How AI Can Help Schools Provide Safer, More Secure Learning Experiences

Data and technology complexity in education has increased drastically in the past two years, as schools have adopted digital collaboration tools and videoconferencing platforms to support distance learning. As these institutions have expanded their technology ecosystem, they've also expanded their attack surface and become high-profile targets for cyber threats, including ransomware and malware.

The solutions implemented by K-12 schools, colleges and universities will likely remain part of the teaching and learning experience going forward, so it's critical for these institutions to secure their IT environments.

A January 2022 Center for Digital Education (CDE) survey of 98 education leaders on the topic of cybersecurity found schools face several challenges in this area. Staffing is a top issue. Nearly two-thirds of respondents (64 percent) said their institution needs to hire additional staff to be better protected against cyber threats; and more than half (57 percent) said they need better staff training to keep up with evolving threats and emerging technologies. Respondents also said their organizations have trouble scaling to meet increased IT demands and grapple with legacy systems that are difficult to secure.

Overcoming these barriers will require schools to become AI-ready. Artificial intelligence (AI) is the foundation for several emerging solutions that feature strong built-in security, automation and insights, all of which can help schools improve their security posture without having to hire more IT staff, expand their cybersecurity skills or undertake costly, time-intensive technology implementations to combat security threats.

64% of respondents said their institution needs to **hire additional staff** to be better protected against cyber threats.

57% said they need **better staff training** to keep up with evolving threats and emerging technologies.

85% of data breaches involve some form of human error, and limited cyber awareness resources can **increase schools' security exposure.**

To become AI-ready in the area of cybersecurity, schools will need to take several steps, including understanding their current vulnerabilities and leveraging solutions with automated security capabilities as a force multiplier to deliver safe and secure learning experiences.

Current Security Challenges in Education

Schools face several security challenges, many of which have become more pronounced over the past two years.

To ensure learning continuity, schools have turned to technologies such as mobile hotspots, cloud-based learning management systems, third-party software-as-a-service (SaaS) applications and other virtual collaboration tools. But IT leaders have learned their technology environment is only as secure as the technologies they've implemented. If vendors don't have robust security protocols in place, schools are more susceptible to breaches. In fact, 33 percent of the educational leaders CDE surveyed said third-party applications with insufficient security standards affect their IT visibility.

School leaders typically aren't experts in cybersecurity, and they have limited staffing and budget resources to address security issues. While schools or education systems may have a dedicated IT person or a small IT team, those employees are likely more focused on system maintenance, managing access and troubleshooting than executing automated, proactive security measures.

Schools face cybersecurity funding issues, as well. Some 25 percent of respondents cited lack of funding as one of their top cybersecurity challenges. Another frequent problem is a lack of proper security awareness training for students, faculty and staff. Eighty-five percent of data breaches involve some form of human error,[1] and limited cyber awareness resources can increase schools' security exposure.

"The challenge of cybersecurity in education is made worse by the fact that state and local leaders tend to view the operational resilience of school infrastructure different from government infrastructure," says Corey Lee, Zero-Trust architect for U.S. education at Microsoft. When it comes to security, Lee says, schools are often left to fend for themselves.

"Education should be viewed as critical infrastructure," he says. "Until that happens, some of these challenges may continue to exist."

Indeed, schools have to balance several competing priorities, says Greg Dinin, a senior customer success account manager for the education sector and worldwide cybersecurity champions program lead at Microsoft. That makes it difficult for education to adopt a preventative approach to cybersecurity, he says.

"Schools have to deal with budgets. They have to deal with educating kids in a safe environment. Unfortunately, unless security threats are knocking at their door, schools sometimes have a hard time taking a proactive stance toward cybersecurity."

AI can help schools take a more aggressive approach to cybersecurity and guard against rapidly evolving threats. But to make full use of this emerging technology, schools must first lay the proper groundwork.

"Being AI-ready means having a data-driven focus to security from a protection, detection and response perspective," says Lee. "That ideally involves some form of automation or intelligence that can take action to mitigate modern-day threats."

As Lee says, data is the key to enabling AI-driven cybersecurity. But that doesn't mean schools have to hire data scientists or in-house analysts. Becoming AI-ready can start with understanding your current data landscape and using

existing technology to get insights from that data to help address security gaps. Finding the right technology partner can help address those gaps with proper tools, resources and support.

Best Practices for Improving Cybersecurity in Education

As schools start on the journey toward AI-ready cybersecurity, they should keep the following best practices in mind:

Assess your current security risks. Even with limited budgets, it's important for school districts and higher education institutions to invest time and resources to better understand their current vulnerabilities and security practices.

Schools can start by taking inventory of what sensitive data they collect, what data they share and where they store all this information. They should also understand what data is encrypted in their systems (and what isn't), the state of their current backup and recovery processes, and whether they have unpatched or outdated software in their environment. Though it would be beneficial for schools to do a wide-ranging cybersecurity risk assessment, they can start by focusing on their most critical IT assets and systems and expand from there as time, budget and resources allow.

