Sponsored by

Spectrum ENTERPRISE

7 cybersecurity facts every K-12 district should know

eSchool News

K-12 school systems make very attractive targets for cyber criminals. As education has become more digital in nature, the use of mobile devices and smart classroom tools has increased the attack surface available to hackers. At the same time, K-12 networks are especially vulnerable to attacks because most schools spend relatively little time or money on cybersecurity.

Cyber attacks might not be completely avoidable, but there are steps that K-12 leaders can take to reduce the odds of a successful attack and protect their sensitive information. The first step is to understand the nature of the threats they face and where they are most vulnerable.

To enhance this understanding, here are seven cybersecurity facts that every K-12 leader should know — along with recommendations to help districts keep their networks and data secure.

1. Since 2016, there have been at least 1,300 successful cyberattacks on K-12 schools in the United States.

For the six-year period from 2016 to 2021, the K-12 Security Information Exchange (K12 SIX) has cataloged 1,331 publicly disclosed cyber incidents affecting U.S. school districts across a wide array of incident types, including student data breaches, ransomware attacks, denial of service (DoS) attacks and more. This equates to a rate of more than one incident per school day, on average.[1]

However, the actual rate of cyberattacks on K-12 school systems is likely much higher. The requirements for school systems to publicly disclose cyberattacks are “weak and routinely circumvented,” the organization says. Given that many attacks are not reported, “the true picture is surely bleaker; anecdotal evidence suggests perhaps 10 to 20 times more K-12 cyber incidents go undisclosed every year.”[2]

Although cybersecurity is a top IT priority for K-12 leaders, many school systems still aren’t doing enough to protect their networks from attacks. “One reason might be that they’re understaffed,” says Doug Levin, head of the K12 SIX. “District leaders also might feel they have too many competing priorities, or else they don’t accurately appreciate the risks they’re facing.” In the end, however, failure to act could be much costlier than adopting proactive, commonsense measures to guard against cyber threats.

“Given increasing reliance on technology for school district operations, there is every reason to expect that, absent significant intervention, cyber incidents will continue to plague school districts, placing members of the public at significant—and avoidable—risk,” the organization notes.[3]

2. Phishing and ransomware attacks against K-12 networks are getting more sophisticated.

While the number of incidents alone should be concerning to K-12 leaders, there is evidence to suggest the severity of these incidents is also on the rise.

“Increasingly, we’re seeing threat actors target school systems specifically,” says Doug Levin, who heads the K-12 Cybersecurity Resource Center. “They’re doing research on the staff at a school district and what roles they occupy. They might try to spoof an email from a superintendent, a principal or a vendor. They might create sophisticated landing pages that duplicate school district websites as a way to trick people into giving them personally identifiable information. This sort of targeted attack is quite concerning, and it’s an escalation of what we’ve seen before.”

Ransomware attacks are also becoming more sophisticated in nature. Criminal actors aren’t just looking to hold K-12 networks hostage, Levin observes, but they’re now stealing data as well. “This increases the leverage they have over the school district to pay their ransom demand,” he explains, “and whether or not the ransom is paid, the criminals also try to monetize that personally identifiable information.”

In addition, ransomware demands have increased dramatically, in some cases far exceeding $1 million per incident. In Broward County, Florida, hackers demanded $40 million in a recent ransomware attack.[4]

Ransomware demands have increased dramatically, in some cases far exceeding $1 million per incident. In Broward County, Florida, hackers demanded $40 million in a recent ransomware attack.

3. Large urban and suburban districts are most at risk.

School districts with significant enrollments appear to be at a greater risk for experiencing a cyber incident than smaller school districts, according to K12 SIX. Although school systems with at least 10,000 students make up 8 percent of districts nationwide, they account for 31 percent of all cyber incidents tracked by the organization.[5]

There are a few factors that might explain this pattern. For instance, larger school systems manage more technology devices than smaller ones, and they have more students and employees using technology—meaning they have a larger threat profile. They also might be subject to more ransomware attacks because they have larger budgets.[6]

On the other hand, districts with smaller enrollments have a smaller threat profile for malicious actors and a lower chance of a being affected by user actions.

