CORO

The Ultimate Guide to Strengthening Cybersecurity at K-12 Schools

2024

Table of Contents

Intro

There are few higher callings than educating the next generation of young people. It’s such a big responsibility that teachers deserve to give it their full focus.

Unfortunately, even with so many schools today being strapped for educational resources, cybersecurity has become an area that warrants more attention.

The problems with school cybersecurity are numerous, including bare-bones IT staffing and extremely meager budgets. Luckily, there are ways to improve your school’s cybersecurity despite these obstacles.

In this guide, we’ll take a look at how schools can get on a path to stronger cybersecurity while being mindful of limitations like funding and resources.

And note that while this guide is being offered from the perspective of a cybersecurity company, it’s an issue close to our hearts; there are a lot of employees at Coro who have children that are students in K-12 schools. So we are all invested in wanting schools to have the best protection possible.

I. Why Schools Are Being Targeted and How to Defend Against It

School districts may not seem like lucrative targets for cyber attacks, especially struggling K-12 schools. However, to a cybercriminal, a school can be a more rewarding target than a bank for several reasons:

- **Data**
  Schools are a treasure trove of information, including student data, administrative records, and the credit card and social security numbers of parents.

- **Success rates**
  Nearly half of all schools that were subjected to ransomware attacks paid the ransom in order to get their data back. When contrasted with other industries, like retail or government, education has a higher chance of forking over the money. Sometimes, when schools refuse to pay the ransom, hackers will reach out to parents of students directly and offer to withhold their data from being sold or made public in exchange for payment.

- **Lack of defenses**
  Schools spend less than 8% of their IT budget on cybersecurity (enterprises tend to spend around 10%), which makes them easier targets.

A ransomware attack or data hack can have devastating consequences on schools, including disruption to classes, identity theft, and financial losses as technology needs to be replaced.

How Are Criminals Getting In?

Criminals use a number of different methods to gain access to schools' networks and systems. According to reports:

- 30% of attacks on lower-educational institutions originated through malicious emails/phishing.
- Email-based attacks drove one in five ransomware incidents for higher educational institutions.
- According to Internet Safety Labs, nearly all apps (96%) used by schools have unsafe data-sharing practices for children.

Considering these common starting points, addressing gaps in schools' security postures doesn't have to be complex or expensive, especially with the right cybersecurity partner.

What Schools Can Do to Protect Themselves From Cyber Attacks

Email Protection

Email security entails safeguarding against cyber threats and unsolicited messages transmitted via email. It encompasses defending against various risks such as inbox hijacking, domain impersonation, phishing attempts, fraud, malware dissemination, spam, and ensuring encryption to shield email content from unauthorized access.

Despite its pivotal role in communication, most email providers lack inherent security and privacy features. This deficiency persists, making email a primary target for cyberattacks.

Endpoint Security

Endpoint protection is a type of cybersecurity software that protects devices like laptops, desktops, smartphones, and tablets from cyber threats. These devices are called "endpoints" because they are the points at which users access a network. Endpoint protection software helps to prevent malware, viruses, and other attacks from infecting these devices. Because a large volume of attacks on schools (and businesses) start with email-based attacks like phishing, endpoint protection is key.

Data Governance Protection

A study by Stanford University and Tessian found that 88% of data breaches are caused by human error. Staff or students may inadvertently share sensitive information, such as personally identifiable information (PII), payment card information (PCI), protected health information (PHI), and other regulated sources of data, which can be exploited.

The right cybersecurity solution employs automated scanning techniques to analyze files and emails within a school's network. This scanning capability allows it to sift through vast amounts of data quickly and efficiently. Upon detecting sensitive data, the software triggers alerts to administrators or designated personnel within the organization. These alerts serve as notifications of potential data leaks or compliance violations, prompting immediate action by administrators to mitigate risks and address any breaches.

Regular Security Audits and Backups

School systems should prioritize conducting routine security audits across all individual schools within their districts. These audits help identify vulnerabilities in systems, enabling swift implementation of security measures to address and mitigate potential risks effectively.

Schools should also perform regular backups of their data to mitigate the impact of potential cyber-attacks. By maintaining up-to-date backups, educational institutions can minimize downtime and swiftly recover essential information in the event of a security breach or data loss incident.

