A **CENTER FOR DIGITAL EDUCATION** THOUGHT LEADERSHIP PAPER

Cybersecurity for the K-12 Classroom

How Security Services Partnerships Protect Today's Schools

SPONSORED BY SOPHOS

Ransomware attacks at K-12 schools — which had been increasing exponentially in the last decade — seem to have leveled off over the past year. But the news is not as good as it seems: The expense of recovering from a cyberattack has continued to skyrocket. The mean cost of an attack in K-12 rose from $1.59 million in 2023 to $3.76 million in 2024, even as the number of incidents decreased.[1]

As attacks grow more disruptive — and increasingly sophisticated — it's more important than ever for schools to have a strong strategy for cyber defense and recovery. But that can be hard. Few schools and districts have the resources they need for a dedicated cybersecurity team or a 24/7 security operations center.

For that reason, many K-12 schools are turning to security services partnerships, in which trusted private sector providers handle all aspects of cyber strategy, ransomware prevention, recovery and risk mitigation.

Successful security partnerships go far beyond traditional vendor/purchaser transactions, or even security consulting services, says Paul Zindell, director of sales engineering for the public sector at Sophos.

"The end goal for education environments should be, 'How do I make sure I have a covered service that is actually looking for these bad actors in my environment and stopping them? Not *talking* about stopping them. Not consulting. But hands-on-keyboard *stopping* these attackers in real time.'"[2]

More Expensive Attacks

$1.59M

Mean cost in 2023 for K-12 organizations to recover from a ransomware attack

$3.76M

Mean cost in 2024

Security services partners handle all aspects of cybersecurity strategy for K-12 education.

The challenges of safeguarding your environment

Firewalls for servers and endpoints once offered sufficient protection to fend off cyberattacks. Those solutions are no longer enough. Schools also need hands-on analysts who study the IT environment, ask questions, run queries and check for active adversaries — and stop them in real time.

“Once the attackers start realizing live individuals are cutting off their connections, stopping their payloads or seeing what they’re doing, that’s usually when they back off and say, ‘Okay, wait a minute, there are actual defenders here who are fighting back,’” Zindell says.

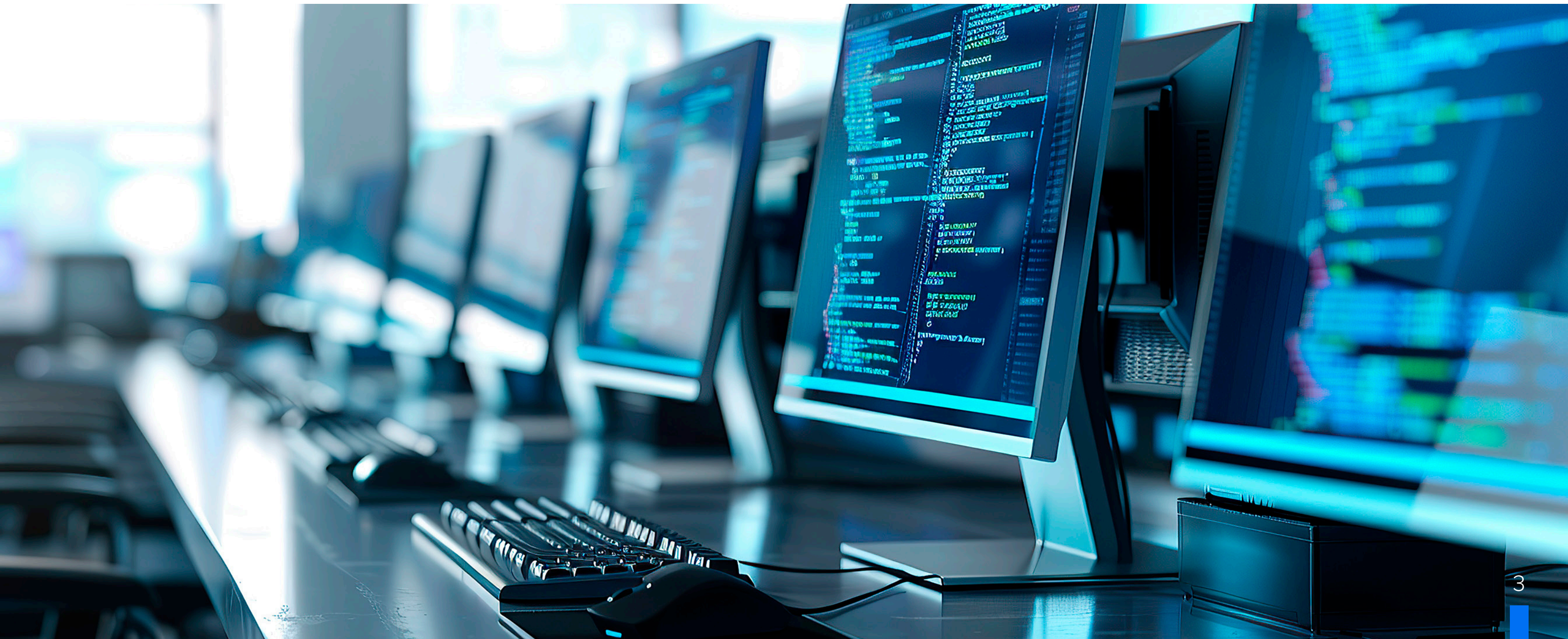
Security starts with understanding the breadth of your IT environment — which can be more complicated than you think. Websites, email networks and laptop computers all represent security vulnerabilities, but so do smart whiteboards, printers, cameras and connected Internet of Things (IoT) devices.