However, it would be a mistake to think that smaller school systems aren't also at risk. "School districts from all 50 states have suffered significant cyber incidents, from very small, rural districts to the largest urban school districts in the nation," the organization observes.[7]

4. Even though K-12 leaders say cybersecurity is a top priority, they still underestimate the risks.

In the most recent survey of K-12 technology leaders by the Consortium for School Networking (CoSN), cybersecurity was recognized as the top IT priority as it has been since 2015, when CoSN first conducted its survey.[8]

However, when asked about perceived cybersecurity risks, the vast majority of respondents (84 percent) did not rate any specific threat as a high risk — and not a single incident type received a high risk rating by a majority of respondents. Phishing was the incident type considered to be the greatest threat, with 45 percent of school district IT leaders rating it as a "medium/high" or high risk. Of those 45 percent, however, only 16 percent consider phishing to be a high-risk threat.

The survey results suggest that K-12 technology leaders continue to underestimate the risk from cyber threats. For instance, phishing scams are on the rise across all sectors, including education. "According to the FBI," CoSN says, "the number of reported phishing complaints doubled from 2019 to 2020, and [phishing] is by far the No. 1 internet crime type. The reality is that all networks and their users are at high risk from phishing scams."

Because phishing scams can be the point of entry for virtually all other incident types, "everyone needs to be on high alert," CoSN says. And given that the FBI and other security agencies jointly stated that K-12 is the most targeted public sector for ransomware, "it is surprising that district IT leaders do not rate this risk higher [as well]."

5. The majority of school districts don't have a cybersecurity plan.

Underestimating the risks posed by cyber criminals might explain why a majority of K-12 districts (59 percent) lack a cybersecurity plan.

According to CoSN's survey, only 41 percent of districts conduct regular audits to test their cybersecurity defenses — and the same percentage of respondents said they have implemented a cybersecurity plan. "These two practices are considered key factors in assessing a district's operational readiness in a digital environment," the organization says.[9]

A cybersecurity plan is the cornerstone of any effort to defend against cyber attacks and mitigate the risks to K-12 networks. A thorough cybersecurity plan should address the policies and technologies that a district will use to guard against cyber threats, as well as its emergency response protocols so that if an attack does occur, employees will know how to respond.

6. Only half of districts require cybersecurity training for all employees — and one-quarter don't require any training.

The vast majority of cyber attacks (85 percent) use social engineering to exploit human vulnerabilities, such as by tricking network users in order to gain entry.[10] This underscores the importance of training students and employees in cybersecurity best practices.