Patching and Updates

Schools should ensure that any software is up-to-date and patched regularly. Patching involves applying updates released by developers and manufacturers, which often include security patches. These updates address vulnerabilities and strengthen the resilience of systems against potential cyber threats. By staying current with patches, schools minimize the risk of exploitation by malicious actors seeking to compromise sensitive data or disrupt operations.

Enabling Two-Factor Authentication

Implementing two-factor authentication adds an additional layer of security to user accounts, requiring a secondary form of verification beyond passwords. By simply incorporating this authentication method, school systems enhance access controls and mitigate the risk of unauthorized account access.

Awareness training and engagement

It's ironic that schools often skip this important step - training, cybersecurity education, and engagement for both students and faculty are often some best defenses. We have a lot more on this topic later on in this guide, but cybersecurity awareness is an ongoing process, and users benefit from periodic updates and refresher courses to stay informed about emerging threats and security best practices.

If you’re not sure where to start with comprehensive cybersecurity protection, our experts can help you figure out a plan that makes sense for your school’s needs. Just get in touch.

II. Navigating budget constraints

For schools that are already battling to fund the learning materials, equipment, teachers, and support they need to foster an environment conducive to learning, threats such as ransomware stretch their overburdened budgets considerably—that is to say, if they can afford to take action at all.

Fortunately, there are solutions that will provide security solutions that can safeguard a school's data without requiring a substantial investment. Here are a couple tips:

Invest in Long-term Solutions

Taking a long-term perspective allows schools to save money and keep up with technology changes without having to make upgrades all the time. Cloud-based solutions, for instance, offer scalability, flexibility, and lower costs by getting rid of the need for infrastructure and upkeep on-site. By spending money on these kinds of solutions, schools can get the newest technologies without spending a lot of money.

Consolidation

If your school district is paying several contracts to various cybersecurity vendors, it could be creating more risk. That's because too many tools can actually make you less safe while draining your budget. Consolidating your cybersecurity solutions into one platform can have dramatic impacts on your protection and reduce the workload on your IT team.

Stay Flexible

As important as it is to consolidate tools and invest in solutions for the long haul, it's equally crucial to stay away from one-size fits all tools. Yes, consolidating with a single vendor is important, but you don't want to get locked into paying for a bunch of features you don't need. Instead, consider a vendor that'll let you pick and choose the protections you want, like Coro.

Keep It Simple

When you're shopping for a new cybersecurity provider, you'll want to go with something that'll make your IT team's life easier. Adding an overly-complicated solution could mean your IT folks spend more time trying to manage and configure their security instead of proactively solving for threats.

Find and Apply for Cybersecurity Grants

In terms of finding more funding for your school's defense, there are some great grant programs available to improve security. Private companies, as well as state and local governments, have opportunities to help K12 schools and higher education institutions around the country address their cybersecurity risks head-on so they can focus on what matters most: teaching the leaders of tomorrow. There's a running list here, but chances are there are some local options available to your school as well.

Consider Tapping the Community

Within any school, chances are there are some parents or partners who are close to either the technology, security, or cybersecurity space. Think about spreading the word to see if there's anyone available to assist as a potential freelancer or first responder, for example.

III. Three Cybersecurity Frameworks for School Systems

Cybersecurity frameworks are valuable tools that guide organizations in navigating the complex landscape of threats and vulnerabilities. These frameworks are essentially sets of standards, guidelines, and best practices that help organizations build and maintain effective security postures.

Think of them as roadmaps designed by cybersecurity experts that outline essential steps to identify, protect, detect, respond to, and recover from cyber incidents. Frameworks provide a structured approach to managing cybersecurity, ensuring no crucial aspects are overlooked. They promote risk assessment and mitigation, helping organizations prioritize their efforts based on potential threats.

Today, many frameworks have been designed for various different stakeholder groups. Some frameworks are general; others are sector-specific. There are three frameworks that have proven popular—and really effective—in the US public school sector:

1. The National Institute for Standards and Technology Cybersecurity Framework (NIST CSF)

The NIST CSF is a comprehensive and broad framework that applies to public and private entities in several areas. The framework has three primary components and covers five high-level functions: identify, protect, detect, respond, and recover.

While this is a thorough and beneficial approach, it's very complex, and understanding and implementing the framework effectively can be daunting for resource-constrained school districts. The latest Nationwide Cybersecurity Review found K-12 schools lagging behind other government agencies in NIST CSF implementation.

