Best Practices for Zero-Trust Cybersecurity in Education

With a preventive cybersecurity strategy, K-12 and higher education institutions can reduce the threat of an attack while saving money and resources.

Schools have drastically expanded their virtual environments in recent years. Largely in response to the COVID-19 pandemic, K-12 and higher education leaders have given students and staff access to school networks through tablets, personal computers and mobile devices.

But this embrace of digital tools creates new vulnerabilities. Every student's tablet, administrator's laptop, or teacher's smartphone is another new endpoint hackers can potentially infiltrate and use as a point of entry into a school's network.

Schools are also particularly vulnerable to hackers because many institutions still use antiquated legacy technologies, either due to a lack of funds or inflexible leadership. The antivirus software many schools use to protect against attacks leaves schools constantly on the defensive against a ransomware threat.

Many schools also rely on cyber insurance as a defensive form of cybersecurity. Rather than implementing stronger security systems, schools assume they will be protected by insurance companies. But insurance does nothing to actually reduce vulnerabilities, and paying a ransom only encourages further attacks.

A preventive, rather than defensive, response strategy can protect against hacks before they begin.

"When you get hacked and you're in a defensive mode, it's already too late. The hackers are already in," says Richard Zizian, CEO at Critical Period Risk Management, the consulting division of a cybersecurity insurance firm.[1] "With a defensive mode, you have to find the malware, contain it and minimize it. With preventive technology, you don't have to do any of that."

A preventive approach goes hand in hand with Zero Trust, which has quickly emerged as a critical framework for modern cybersecurity. Zero Trust is predicated on the idea that, rather than having "trusted" in-network users, every individual and every device must be continuously verified in order to maintain access to networks and data.

Below are five best practices for implementing a preventive Zero-Trust cybersecurity response that will keep data secure while saving schools valuable time and resources.

1 Think beyond brick and mortar.

When establishing a defensive cybersecurity strategy, schools need to think beyond the four walls of the classroom.

"School leaders need to ask themselves, 'What does my perimeter look like today?'" says Rick Remes, senior carrier enterprise channel manager at Lookout. "That perimeter is likely radically different than what you first architected it for."

In today's world of tech-enhanced education, the perimeter of the school network extends to any location that a student might learn or a staff member might work.

To account for this change in the perimeter and endpoints of a school network, CISOs and other IT leaders in education must think beyond the physical school and develop a cybersecurity strategy that reflects the complex digital ecosystem of schools today.

2 Apply multiple solutions.

Because of the complexity of modern education technology systems, IT leaders need to adopt a multi-solution strategy to achieve a Zero-Trust model.

"No one product covers the full spectrum of all attack surfaces," says Zizian. "But there are solutions that can put specific surfaces in a Zero-Trust, no-hack environment."

With a multi-pronged approach, IT leadership can protect sensitive information across all surfaces and in all locations.

If schools want to start with one tool, Zizian recommends they begin by implementing a solution that addresses any potential mobile threats. Mobile devices have become the preferred attack surfaces for hackers largely because many people don't think to install cybersecurity tools on their phones. By implementing a technology to prevent against these attacks, schools can avoid many of the latest and most common malware attacks.

3 Find the right strategic partners.

While school leaders may be wary of implementing new cybersecurity solutions, the implementation process can be drastically streamlined when working with a responsible and responsive vendor.

The ideal vendor will wholeheartedly embrace a preventive Zero-Trust mindset. The partner will also offer consistent support for a school throughout the implementation process and beyond. The provider should work with the school to run the solution in discovery mode prior to implementation, ensuring it works well with various endpoints and other school equipment.

A responsible vendor should also work closely with operators to teach them how to utilize any analytics dashboards so they can easily monitor the security environment themselves.

With a trustworthy vendor that embraces Zero Trust, schools can be sure they have the best technology and the appropriate training.

4 Change leadership's mindset.

IT leaders must convince education administrators to embrace the shift in cybersecurity strategy from defensive to preventive.

Many school leaders are resistant to technological changes, often due to concerns about cost or the amount of labor required. Some administrators simply don't think a cyberattack will occur in their institutions.

"School districts may think, 'It's not going to happen to me,'" says Remes. "Leaders may think they have their cybersecurity squared away, but there is a [higher] level of sophistication in cyberattacks today. Schools need to be prepared."

To convince schools to procure the necessary solutions, IT will need to communicate the benefits of defensive cybersecurity to school leadership. In particular, technology leaders will need to convince administrators that adopting preventive strategies actually saves time and money in the long run.

> "Preventive technology is a much more efficient way to deal with cybersecurity issues, but it takes a mindset change."
>
> *Richard Zizian, CEO, Critical Period Risk Management*

"Preventive technology is a much more efficient way to deal with cybersecurity issues, but it takes a mindset change," says Zizian.

5 Focus on cyber resilience.

Human beings inevitably make mistakes. They will open phishing emails and unknowingly log onto dangerous networks. If people will always create vulnerability within a school's network, school cybersecurity solutions must anticipate those vulnerabilities. A security approach based on resilience focuses on mitigating risks and minimizing the impact of breaches when they do happen.

"Human nature will cause people to inevitably click on links they shouldn't," says Zizian. "Zero-Trust technology acknowledges that attacks will occur and stops them before they can start."

Conclusion

K-12 schools and institutions of higher education have a responsibility to protect students and ensure the safety of faculty, staff and administrators. In the digital age of take-home devices and technology-enhanced learning, schools cannot afford to wait for a cyberattack to happen.

By embracing solutions that offer a proactive approach to cybersecurity – and adopting a preventive mindset based on Zero Trust and cyber resilience – schools can maintain a teaching and learning environment that's safe and secure for everyone.

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

1. https://webinars.govtech.com/Risk-Management-Strategies-for-K-12-and-Higher-Ed-Ransomware-Preparedness-and-Cybersecurity-Insurance--140179.html

Produced by: 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: Lookout

The Lookout Security Platform is a unified and scalable cloud-delivered solution that enables government agencies to meet today's Zero Trust Architecture standards and mitigate data protection risks. Lookout's triple-play integration across secure access technologies such as CASB, ZTNA, SEG, and MES. For more information, visit **www.lookout.com/solutions/government/state-and-local**.

IMAGE PROVIDED BY ADOBESTOCK