filtering capability does the same with websites, preventing students from visiting unwanted or malicious sites. A UEM supporting multiple operating systems also removes the hassle of using a different solution for each OS.

Educational institutions will always have a significant quantity of sensitive and personal data. Therefore, it is imperative to protect this data to retain the privacy and confidence of students, parents, and staff. The scariest part is that losing sensitive data, such as student records, can put students or their families at risk of dangerous attacks such as phishing scams or even identity thefts. One way to prevent this is to employ strong data storage procedures and encrypt data at rest and in transit.

To that extent, deploying a Data Loss Prevention (DLP) solution goes a long way in protecting data privacy. A major element of avoiding breaches of such nature consists of closely monitoring the flow of sensitive data. DLP systems can help these institutes track and protect their data by enforcing preconfigured policies. Additionally, institutions must make it a top priority to comply with data privacy laws like the Family Educational Rights and Privacy Act (FERPA), the General Data Privacy Regulation (GDPR) or other legislations based on your location.

Related: The How-To: Protect Your Business From A Data Breach

Finally, no cybersecurity system is foolproof, which is why educational institutions must have a well-defined incident response and disaster recovery plan in place. The effect of a potential cybersecurity incident can be reduced by regularly backing up important data and testing disaster recovery plans, ensuring that the institution can recover quickly and carry on with business as usual. In the event of such an attack, having a cyber insurance policy offers a solution to diminish the fallout. An insurance policy covers the monetary expense in

the face of ransomware, data breaches and other cybersecurity dilemmas.

Promoting a culture of cybersecurity awareness

A predestined step in constructing a formidable cyber defense is developing a culture of cybersecurity awareness. Strong password usage, recognizing phishing attempts, and preserving personal information are just a few of the safe online habits that may be inculcated through regular training sessions and awareness programs. The changes brought by North Dakota in its curriculum and pedagogy are a palpable example of promoting cybersecurity awareness.

As educational institutions become more dependent on technology, addressing cybersecurity is not an option—it is a necessity. Schools and colleges move towards a more secure zero trust-based architecture by fostering a culture of cybersecurity awareness, installing secure network architecture, preserving data and privacy, enhancing endpoint security and developing proactive incident response procedures. With cyber scams getting more problematic to identify, going forward with a zero-trust mentality can bolster their security architecture and protect their students and data.

<https://www.entrepreneur.com/leadership/schools-arent-safe-from-cyberattacks-heres-how-to/454351>