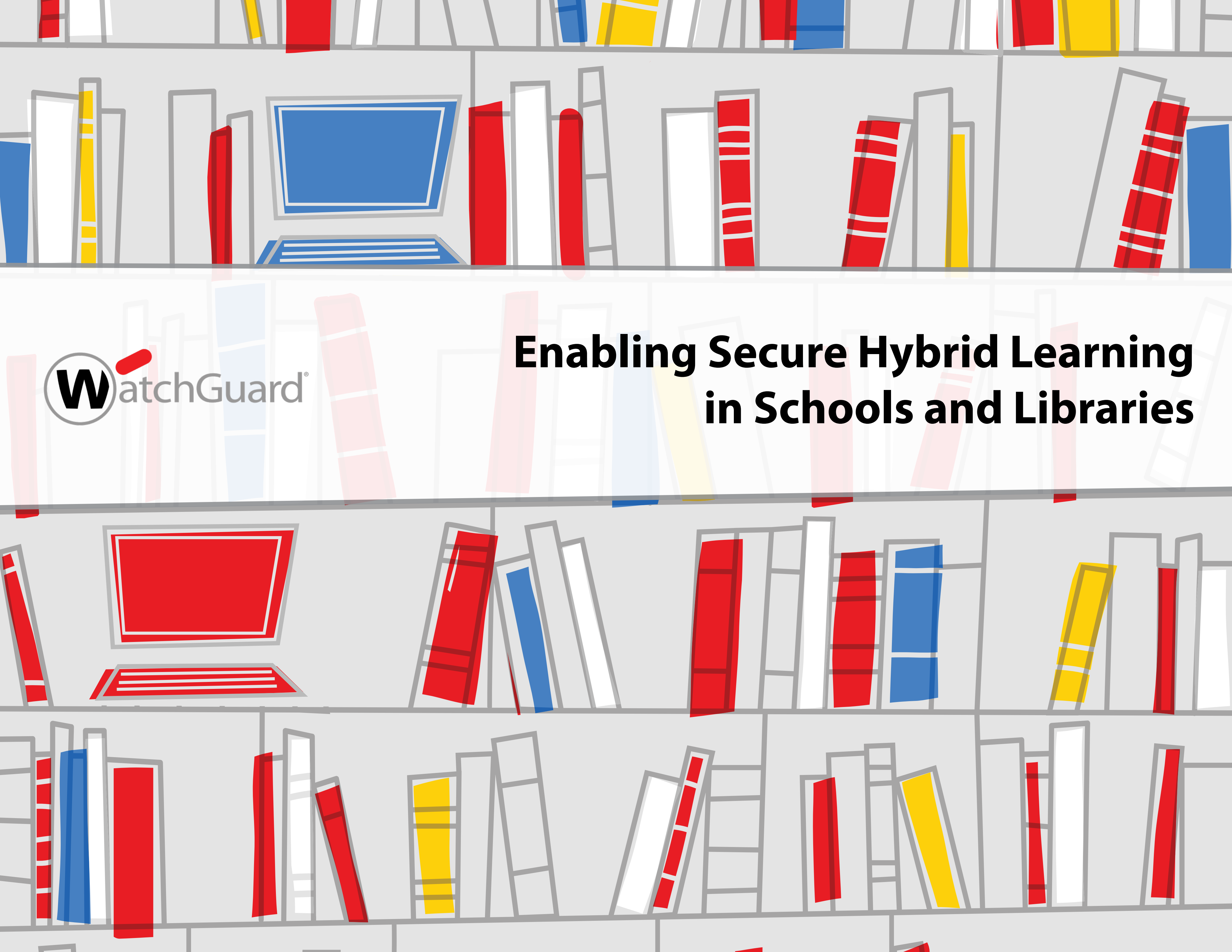