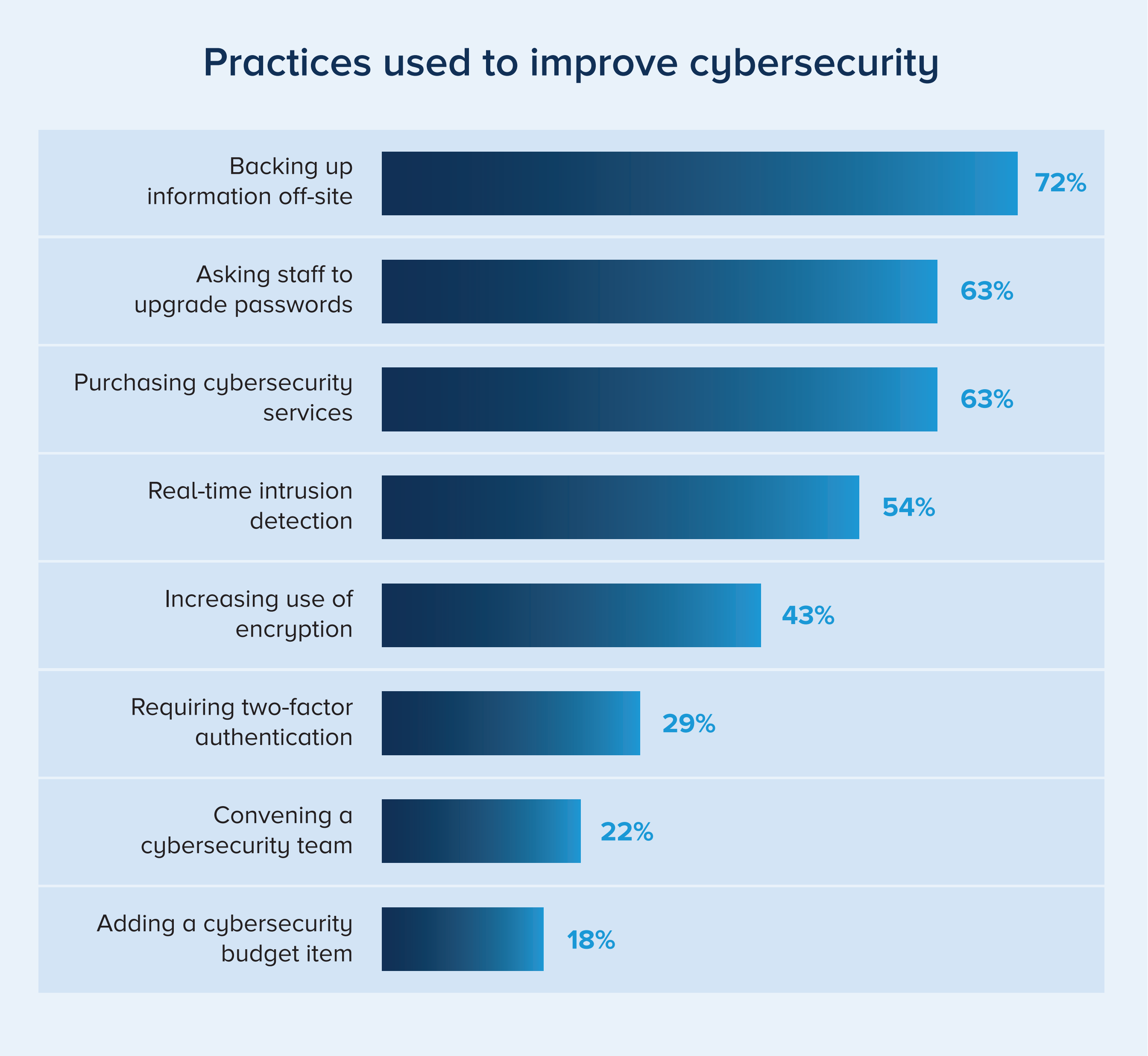
While nearly three out of four districts (74 percent) either require or plan to require cybersecurity training for employees, only half currently require this for all staff members. "Training just one stakeholder group is not sufficient," CoSN says, "as all staff are vulnerable to attacks that can endanger the network and/or put personally identifiable information at risk."[11]

The lack of any training at all is the worst-case scenario, and just over a quarter of districts (26 percent) don't require any employee training on cybersecurity. As CoSN advises: "TRAIN, TRAIN, TRAIN! Make sure everyone knows security awareness is their job and who to talk to if they make a mistake."[12]

7. There are many other steps that districts should be taking, such as monitoring for network intrusions in real time.

CoSN's survey suggests there is considerable room for improvement in the strategies that districts are using to secure their networks.

For instance, only 72 percent of districts back up all of their information and store it offsite in case of an attack. Just 63 percent of districts purchase specific cybersecurity products and services, and only 54 percent monitor their networks in real time for unauthorized intrusions. Fewer than half of districts (43 percent) are increasing their use of data encryption.[13]



Recommendations for K-12 districts

Consider managed network services.

