WHITE PAPER

Embracing Security Operations in the Educational Sector

Executive Summary

Nearly every part of the educational sector has fallen victim to a cyberattack, from elementary schools to universities. Securing education is no longer a "nice to have" but a "must do" and is a growing concern among the global educational community.

Creating and maintaining effective information security and cybersecurity operations in education comes down to people, processes, and tools. It's crucial for IT and security leaders across the entire spectrum of educational institutions to find the right balance between the three. While there are success stories of achieving that balance, there's always more to do to identify, understand, and mitigate cybersecurity risks to these organizations. Establishing and improving existing cybersecurity operations must become a priority.

In 2022, the average cost of a data breach in the educational sector was $3.86M, up from $3.79M in 2021.[1]

Essential Components of Cybersecurity: People, Processes, and Tools

People are arguably the foundation of any cybersecurity program. Try this experiment: First, gather a diverse group of five IT and cybersecurity experts who work in education and see if they agree that there's an ongoing talent shortage of cybersecurity professionals, particularly in the educational sector. Second, ask that same group what skills, education, and certifications are needed to excel in a cybersecurity career. Finally, ask that group to reflect on their respective careers. Looking back, what would they have wanted to learn in the first few years of their security careers?

You'll likely get agreement on the first question, similar answers to the second, and wildly different answers to the third. People are invaluable components of any security program and understanding what security operators want and need is essential. Having ongoing conversations and feedback sessions with IT and security professionals will not only help you retain the talent you have but can also serve as a catalyst for finding efficiencies in your processes or technologies that will make everyone's lives easier.

Processes are like politics: the more localized they are, the more likely it is that they will be followed. Ask those same five experts if the processes in place at their respective schools, college, or university are derived from current policies and laws. Then ask if they feel that the regulations in place help or hurt their cybersecurity operations. Security leaders must be aligned with campus leaders and have a shared understanding of how the local, state and federal laws and regulations impact cybersecurity. With many states enacting new or more stringent data privacy laws, ensuring educational processes are compliant and current requires perpetual due diligence.

Having the right tools in place will make or break your cybersecurity program. Do those five experts believe the tools available to their teams and users are cost-effective? And are those tools valuable in their day-to-day operations?

The resources we have at our disposal today—the people, processes, and technologies—must meet the team's ongoing needs regarding availability, effectiveness, and cost. If they don't meet the team's needs, now is a great time to reexamine what's needed to establish or enhance your security operations.

The Challenges with the Current State of Cybersecurity in Education

Many educational institutions are racing to the head of the class when embracing digital transformation. From implementing eLearning to taking greater advantage of the cloud, organizations are increasingly prioritizing ways to enhance student learning opportunities across distributed campuses. However, while this new level of connectivity benefits students, teachers, and staff, these changes introduce many security implications.

Faculty, researchers, and students can now work or learn from anywhere and can directly access sensitive school data via cloud-delivered applications controlled by third-party vendors. Yet this leaves endpoint security as the only "layer" controlled by the organization. This also means networking tools provided for security at remote locations should be presumed vulnerable.

Additionally, today's ever-evolving array of threats is often specifically designed to bypass those traditional prevention-oriented security technologies teams relied on in the past. Cybercriminals are evading traditional security protocols and tools by breaking attacks into the stages described in the MITRE ATT&CK framework and then making subtle changes within each stage. The best defense includes continual inspection for signs of intrusion and quickly responding when and where indications of compromise or other anomalies are found.

Detection and response are now more complex, thanks to the evolution of technology and the constant changes in attacker tactics. The volume and complexity of digital activity in today's educational organizations mean more resources are required for IT and security teams, many of which are already stretched thin. With the right people, processes, and tools in place, security and IT teams can avoid an uphill battle when it comes to protecting the organization's networks and data.

While using automation can help lighten a security professional's workload in some instances—or at least free up some time to focus on other tasks—clever cybercriminals are often able to simulate activity that appears legitimate. This increases the chances of malicious activity going undetected. The challenge is to balance the additional cost of automation with the cost to maintain the person doing the work now—assuming the work is being done. While this is a challenge given the distributed nature of many educational organizations, security leaders need to make the case either way. The first step in this process is gathering and correlating data. Gathering as much data as possible from as many sources as possible is a daunting task. Start with the number of endpoints, network devices, and cloud resources. Then identify the procedures and steps a machine could do instead of a human. Remember, the candidates for automation are those tasks in your standard operating procedures and playbooks that are recurring and rarely change.