Schools may have hundreds of vulnerable exposure points they don’t know about.

“For a lot of IoT items, whether it’s food services or heating and air conditioning systems, if there’s a path where someone can get in, they can then start accessing other systems from inside,” says Tom Ryan, Ph.D., a Center for Digital Education senior fellow and the former chief information and strategy officer for the public school systems in Santa Fe and Albuquerque.[3] “So even though it might be a lot of work, it’s critical to create a checklist of things that are crucial so that you can reduce your exposure.”

Schools are often surprised by the extent of their vulnerabilities. “I’ve had a lot of conversations with customers who say, ‘Oh, yeah, we don’t have much that’s exposed,’” Zindell says. “‘We just have a website, and that’s about it.’ Then we run an external vulnerability scan and find hundreds and hundreds of items that are exposed.”

Penetration testing is also an important part of assessing your security needs. This involves a controlled, simulated cyberattack to evaluate your security readiness.



Ryan says he has encountered some schools that are reluctant to conduct a penetration test because they know they will fail. They're missing the point, he says. "It's not a test where you're getting an A, B, C or D. It's a test to help you identify what needs to be corrected."

Security services providers make these assessments less daunting.

"A lot of people neglect to do those vulnerability assessments because it's a lot of work, but they forget that they don't have to do it alone," Ryan says. "Instead of installing some huge platform, learning how to use it, getting a certification and then running a vulnerability scan, they can have a service that does it for them."

Establishing a security services partnership

As K-12 districts and schools consider a security services partnership, there are some valuable points to keep in mind.

☑ **Find a partner before you need them.** It's best to have trusted partners and a plan in place before your school experiences a cybersecurity incident. This ensures your provider has a keen understanding of your IT environment and your specific needs.

"You don't want to be searching for that partner in the middle of a ransomware attack or a cyber event," Zindell says. "You want somebody who already knows what you're doing and understands your infrastructure."

A security partnership also reduces the risk of an attack in the first place. A trusted provider has expansive IT teams with the necessary security skill sets, along with the latest threat detection tools. They will fortify your school's security environment far better than you likely could on your own.

☑ **Find a partner with the right experience.** Education is the most likely sector to experience a ransomware attack, with 63% of K-12 schools worldwide reporting in 2024 that they had been hit by an attack within the past year.[4] (In 2023, that number was 80%.) Look for a security partner with deep experience in public education. Their expertise and understanding of the K-12 security landscape will strengthen your cyber defenses and help manage risks of an attack.