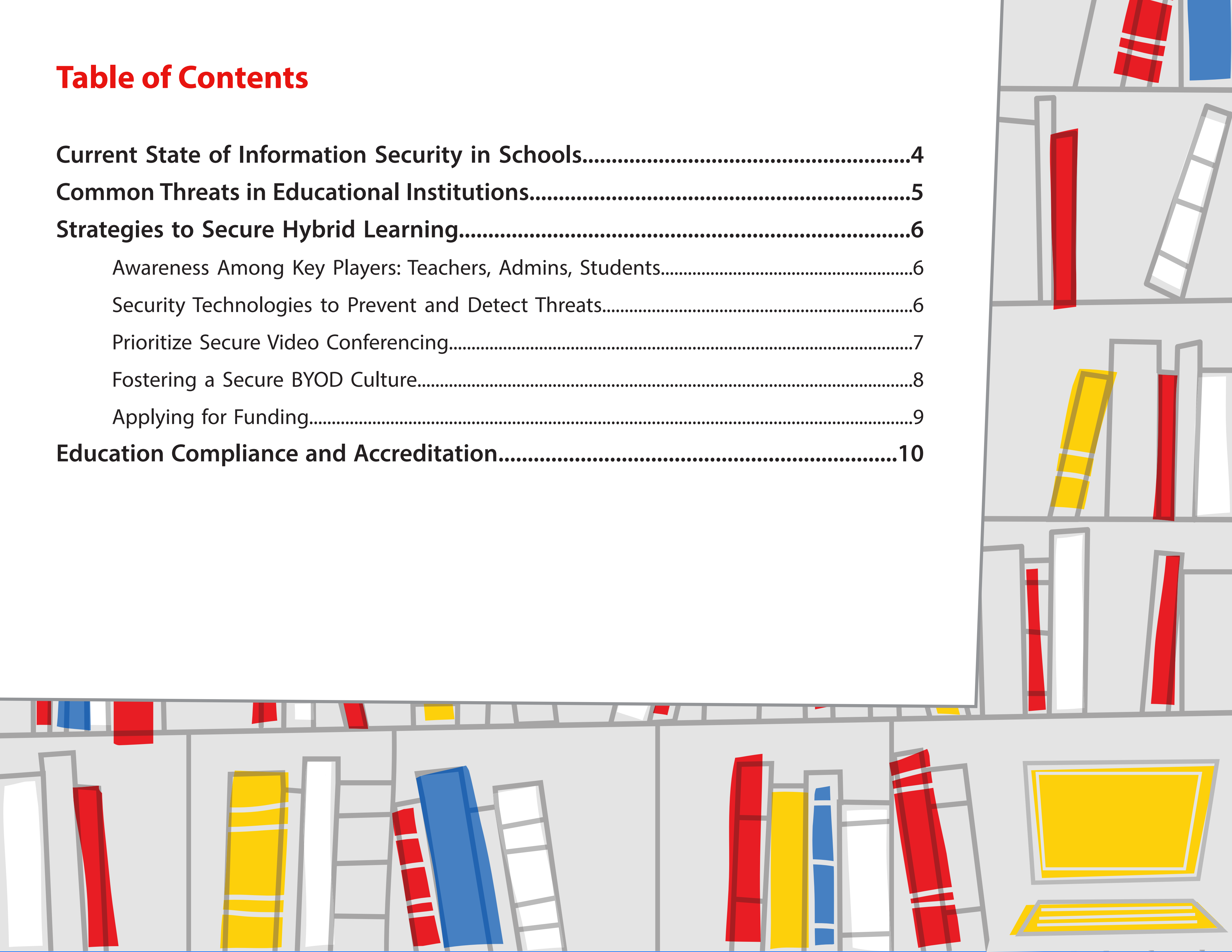