The most common cyber threats in education are:

1. **Ransomware**
2. **Data breaches and leaks**
3. **Phishing scams (including emails, text messages, and business email compromises)**
4. **Distributed denial-of-service (DDoS) attacks**
5. **Third-party vendor incidents[2]**

Lastly, the cybersecurity talent shortage continues to pose challenges for all industries, including the educational sector. According to a recent industry survey of IT professionals, only 26% of the respondents strongly agree that they have the right tools to perform their jobs.[3] And according to the MS-ISAC K–12 Report: A Cybersecurity Assessment of the 2021-2022 School Year, the average school district spends 8% or less of its annual IT budget on security, with 18% of districts spending less than 1%.[4]

This resource shortage is likely a factor in the number of security incidents that education-focused organizations suffer each year. In 2022, the sector experienced a 44% increase in cyberattacks compared to the previous year.[5]

The Cost of Standing Still

According to the Verizon 2022 Data Breach Investigations Report, the educational industry is experiencing a dramatic increase in ransomware attacks, with ransomware making up 30% of the industry's total incidents.[6] A recent news report notes that at least 44 universities or colleges and 45 U.S. school districts were hit by ransomware attacks in 2022, although many more incidents likely occurred but were not publicly disclosed.[7] The volume and increasing sophistication of these threats mean that the educational sector at large is more susceptible than ever to falling victim to stolen credentials and phishing attacks, potentially compromising the personal information of its faculty and students.

The bottom line is that cybersecurity must be a priority in education. Universities, colleges, schools, and districts that do not pay attention to security operations will not be ready when the next cyberattack takes their network offline. The continuing digitization of education and the expansion of the educational IT footprint increases an organization's cyber risk. Integrating more technology into students' and faculty members' daily routines means more significant potential for the loss of those capabilities and the data they handle. All it takes is one incident to impact school operations or student safety or shatter the confidence and trust among parents and administrators.

Cyber-related attacks on educational vendors are costly in fiscal stability and reputational impact, and there are numerous examples of how far-reaching the repercussions of these breaches can be. In 2022, technology integrator Illuminate Education experienced a data breach that exposed over 3 million student records across two of the largest public school systems in the United States: the New York City Department of Education and the Los Angeles Unified school district (LAUSD).[8] Michigan's South Redford school district suffered a cyberattack that closed its schools for two days.[9] A cyberattack in Albuquerque, New Mexico, also forced schools to cancel classes.[10] And LAUSD was hit with a ransomware attack that prompted an unprecedented shutdown of its IT systems.[11]

While the prospect of falling victim to a cyberattack is unsettling for any IT or security leader, the good news is that there are simple, practical steps educational institutions can take today to protect their networks and sensitive data better.

Strategy #1: Make Security Awareness Everyone's Job

All staff members at educational institutions—including those who work outside of security and IT—are high-value targets for threat actors. Implementing network access controls is essential but not enough to curb attackers. Network users are often your first line of defense when it comes to halting a potential attack. Case in point: 82% of breaches that occurred in the past year involved the human element.[12]

An essential element of your school or college's cybersecurity strategy should be building a cyber-aware culture that helps all network users recognize the key indicators of a potential cyberattack. Awareness training must be engaging and interactive and delivered in multiple formats. Your security awareness program should also assume that longtime staff members still need refreshed training and new learning experiences. Keeping skills and knowledge updated is daunting and, at times, a challenge many will try to avoid. But it's crucial to protecting your environment. Find ways to make security awareness training fun and interesting and reiterate that users can also put these learnings into practice at work and home.

As for any IT or security staff members you have in-house, offer them opportunities to attend security-focused trainings or conferences. Refreshing their knowledge about common reference frameworks—such as MITRE ATT&CK—can help educate IT and security staff about attack surfaces and attack types, potentially spurring new detection strategies. If possible, incorporate quarterly or twice-yearly incident response tabletop exercises into your security program. These activities can help you hone your processes related to incident response, which prove invaluable when an actual attack occurs.

Strategy #2: Consolidate Your Networking and Security Technologies

Many students and faculty now access school resources at home and will continue to do so for at least a portion of their respective weeks. They may also spend time in the office, on campus, or on the road. Regardless of location, educational organizations must maintain a consistent security profile and posture for each user while enabling the appropriate degree of access to the institution's applications, services, and information. Simply using the traditional virtual private network (VPN) does not offer the intelligence and granularity of access required for always-on remote access, nor are the traditional home network and endpoint security measures adequate. This work-from-anywhere (WFA) era requires innovative approaches to secure users and their devices.

The most effective defense against clever cybercriminals looking to exploit the move to WFA is to consolidate networking and security point products. When networking and cybersecurity work together as a unified system, operating securely in the highly dynamic environment becomes a consistent resource for an educational institution that can scale, change, and adapt to student and faculty needs without compromising security. Designing and planning for upgrades, adjusting access controls and network segmentation, and consistently protecting data become easier. Expanding the network perimeter to include new devices, platforms, applications, and services—including those within the operational technology (OT) realm, like security cameras and door alarms—is more efficient.