2. The Center for Internet Security Critical Security Controls Framework (CIS Controls)

Developed by the Center for Internet Security, the CIS Controls offer a more focused approach. Its 153 recommended practices, organized into 18 categories and grouped into three Implementation Groups (IGs), target specific cyber-attack tactics. The three implementation groups include:

- **Implementation Group 1 (IG1)** is best-suited to small to medium-sized businesses with limited IT and cybersecurity expertise, with an emphasis on protecting IT assets and people. The emphasis is on preventing wide, non-targeted cyberattacks (essential cyber hygiene). IG1 organizations prioritize operational continuity and the protection of low-sensitivity data.
- **Implementation Group 2 (IG2)** is suited for businesses with specialist IT asset and system management teams that must meet federal or state cybersecurity compliance requirements. IG2 enterprises manage sensitive data and can withstand temporary service interruptions.
- **Implementation Group 3 (IG3)** covers all 153 CIS-recommended best practices for companies with several specialized cybersecurity specialists who must adhere to federal and state legislation. IG3 best

practices are intended to prevent targeted attacks from sophisticated adversaries and to lessen the impact of expected zero-day attacks.

Schools might find IG1 and IG2 particularly relevant. IG1 addresses essential cyber hygiene suitable for limited staff environments, aligning with the majority of smaller schools. IG2 caters to organizations with dedicated IT staff and regulatory compliance requirements, reflecting the needs of larger districts or those facing heightened risks.

Will it work for your school? On the one hand, this framework helps schools prioritize critical security measures based on their size, resource and risk profile, provides specific, easily understood best practices and targets known attack vectors relevant to the educational sector. On the downside, it doesn't offer the comprehensive guidance of the NIST CSF. There are regular updates, and keeping up with new versions can be resource-intensive.

3. The K12 SIX Essential Cybersecurity Protections for School Districts (K12 SIX Essential Protections)

Unlike broader frameworks like NIST CSF or CIS Controls, K12 SIX stands out for its specificity. Designed specifically for school districts, the K12 SIX Essential Protections offer a highly relevant and practical framework. Its 12 actionable defenses address common cyber threats faced by schools and align with insurance requirements and government guidance. Categorized and presented with a four-level implementation rubric across four categories, it helps schools prioritize and measure progress.

These categories represent the key areas of focus for the framework:

- **Network traffic sanitization**
  This focuses on measures to block malicious traffic and protect against online threats entering or leaving your school network.

- **Device safeguarding**
  This covers securing all devices used within the school, including computers, tablets, laptops, and mobile phones.

- **Identity protection**
  This is crucial for safeguarding confidential data of students, teachers, and staff, including passwords, access controls, and data encryption.

- **Regular maintenance**
  This emphasizes the importance of ongoing activities like patching vulnerabilities, updating software, and conducting backups to maintain effective defenses.

Each category consists of four levels of implementation:

1. **At risk:** This indicates the absence of basic control measures, leaving the school vulnerable to cyber threats.

2. **Baseline:** This signifies the implementation of essential security practices to address minimal requirements.

3. **Good:** This represents a more advanced level with stronger security measures in place.

4. **Better:** This reflects the best possible implementation, exceeding basic requirements and providing robust protection.

Using this rubric, schools can assess their current cybersecurity posture within each category, identifying areas where they are "at risk" and need improvement. It also provides a roadmap for progress, highlighting areas where they can move from "baseline" to "good" or even "better" by implementing additional recommended practices.

Compared to NIST CSF or CIS Controls, K12 SIX is designed for beginners and offers fewer best practices, but seamlessly integrates with CIS Controls and NIST CSF for further growth.

The Journey of Cybersecurity Maturity

Think of K12 SIX as the launchpad on your cybersecurity journey. Start here, implement its recommendations, and gradually progress towards more comprehensive frameworks like NIST CSF or CIS Controls as your resources and expertise evolve. Here are some recommendations to bear in mind:

- **Choosing a Framework Is Less Important Than Using It Effectively**
  Frameworks are closely aligned and often interrelated to one another, which means choosing a specific framework isn't all important - committing to a framework and to cybersecurity risk management is all that really matters.