WatchGuard

Enabling Secure Hybrid Learning in Schools and Libraries

Table of Contents



Data security is a top priority across industries. For the education sector in particular, this touches on both the need to protect devices as well as sensitive information and user privacy (student, staff, and family personal information).

With the current landscape in which schools are operating, where they are enabling learning in-person, virtually, and through personal devices, what are the top cybersecurity risks impacting this sector? More importantly, what strategies can decision-makers adopt to deliver secure learning across platforms?

This eBook will discuss ransomware, the greatest vulnerability in the education sector, as well as other key threats, along with policies and best practices that are helping educational institutions remain secure in the classroom and online.

Current State of Information Security in Schools

Ransomware is the greatest cyber threat in the education sector. IDC's 2021 Ransomware Study found that **37% of global organizations** were victims of some form of ransomware attack that year. For schools – kindergarten through twelfth grade – these attacks have increased significantly in recent years. According to the Multi-State Information Sharing and Analysis Center (MS-ISAC), 57% of ransomware incidents between August and September of 2020 (in the US) involved K-12 schools.

Other reports, like Emsisoft's annual report in 2021, showed that ransomware attacks affected more than 2,300 thousand local governments, schools and healthcare organizations.

But this isn't just an issue affecting schools in the United States. The UK's National Cyber Security Centre (NCSC) has issued ransomware attack warnings after several reports were made. In one instance, these threats forced a school to postpone its reopening.

Why schools pay ransom after an attack

Many school districts have made the news for deciding to pay ransom after falling victim to a breach. Some have paid as much as half a million dollars.

When a ransomware attacker infiltrates a school district's network, they can lock up access to computers, systems, and valuable personal information. In some cases, staff could not get paid due to the breach. On top of that, the risk of losing data or worse, suffering an online data leak, puts too much pressure on school administrators, which is why many choose to pay the ransom.

Reporting incidents: If your school or organization has been a victim of ransomware, report it immediately to your local government or field office. Bringing this issue to public officials can create additional opportunities to deliver greater funding or resources so educational institutions have the support they need to optimize cybersecurity in their environments.

Common Threats in Educational Institutions

- Phishing: Malicious activity performed to steal sensitive data such as username, passwords, credit card information, etc.
- DDoS: Distributed denial of service or DDoS attacks target network assets to try to cause a shutdown. These attacks commonly cause disruption rather than a data breach.
- BYOD: (bring your own device)
- Doxing and cyberbullying: The act of releasing private information, statements or records on the Internet to cause harm, such as exploitation, financial harm, or defamation.
- Domain spoofing: A type of phishing attack where hackers register web domains using similar naming conventions as legitimate websites in an attempt to trick users into a scam.
- End-of-life software: Outdated software and IT appliances that don't get the necessary patching, upgrades and maintenance can be a source of vulnerabilities.

Strategies to Secure Hybrid Learning

Prioritize Awareness Among Key Players: Teachers, Admins, Students

Educate teachers, employees, and administrators about social engineering attacks to limit cybersecurity risks. Introducing security concepts through awareness training programs can help create secure practices when accessing computers, systems, and login credentials. Key security awareness education should include:

- Detecting phishing attempts
- Using email security best practices
- Avoiding weak or exposed passwords
- Reporting incidents to IT department

Prioritize Practices That Prevent and Detect Threats

Filter content

While IT is proactive in blocking restricted content, having additional capabilities can help block websites, emails or files that can lead to vulnerabilities and incidents. These restrictions provide greater protection against threats, but also support compliance regulations, such as the Children's Internet Protection Act (CIPA). Content filtering can be deployed using hardware appliances or software as a service (SaaS).

Monitor access

Visibility tools that track and expose threats and identify user behavior contributing to a compromised network are a must-have for achieving compliance. Tracking network security threats, issues and trends accelerates the ability to eliminate threats, set meaningful security policies across the network, and meet critical compliance mandates.

Protect user access with MFA

Because passwords can be compromised so easily, education institutions should implement multi-factor authentication (MFA) alongside any BYOD programs. Look for a solution with optimal user experience that can make it easy to enable authentication right from a user's own phone after a simple install and activation.

Commit to strong and secure Wi-Fi

School Wi-Fi is critical to enable learning, admin, and teaching duties. To deliver secure Internet access, focus on private networks and access points that can handle density without risks. Consider Cloud-managed Wi-Fi solutions for optimized performance, greater visibility and reporting.

Enable Secure Video Conferencing

Video-assisted learning is the most-adopted technology among educational institutions. In a Pulse study, 52% of IT decision-makers in the education sector said that they were planning to invest in video conferencing technologies. According to the Cybersecurity and Infrastructure Security Agency (CISA), the four main steps in ensuring secure video conferencing are: control access, secure connectivity, protect file and screen sharing, and use updated versions of video applications.

Recommended video conferencing best practices

- Make sure your remote learning policies include guidelines for the use of video conferencing. Create training materials to ensure that admins, teachers, and students understand how to apply and follow established policies.
- Only allow use of tools and software approved by the school.