☑ **Work together to develop a security plan.** Having a partnership in place lets you plan for a better response. Proper planning ensures everyone knows what to do in the event of a cyberattack. "If we have *this* type of attack, then boom, we go through *these* steps," Ryan says. "You have this responsibility, and that person has another."

Go Deeper

Watch this webinar:

Building a Protected K-12 Classroom

Download this rapid roadmap:

CENTER FOR DIGITAL EDUCATION

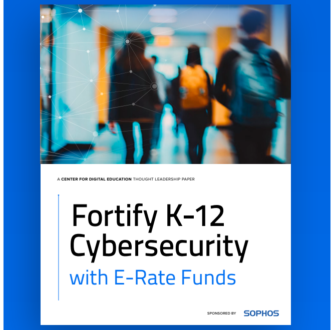
RAPID ROADMAP

NEW RULES FOR SCHOOLS ARE COMING

How to prepare for new requirements on reporting cyberattacks.

SPONSORED BY: SOPHOS

Download this paper:


A CENTER FOR DIGITAL EDUCATION THOUGHT LEADERSHIP PAPER

Fortify K-12 Cybersecurity

with E-Rate Funds

SPONSORED BY SOPHOS

A precise incident response plan is difficult to coordinate without a security partnership, he says. “You can’t operate like that unless you’ve established the right partner. You certainly don’t want to be doing it in the middle of your superintendent calling and saying, ‘What is going on?’ Time is important.”

☑ **Get buy-in — and get it in writing.** Help budget directors and non-IT leaders understand the stakes related to cybersecurity. Your incident response plan should explain what your schools should do in the case of a cyberattack, as well as the consequences that will happen if you don’t. If the school board votes against funding the response plan, have someone sign off on it so it’s in writing that the board declined to fund it.

“That gets attention, especially when somebody signs, ‘Yeah, we choose not to do this,’” Zindell says. “And it protects you. You don’t want people to blame you for the response to a ransomware attack when you couldn’t implement a plan because there was no funding for it.”

No school wants to be hit by a ransomware attack. But it’s a near-certainty that you will be.

Conclusion

No school wants to be hit by a ransomware attack. But it’s a near-certainty that at some point you will be. And with increasingly connected learning environments and digital administrative services, the impact of an attack can be devastating.

A security services partnership is an ideal way to optimize your cybersecurity efforts, make the most of limited resources and ensure continuity in teaching and learning.

“If you think the cost of a security partnership is expensive,” says Ryan, “consider a million-dollar ransom bailout just to get your system back up so your teachers can teach and students can learn.”

1. https://news.sophos.com/en-us/2024/07/11/the-state-of-ransomware-in-education-2024/
2. https://webinars.govtech.com/Building-a-Protected-K-12-Classroom%3A-Cybersecurity-for-the-Modern%2C-Connected-Learning-Environment-143384.html
3. https://webinars.govtech.com/Building-a-Protected-K-12-Classroom%3A-Cybersecurity-for-the-Modern%2C-Connected-Learning-Environment-143384.html
4. https://news.sophos.com/en-us/2024/07/11/the-state-of-ransomware-in-education-2024/

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

gt CENTER FOR DIGITAL EDUCATION

Produced by the 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

SOPHOS

Sponsored by Sophos
Sophos delivers superior cybersecurity outcomes by providing cybersecurity as a service to protect companies of all sizes from the most advanced cyberthreats. Our cybersecurity products and services include managed detection and response (MDR), firewall, email, endpoint (XDR), and cloud native security protection. Sophos products and services defend against ransomware, phishing, malware, and more. They connect through the cloud-based Sophos Central management console and are powered by Sophos X-Ops, our cross-domain threat intelligence unit. We provide fully managed security solutions so you can manage your cybersecurity directly with our security operations platform. Or, you can supplement your in-house team with Sophos' products and services.

www.sophos.com

ADOBESTOCK/AI GENERATED