With consolidation, gathering and analyzing the correct technical data gets easier, which makes experimentation and learning possible. Technologists and analysts can expand their knowledge of the organization's footprint and experiment with new protection or detection strategies without exposing critical resources. This consolidation also results in greater efficiencies for a security or IT analyst already wearing multiple hats.

Strategy #3: Staff for Success

Many K–12 IT teams do not have a designated full-time security professional. Likewise, many small college IT teams, and even some moderate-sized educational institutions, need more professional security staff.

Security is often the responsibility of more experienced IT professionals who can only devote half of their time, or even less, each week to managing the organization's security tools. Rare is the K–12 school district or smaller college that has a full-time Chief Information Security Officer (CISO). While some have a more senior manager who looks after the health of the security program, it's common for the program to be divided among several staff members or placed in the hands of the team member with the longest tenure, regardless of their security-specific training and experience.

Less than a quarter (24%) of security professionals say they are not getting their normal workload accomplished within a normal 40- to 45-hour week.[13] And 70% of the security professionals responding to the 2022 (ISC)^2 Cybersecurity Workforce Study believe their organization does not have enough professional staff in place to adequately secure the organization.[14] That survey also shows only 64% of those who work in education believe they can adequately mitigate the risk they find.[15]

The staffing challenge goes beyond sheer numbers. Vulnerability management and risk mitigation require knowledgeable and experienced professionals. With salaries in other industries far outpacing those in the educational market, leaders need to find creative ways to offset the issue by offering additional incentives. Some short-term colleges and universities may provide students with opportunities for work-study and internships to add talent to their teams. Others are relaxing some of the more demanding educational and certification requirements for early career professionals.

Adopting Better Security Programs in Education

Educational leaders must work with K–12 districts and influence college and university boards to be actively involved in strategic planning and funding regarding cybersecurity. Next, those leaders must empower technologists, K–12 educators, higher-education faculty, researchers, and administrators as they commit to increasing the security posture at their campuses, districts, and schools. This requires a collaborative approach to strategic planning and continuing digital transformation, with security being top of mind. It also involves understanding and resolving technical debt from older and end-of-life technology, lack of consistency in patching and remediation, and aging and redundant software and applications. It's unrealistic to think that everything can be fixed at once, but success can be achieved by taking incremental steps to improve the organization's security posture.

While 2022 marked a year of significant and persistent attacks on the educational industry—from K–12 districts falling victim to ransomware to eLearning platforms being compromised—the future can still be bright for cybersecurity in education. Implementing the proper cybersecurity security controls and then performing the right level of security operations will protect the community today and in the future.

[1] "Cost of a Data Breach 2022," IBM, July 27, 2022.

[2] Katie Frichen, "6 Essential K–12 Cybersecurity Protections for the 2022-23 School Year," Security Boulevard, October 13, 2022.

[3] "ITPro Today's 2022 Salary Survey Report," ITPro Today, September 23, 2022.

[4] "MS-ISAC K–12 Report: A Cybersecurity Assessment of the 2021-2022 School Year," MS-ISAC and Center for Internet Security, November 2022.

[5] Alessandro Mascellino, "Education Sector Experienced 44% Increase in Cyberattacks Over the Last Year," Info Security Magazine, October 14, 2022.

[6] "2022 Data Breach Investigations Report," Verizon, May 24, 2022.

[7] Matt Kapko, "Ransomware Hit US Schools at Steady Rate in 2022," Cybersecurity Dive, January 4, 2023.

[8] David Saleh Rauf, "Illuminate Education Removed from Ed-Tech Privacy Pact Following Data Breach," EDWEEK Market Brief, August 10, 2022.

[9] Raymond Strickland, "Officials Provide Update on Cyberattack that Shut Down South Redford Schools," CBS Detroit, September 21, 2022.

[10] Olivier Uytterbrouck and Jessica Dyer, "School's Out as Cyberattack Forces APS to Cancel Classes," Albuquerque Journal, January 12, 2022.

[11] Stefanie Dazio, et al., "Huge Los Angeles Unified School District Hit by Cyberattack," The Associated Press, September 6, 2022.

[12] "2022 Data Breach Investigations Report," Verizon, May 24, 2022.

[13] "ITPro Today's 2022 Salary Survey Report," ITPro Today, September 23, 2022.

[14] "2022 (ISC)^2 Cybersecurity Workforce Study," (ICS)2, October 24, 2022.

[15] Ibid.

February 7, 2023 1:14 PM

1901777-0-0-EN