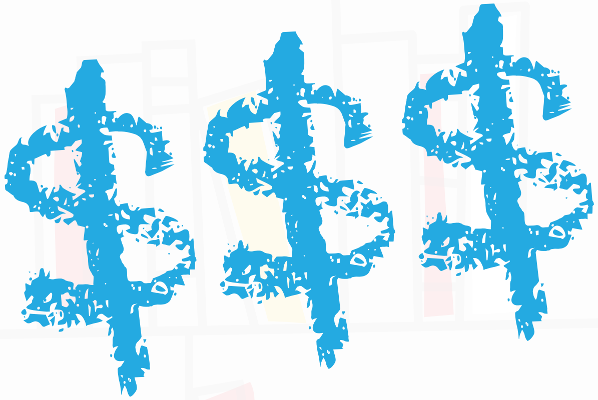
Foster a Secure BYOD Culture

Now more than ever, we're embracing the bring-your-own-device culture. Not only are students and teachers more comfortable using their own devices – and therefore more productive – BYOD programs implemented in schools breed greater device longevity (as students are more likely to care for their own equipment), increased student collaboration and organization, and even empowerment, as there are a multitude of apps available to encourage and assist learning, including those specific to reading and writing. And of course, institutions that implement BYOD programs enjoy major cost savings when staff and faculty bring their own devices, negating the need to purchase 1,000 laptops and the various maintenance and upgrading services that come with them.

But there are many security and privacy concerns with students having uninterrupted access to their devices – after all, BYOD has coined a copycat term: BYOR (bring your own risk). Personal devices are much more prone to malware, accessing consumer sites that don't necessarily provide the same level of security afforded sites designed for business-to-business transactions. Also important to consider are the resources and bandwidth required from IT staff; forgotten passwords, data loss, email synchronization, and difficulty accessing wireless networks are a small sample of the issues IT support may be inundated by with the adoption of BYOD.

Leverage Funding for Cybersecurity

Educational institutions can't afford NOT to invest in security. Though even small districts have multi-million-dollar budgets, cybersecurity provisions are often limited, making schools an easy target. Cybercriminals are well aware that network defenses in education are often poor and ransoms are more likely to be paid. After all, schools cannot function without access to their data. Take the Manor Independent School District in Texas for example; they lost $2.3 million due to a phishing attack. In almost 90% of these attacks, criminals used Gmail accounts to send phishing emails.



Three ways to support security in schools through additional funding

Local, state, or nationwide funding programs

Find out if your district is eligible for subsidized programs by local or federal entities. In the US, for example, the E-Rate program provides funding to schools and libraries for eligible IT technology and services.

Check out the E-Rate eligible services >

Grants from nonprofit organizations

As with other needs that may not be addressed in the regular school or district budget, grants offer a chance to fund cybersecurity projects. A good first stop for cybersecurity grants is to check out nonprofit organizations supporting educational institutions and find available grants that qualify for technology or services investment.

Parent Teacher Association (PTA) or similar groups

Some school districts have parent-driven committees whose purpose is to support school fundraising opportunities. This too can be an effective way to identify additional funding streams to optimize the technologies and services that enable a cyber-secure learning environment.

Work with a service provider

A managed security provider (MSP) can work as an extension of your institution to fill any IT security gaps through managed service offerings, such as initial deployment and configuration, ongoing maintenance, monitoring, reporting, and more. These types of managed security services are critical for organizations that do not have the required in-house resources or expertise to ensure continuous protection and a strong security posture – all while reducing the need for dedicated headcount.

Education Compliance and Accreditation

As new technologies and online resources are integrated into learning programs, concerns around student privacy and security naturally arise. Educational facilities around the world are required to meet local or national Internet safety regulations or face significant financial consequences.

Children’s Internet Protection Act (CIPA)

CIPA imposes requirements on schools or libraries that receive discounts for Internet access or internal connections through the E-Rate program – a program that makes certain communications services and products more affordable for eligible schools and libraries. Schools and libraries subject to CIPA may not receive the discounts offered by the E-rate program unless they certify that they have Internet policies in place that include technology protection measures. These measures must block or filter Internet access to pictures that are obscene or harmful to minors.

Keeping Children Safe in Education (KCSiE)

Similar in design, the UK’s KCSiE is a child-centered and coordinated approach to safeguarding impressionable children under the age of 18. Core to the KCSiE regulation is the requirement for schools and colleges to do all they reasonably can to limit a child’s exposure to risks from the school’s or college’s IT system. As part of this process, they need to ensure that they have appropriate filters and monitoring systems in place. It is noted, however, that educators should be careful that “over blocking” does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.

