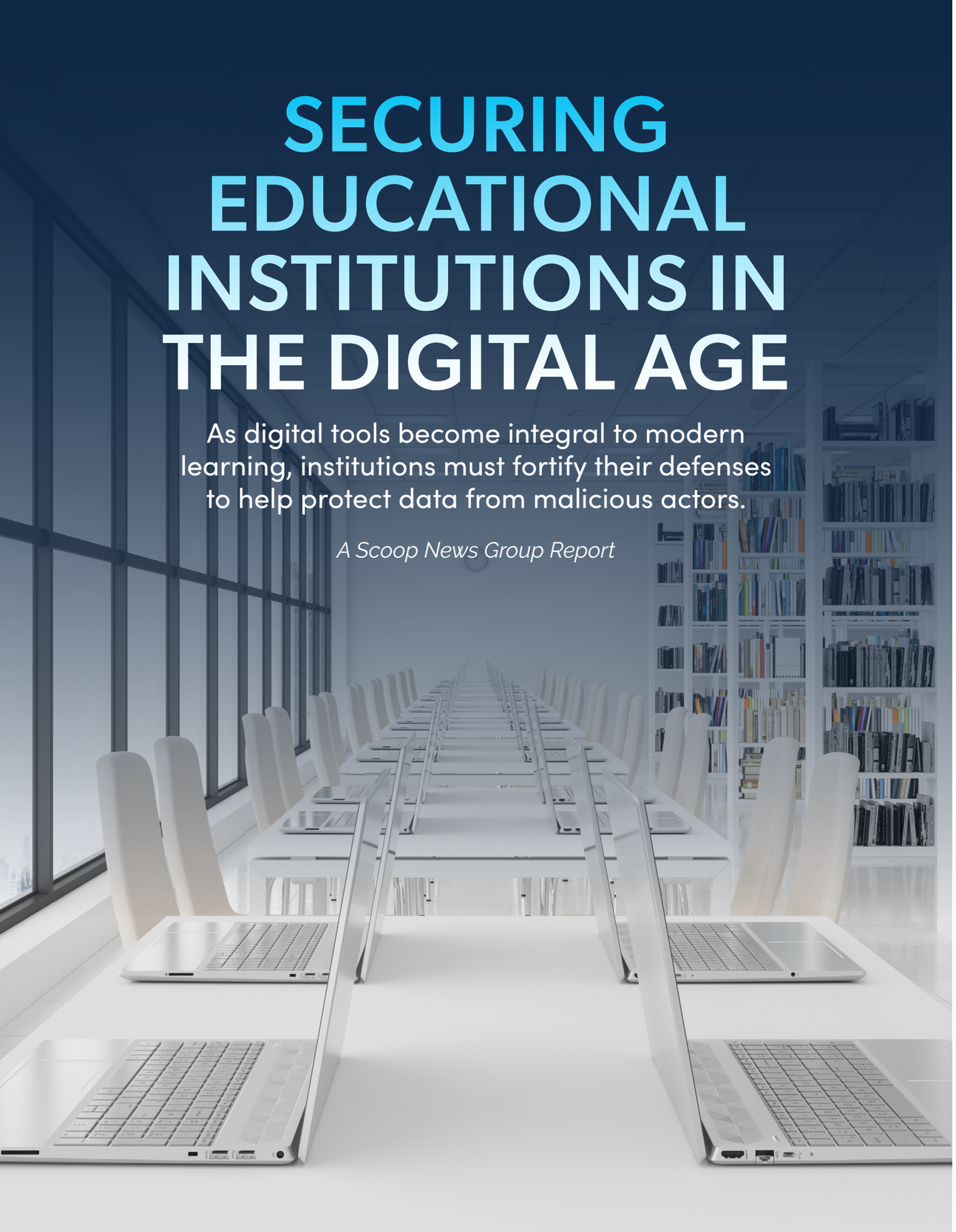
SECURING EDUCATIONAL INSTITUTIONS IN THE DIGITAL AGE

As digital tools become integral to modern learning, institutions must fortify their defenses to help protect data from malicious actors.

A Scoop News Group Report



Imagine one of the largest school systems in the country falling victim to a vicious cyberattack because they refused to pay the ransom demanded — and then trying to recover after the release of 500GB of sensitive information.

Unfortunately, that scenario became a harsh reality for the Los Angeles Unified School District. Threat actors published stolen data, including Social Security numbers, bank account information, W-9 forms and sensitive student health information. More ominously, the wave of ransomware attacks plaguing U.S. schools keeps rising, prompting the White House to announce a series of new initiatives at a first-ever cybersecurity summit in August on school ransomware attacks.

"Last school year, schools in Arizona, California, Washington, Massachusetts, West Virginia, Minnesota, New Hampshire and Michigan were all victims of major cyber-attacks," Anne Neuberger, the U.S. deputy national security advisor for cybersecurity, said at the summit. Nearly one in three U.S. school districts experienced a breach by the end of 2021, according to the Multi-State Information Sharing and Analysis Center.

America's 13,000 school districts play a critical role in serving families and communities across the nation. In the digital age, the need to prioritize cybersecurity has become more apparent than ever. The widespread adoption of digital tools and platforms since the pandemic has opened new opportunities for learning and collaboration. However, this digital shift has also exposed educational institutions to an evolving cyber threat landscape.

As seen with the LAUSD, the education sector is increasingly becoming a prime target for cyberattacks due to the wealth of sensitive data they store. This includes personal information of students and faculty, financial records and valuable research data.