Define your security strategy and goals. Once schools identify their current security gaps, they can formulate a strategy for addressing them. The CDE survey found education institutions understand technology will play a key role in their efforts to develop a more responsive security strategy. To better protect against cyber threats, education leaders said their schools will need to provide students and staff with tools to secure their home networks (40 percent); procure solutions that provide additional monitoring (25 percent); and increase their own use of automation, AI and machine learning to secure their networks (20 percent).

These results indicate schools are primarily focused on prevention and detection. Dinin and Lee both say it's also critical for education institutions to center their security strategy around Zero-Trust principles to respond more effectively to threats. Zero Trust is a security approach based on the principle of least privilege. It involves granting access to systems based on a user's role and continuously authenticating users, applications and devices — even after they've entered the network.

Schools can use Zero Trust as a framework for developing policies regarding which users and devices should have access to which systems and data. A comprehensive strategy should encompass multi-layered security approaches and governance policies that focus on strengthening password security, mobile device management and rules governing remote access. The right strategy should also include an incident response plan that details the steps schools will take to mitigate the impact of an attack when a breach occurs. Ongoing cybersecurity training for students, faculty and staff is also important.

Once schools have defined their plan, they can adopt technologies like security monitoring solutions and AI-driven security tools to reduce their attack surface and address specific security gaps.

It's critical for education institutions to center their security strategy around Zero-Trust principles to respond more effectively to threats. A Zero-Trust framework will help them develop policies regarding which users and devices should have access to which systems and data.

Work with a strategic partner. As threats evolve, education institutions will find it increasingly challenging to adequately address security on their own. Collaborating with a trusted partner can bring greater automation, visibility and efficiency to schools' security operations.

The right partner can offer solutions with integrated AI and machine learning capabilities, along with expertise and ongoing guidance to help schools maintain a strong security posture in the face of changing threats.

Lee says a technology partner can help schools better map their security priorities to the capabilities they have — and what they

AI can help schools move from cyber defense to offense. However, for schools to harness the full power of this technology, they must understand their current security gaps, define their security goals and collaborate with a partner that offers AI-enabled solutions with integrated security.

need — while addressing their cybersecurity insurance requirements. A partner can also enhance schools' AI maturity and their use of AI-enabled security tools, he says.

"It's important to start off with strategic conversations about how schools can leverage AI as part of a Zero-Trust strategy or their overarching security architecture," Lee says, adding that in many cases schools may already have AI-ready tools in their environment they can use to improve security.

When assessing specific teaching and learning solutions, look for products that have been built with security in mind. They should have embedded endpoint detection, identity and access management, and comprehensive data and application protection capabilities. Look for collaboration tools that encrypt network communications by default, and solutions that leverage multi-factor authentication features.

Dinin adds that schools will benefit most from integrated solutions that improve their cyber resilience.

"In the past, there was this notion of best-of-breed security solutions solving the security problem," Dinin says. "But today, considering how important it is for schools to respond on a timely basis, best-of-integration solutions trump that. Relying on 15 different vendors to provide holistic security often leads to schools spending more money and having to stitch everything together or create more environmental complexity. With an integrated security platform provider, you can cut down on implementation time and be sure everything works together. You're also consolidating your security spend."

Advancing AI-Ready Cybersecurity in Schools

Schools' main priority is to educate students. But as these institutions have now become prime targets for hackers and cyber criminals, security has become an integral part of their efforts to create the best possible learning environment for students.

AI can help schools move from cyber defense to offense. However, for schools to harness the full power of this technology, they must understand their current security gaps, define their security goals and collaborate with a partner that offers AI-enabled solutions with integrated security. Taking these steps will help schools advance both their AI and security maturity.

"We have to focus on modernizing security operations across education, and ultimately what that means is helping schools respond faster to attacks and put themselves in a position to recover quickly and be more resilient," Lee says.

This piece was written and produced by the Center for Digital Education Content Studio, with information and input from Microsoft.

[1] https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2021-dbir-executive-brief.pdf

Produced by: gt CENTER FOR DIGITAL EDUCATION

The Center for Digital Education is a national research and advisory institute specializing in K-12 and higher education technology trends, policy and funding. The Center provides education and industry leaders with decision support and actionable insight to help effectively incorporate new technologies in the 21st century. **www.centerdigitaled.com**

For: Microsoft

Microsoft is the leading platform and productivity company for the mobile-first, cloud-first world, and its mission is to empower every person and every organization on the planet to achieve more. In education, it's to empower every student. We believe limitless potential is within every student, every educator, every school. Together we can unlock this potential by providing technology that empowers educators and inspires students. Learn more at **microsoft.com/education**.

IMAGES PROVIDED BY SHUTTERSTOCK.COM