With exposure to the web only increasing, the need to meet Internet safety regulations – and thereby enjoy the protections they afford schools, their faculty, and their students – is clear.

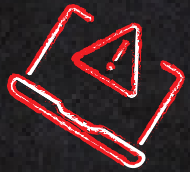
Other Things to Consider for a Secure Learning Experience

Conduct security assessment

There are several options for conducting the assessment itself, but all typically include reviewing the threats against your assets (who/what can cause you harm), identifying vulnerabilities (how harm can occur), and likewise, identifying the consequences (what assets can be harmed, and to what degree).

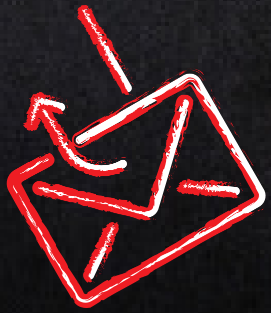
Network segmentation

In addition to being a security-driven best practice, network segmentation can also play an important role in maintaining your network's efficiency. In large, unsegmented networks, all computers can communicate with all other computers, and the chance for network congestion rises. Segmentation divides your school's network into smaller networks, or "clusters," which will help them perform faster and more efficiently.



Application filtering

As much a necessity in keeping kids on task as it is keeping them safe and schools compliant, application filtering tools restrict what kids can see or when they can see it online. This practice tightens security across your network and adds productivity safeguards, enabling administrators to monitor and control access to the Internet.



Conclusion

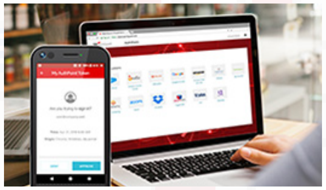
Schools are embracing technology at a faster speed to enable hybrid learning and adapt to a more flexible experience. Why prioritize deploying strong cybersecurity in schools and libraries? To remove the challenges that get in the way of what matters most: teaching and learning. Let's continue to take action to maintain availability in our schools so they can do the important job of educating our children. Let's support the initiatives that empower schools with the tools and resources to enable a secure learning environment so our communities can learn anywhere, anytime.

- Foster a culture of security-aware students, teachers, and admins
- Implement technologies that protect, prevent, detect, and respond
- Update software regularly
- Establish consistent remote-learning policies to ensure secure access

THE WATCHGUARD PORTFOLIO

Network Security

WatchGuard Network Security solutions are designed from the ground up to be easy to deploy, use, and manage – in addition to providing the strongest security possible. Our unique approach to network security focuses on bringing best-in-class, enterprise-grade security to any organization, regardless of size or technical expertise.



Multi-Factor Authentication

WatchGuard AuthPoint® is the right solution to address the password-driven security gap with multi-factor authentication on an easy-to-use Cloud platform. WatchGuard's unique approach adds the "mobile phone DNA" as an identifying factor to ensure that only the correct individual is granted access to sensitive networks and Cloud applications.

Secure Cloud Wi-Fi

WatchGuard's Secure Wi-Fi Solution, a true game-changer in today's market, is engineered to provide a safe, protected airspace for Wi-Fi environments, while eliminating administrative headaches and greatly reducing costs. With expansive engagement tools and visibility into business analytics, it delivers the competitive advantage businesses need to succeed.

Endpoint Security

WatchGuard Endpoint Security is a Cloud-native, advanced endpoint security portfolio that protects businesses of any kind from present and future cyberattacks. Its flagship solution, WatchGuard EDPR, powered by artificial intelligence, immediately improves the security posture of organizations. It combines endpoint protection (EPP) and detection and response (EDR) capabilities with zero-trust application and threat hunting services.

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in unified cybersecurity. Our Unified Security Platform® is uniquely designed for managed service providers to deliver world-class security that increases their business scale and velocity while also improving operational efficiency. Trusted by more than 17,000 security resellers and service providers to protect more than 250,000 customers, the company's award-winning products and services offer five critical elements of a security platform: comprehensive security, shared knowledge, clarity & control, operational alignment, and automation. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit WatchGuard.com.