Recognizing this growing threat, the Biden-Harris Administration's initiatives seek to bolster K-12 cybersecurity with the overarching goal of improving the resilience of schools against cyberattacks. This includes providing resources, guidance, and support to help schools better protect students, families, teachers and administrators from malicious cyber activities.

Cybersecurity was ranked as the top priority for the fifth consecutive year among 1,200 education technology leaders surveyed by the Consortium for School Networking. Interestingly, the same report found that despite the critical importance of cybersecurity, a third of respondents do not have sufficient resources to manage their cybersecurity—and more than 60 percent do not have a full-time cybersecurity position within their IT staff.

Educational institutions are no strangers to operating within tight budgets. While increased spending doesn't always guarantee better security, the lack of adequate resources to invest in robust cybersecurity infrastructure and staffing hinders their ability to detect, prevent and respond to threats effectively.

There are strategies for mitigating these threats, according to the 2023 Comcast Business Cybersecurity Threat Report. The report offers valuable insights to address a range of threats, which can encompass various forms, including phishing campaigns, distributed denial-of-service (DDoS) attacks, and sophisticated ransomware attacks.

Vulnerability to attacks and rising cyber threats

"Education is a significant target area for DDoS attacks," the 2023 Comcast Business Cybersecurity Threat report notes, with 46% of attacks targeting the sector. And DDoS attacks have plagued schools even before the COVID-19 pandemic. During the pandemic, students realized the ease and affordability of launching DDoS attacks, utilizing botnets from the dark web to disrupt online learning.

"The complexity of cybersecurity requires continuous monitoring and guarding against intrusions 24/7."

Ivan Shefrin

Executive Director, Managed Security Services Comcast Business

As highlighted in the threat report, adversaries in the cyber world take the path of least resistance. Ivan Shefrin, Executive Director of Managed Security Services at Comcast Business, explains how they capitalize on the vast availability of stolen credentials on the dark web.

> *Notably, services for conducting phishing, ransomware and other attacks are readily purchasable with minimal technical knowledge required. This has given rise to a black-market economy around cyberattacks, with phishing and stolen credentials being the favored tools for infiltrating school systems. To counter this, we emphasize the importance of anti-phishing measures, including security awareness training.*
>
> **- Ivan Shefrin**

Everyone, including cybersecurity experts, can fall victim to phishing attacks due to the fast-paced nature of work, where it's easy to click on a seemingly legitimate link or open a suspicious email attachment. Threat actors can use subtle URL variations and employ techniques that automatically download malware without the user's knowledge.

Cybersecurity is not solely about securing the network perimeter

"The evolving landscape has shifted the focus from solely safeguarding the perimeter of a school's network to helping to protect the internal systems as well," says Shefrin.

Modern educational institutions have diverse network entry points, including cloud applications and mobile devices, which threat actors can exploit. Insider threats from students or staff and advanced persistent threats that can go undetected by perimeter defenses are also concerns. To effectively address these challenges, institutions need cybersecurity solutions that cover all endpoints, systems, and cloud environments.

"Even large organizations can't always afford the substantial investment required for building and maintaining an in-house cybersecurity team. Outsourcing to companies like Comcast Business, which provides Managed Detection and Response services, can be an affordable and effective solution," adds Shefrin.

Integrated cybersecurity solutions

To help protect themselves from cyberattacks, education technology leaders need to take a layered approach to cybersecurity. This is where industry partners and managed services can play a valuable role. Partners can provide schools with access to cutting-edge security solutions and expertise. They can take over the day-to-day management of a school's cybersecurity, freeing IT staff to focus on other priorities.

Leveraging industry partners and managed services for cybersecurity offers numerous advantages for schools. These include access to cutting-edge security solutions like next-gen firewalls and endpoint detection systems, which help protect against evolving threats. Additionally, industry partners bring a wealth of expertise, aiding schools in evaluating security risks and implementing tailored measures while staying informed about emerging threats and technologies. Moreover, managed services providers can alleviate the operational burden by assuming the responsibility for daily cybersecurity management, enabling IT personnel to concentrate on other critical tasks, ultimately streamlining school operations and cost-effectiveness.

Optimal strategies for leaders to prepare both for security and data breaches and where to focus resources on closing the gaps to improve their school's security posture include:

- **Mitigate phishing risks with security awareness training and email gateways scanning for harmful content.**
- **Enhance security via centralized identity management, multi-factor authentication, and rigorous directory audits.**
- **Strengthen security with zero-trust policies, especially for critical assets.**
- **Secure credentials in a hardware vault.**
- **Ensure remote access security with identity-based certificates and multi-factor authentication.**
- **Maintain data integrity with scheduled, encrypted backups.**
- **Proactively manage vulnerabilities through scanning, updates, and monitoring.**
- **Reduce attack surfaces with hardened configurations.**
- **Improve endpoint security with endpoint detection and response solutions.**
- **Segment networks to minimize the impact of incidents.**
- **Deploy unified threat management firewalls and domain name system security.**
- **Continuously monitor security events and consider managed detection and response services.**
- **Prepare for breaches with a documented incident response plan.**

Each organization's IT environment is unique, and Comcast Business is able to integrate these diverse elements and simplify the implementation of cybersecurity. This approach aligns with the concept of defense in depth, which means helping to protect not just the network perimeter but also internal systems.

Education technology leaders stand to benefit by taking steps to consider industry partners and managed services in their cybersecurity strategies. By doing so, they can help protect their schools from cyberattacks and help keep their students and staff safe.

Learn how Comcast Business offers tailored solutions to help safeguard your network and connected devices.

STATESCOOP | EDSCOOP COMCAST BUSINESS

This report was produced by Scoop News Group, for EdScoop and StateScoop and sponsored by Comcast Business.