When school districts purchase and install their own network infrastructure, they're also accountable for implementing patches and upgrades to keep these systems secure. With E-Rate eligible Managed Internal Broadband Services, districts can extend the capabilities of overworked IT staff and keep up with rapidly evolving network needs—while also enhancing their security. With managed services, security patches and firmware changes are installed automatically, keeping network systems continually secure and up to date.

Invest in multiple cybersecurity defenses.

A multilayered approach to network security offers the best protection from cyber threats. In a multilayered approach, school systems employ multiple security systems and technologies to protect various operational layers from attacks, such as a firewall service to protect the internet gateway, antivirus and anti-malware software to shield network endpoints, DDoS protection to guard against a distributed denial of service attack and so on. These multiple defenses all work together to enhance security by protecting against numerous types of threats, as well as multipronged attacks that seek to gain network access through multiple channels.

Partner with a trusted provider for help.

Many K-12 districts lack the in-house expertise to implement sophisticated cyber defenses. A reliable service provider with extensive experience in serving the K-12 market can help. Spectrum Enterprise has helped hundreds of K-12 clients improve their cybersecurity with hands-off services that don't require the use of IT staff time to administer, such as their Managed Security Service and DDoS Protection solutions.

An urgent need for action

With cyber threats of all types on the rise, K-12 leaders can't afford to wait any longer to take comprehensive action to secure their networks and data from attacks. A multilayered approach to cybersecurity offers the best chance of defense. K-12 districts can balance the need for sophisticated protection and simplicity of operation by choosing security as a managed service. With the right partner, districts are supported from design through implementation and beyond.

Learn how Spectrum Enterprise is uniquely qualified to protect K-12 networks:
enterprise.spectrum.com/k12ed

[1] Levin, Douglas A. (2022). “The State of K-12 Cybersecurity: Year in Review – 2022 Annual Report.” K12 Security Information Exchange (K12 SIX). https://www.k12six.org/the-report

[2] Ibid.

[3] Ibid.

[4] “Cyber Criminals Attack Broward County Public Schools, Demand $40M,” NBC 6 Miami, April 1, 2021 https://www.nbcmiami.com/news/local/computer-hackers-demanded-40-million-from-broward-schools-after-breach-report/2419205/

[5] Levin (2022).

[6] Ibid.

[7] Ibid.

[8] “The State of EdTech Leadership 2021 Survey Report,” Consortium for School Networking (CoSN) https://www.cosn.org/focus-areas/leadership-vision/state-edtech-leadership

[9] Ibid.

[10] “Most Digital Attacks Today Involve Social Engineering,” Security Intelligence, Aug. 13, 2021 https://securityintelligence.com/articles/most-digital-attacks-today-involve-social-engineering/

[11] “The State of EdTech Leadership 2021 Survey Report,” CoSN.

[12] Ibid.

[13] Ibid.

eSchool News

This report was produced by eSchool News, the leading online platform that delivers daily technology news and information to K-12 education administrators, educators, and technology professionals, and dedicated to the advancement and wise use of technology to improve teaching and learning for all. eSchool News offers ed-tech decision makers a wide range of informative content — including newsletters, webinars, case studies, white papers, websites, and more — that provide in-depth coverage of the latest innovations, trends, and real-world solutions impacting the education community. **Explore more at www.eSchoolNews.com**

Spectrum ENTERPRISE™

About Spectrum Enterprise

Spectrum Enterprise, a part of Charter Communications, Inc., is a national provider of scalable, fiber technology solutions serving many of America's largest businesses and communications service providers. The broad Spectrum Enterprise portfolio includes networking and managed services solutions: Internet access, Ethernet access and networks, Voice and TV solutions.
The Spectrum Enterprise team of experts works closely with clients to achieve greater business success by providing solutions designed to meet their evolving needs.
For more information, visit enterprise.spectrum.com.