- **Work Within Your Limits**
  Even with enough resources, developing a mature cybersecurity risk management program can take years. Investing in stronger frameworks may drain resources away from actions that can strengthen defenses in the short run. If your resources and expertise are limited, focus your attention where it can have the biggest impact and then look to build on that. Along those lines, consider cybersecurity solutions that aren't one-size-fits-all, and instead can work around your most pressing needs.

- **Keep Evolving**
  Cybersecurity frameworks are developed to address vulnerabilities and threats. Not all best practices are applicable to all K-12 organizations due to variances in technology, IT systems, risk tolerance, cybersecurity capacity, and budgets.

Remember, frameworks are just tools. Ultimately, achieving robust cybersecurity requires a multi-layered approach, including ongoing training and risk awareness, collaboration and monitoring.

IV. How Awareness Training Helps Protect Schools

When it comes to schools, getting leadership, faculty, staff, and even students into the process of detecting threats can go a long way toward stronger defenses.

KnowBe4 is a security awareness training platform that helps organizations train team members to understand and recognize cyber threats.

We spoke with Just about what hackers are really after when they attack schools, advice to IT departments working at these organizations, and why schools may want to team up.

This interview has been cut down for length; to read the full interview, visit our blog.

“It’s not just IT or InfoSec’s job to make sure we're secure, it’s everyone’s job.”

John Just | Chief Learning Officer | KnowBe4

Q. In terms of implementing stronger cybersecurity protection, what are some of the common themes you've seen in schools and universities? What are some of the challenges that they're facing in implementing stronger protections?

John Just:

“Yeah with K12 schools, obviously taking off prem, on prem data center things that can be (targeted by) ransomware and moving those to more cloud protection with multi-factor authentication.

“Cloud-based systems that are easily recoverable and backed up and a better hardening of protection. And like we said at the beginning about our job: see something, say something. If you can, get as many people involved in that as possible.

“Often with these attacks, what we're seeing is you've got several teachers that are already compromised, right? It’s already there in their email accounts. And then (attackers are) able to social engineer from the inside. So, very complex, multi-layer attacks.

“And I say very complex, but really not that complex when you think about it; it's low-hanging fruit, and (the attackers) are able to then move around internally and convince people to give them access to things or get access to things that they really shouldn't.

“So raising that awareness and building that culture of seeing something and saying something. Being educated about what the red flags are and being part of that alert system to be able to tell people if they're seeing something that's unorthodox. It’ll add to a big physical presence right within colleges and universities.

“So the old USB attack that's been around forever and some of these more tried and true that, you know now within the organizations like businesses. Are not going to, you're not going to just walk in and plug in a USB into something and that's not going to work anymore, right? But I could walk into a school library right now and I could bring a USB key with me.

“And I can install malware and I can get that spreading throughout the network. So there's that physical component that I have to be aware of as well. And again, see something, say something and be part of that human firewall.

“In terms of I guess one of the challenges you're seeing, is it an awareness thing? Is it a budget thing? Is it all of the above? Is it just not having big IT teams? I think all that plays a role. I think all that plays a role.

Q. What advice would you give to IT directors who are working at a school like a K12 or a university today in terms of improving their protection?

John Just:

“Educate yourselves. Educate your staff. It's an ongoing problem… Your adversaries are learning constantly. And so you need to be learning constantly.

“This is a persistent problem that's not going to have an easy solution. And I think some of the mindset out there is we're going to patch this. We're going to patch the social engineering. But just like patching, there's a new patch that comes out all the time as vulnerabilities. And we have to think of it as ongoing patching. It's not going to be finished.”

“And so if you have that would be number one. Have that mindset that this is a persistent ongoing problem that I need to have a persistent ongoing solution for. And we sometimes get wrapped up in, ‘Okay, the sales people are telling me if I buy this one firewall, if I buy this magic device, if I buy this, if I buy that.’ You're not going to buy your way out of this problem.

“So even though you don't have the budget, which is a problem in education. The good news is you're on a level playing field with the people who do have the money. So you have to, I mentioned, you have to get leadership involved. You have to get them to buy in. Sometimes you have to do a separate training program for execs.

Conclusion

Schools are facing unprecedented challenges from cyber attackers, and our students deserve better protection. Whatever path you choose to help protect them, let’s deliver stronger protection year after year. Hopefully these tips can help, Coro has lots of affordable options for schools. If you need more assistance, please reach out.