Making the Grade:

Getting – and Keeping – High Marks in K-12 Education Security

WatchGuard®

Table of Contents

Overview

Managing the networks for an educational institution is much more a master class in information technology than an introductory course. Combining a user base of students and faculty spread over a large campus, connecting over wired and wireless networks, and the need for access to a broad variety of online learning tools and resources – all while maintaining adequate controls for a safe Internet experience – is no small feat. Frankly, no other environment tests its IT infrastructure more in terms of both performance and security than in education – but thankfully, WatchGuard helps institutions make the grade every day.

Uniquely architected to be the industry's smartest, fastest, and most effective network security products, WatchGuard solutions address the key challenges faced by education today: from achieving and maintaining compliance standards, to securing the explosive BYOD movement. With WatchGuard, educational institutions get – and keep – high marks in security.

KEY CHALLENGE:

Maintaining Compliance and Accreditation

Achieving regulatory compliance is not unlike an exam that never ends – but the stakes are much higher and there's no multiple-choice options. As new technologies and online resources are integrated into learning programs, concerns around student privacy and security naturally arise. As such, educational facilities around the world are required to meet local or national Internet safety regulations, or face significant financial consequences.

Enacted by Congress in 2000 to address concerns around Internet access, the Children's Internet Protection Act (CIPA) is one such regulation. 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. Additionally, before even adopting such a policy, both schools and libraries must provide reasonable notice and hold at least one public hearing or meeting to address the proposal.

Similar in design, the UK's Keeping Children Safe in Education (KCSiE) is a child-centered and coordinated approach to safeguarding impressionable children under the age of 18. For the purposes of the regulation, safeguarding is defined as protecting children from maltreatment; preventing impairment of children's health or development; ensuring that children grow up in circumstances consistent with the provision of safe and effective care; and taking action to enable all children to have the best outcomes. 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.

WatchGuard

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 includes technology protection measures. These measures must **block or filter** Internet access to pictures that are **obscene or harmful to minors.**

Solutions:

MONDAY

CONDUCT A SECURITY ASSESSMENT ✓

To-Do

Completing a network security assessment can alert you to any critical security gaps in your network and inform future allocation of funds to any necessary technology. There are a number of 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).

TUESDAY

FILTER CONTENT ✓

To-Do

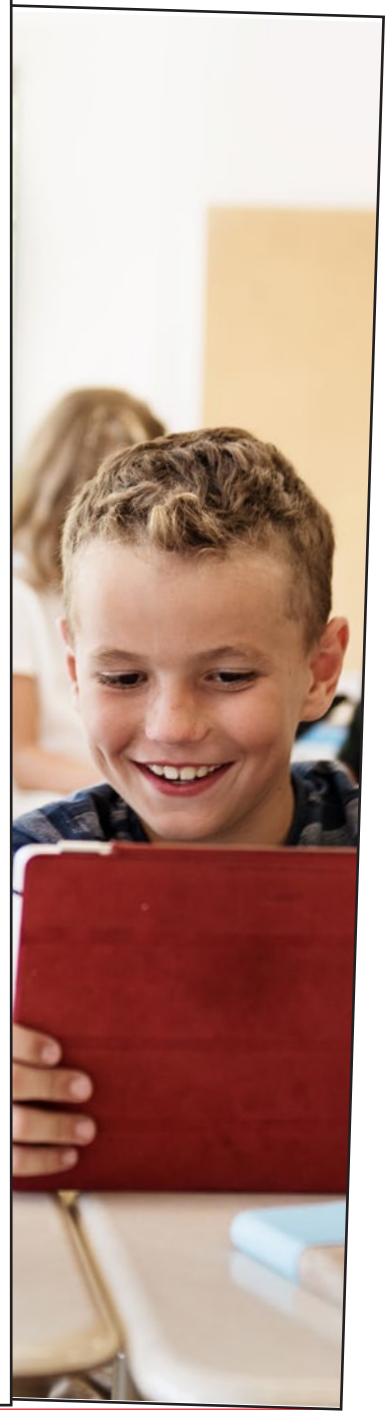
Blocking access to inappropriate material and websites, content filtering tools can also create activity logs that determine which user was acting inappropriately. When IT is proactive in blocking restricted content, schools and libraries prevent users from accessing unsavory sites in the future. Additionally, dated firewalls are an easy way to fall out of compliance, and firewall protections equipped with filters that restrict access to specific sites, such as WatchGuard's Firebox® appliances, are eligible for E-Rate funding. For that reason, firewalls should be a priority.

WEDNESDAY

MONITOR ACCESS ✓

To-Do

Visibility tools that track and expose threats and identify user behavior contributing to a compromised network are a must-have for achieving compliance. WatchGuard Dimension provides granular, big-data network visibility without the associated cost and complexity. By tracking network security threats, issues and trends, it accelerates the ability to eliminate threats, set meaningful security policies across the network, and meet critical compliance mandates.



KEY CHALLENGE:

Securing BYOD (Bring Your Own Device)

Gone are the days when a three-ring binder, scientific calculator, and a some freshly sharpened no. 2 pencils were the most critical tools among a student's school supplies. Today – whether they're found in a grade school backpack or on the table of a college library – smartphones and tablets are number one on most back-to-school shopping lists. Businesses have seen myriad benefits follow the implementation of BYOD programs, including higher productivity of employees, increased happiness and general satisfaction of employees, and significant cost savings by eliminating the need to buy each and every employee specific equipment. With business-driven BYOD programs seeing A+ results, educational facilities are following suit. 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: 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, synching of email and difficulty accessing wireless networks are a small sample of the issues IT support may be inundated by with the adoption of BYOD.

WatchGuard

BYOD programs have many benefits, including **higher productivity** of employees, **increased happiness** and general satisfaction of employees, and **significant cost savings** by eliminating the need to buy each and every employee specific equipment.

Solutions:

MONDAY

BLOCK ILLEGITIMATE ACCESS WITH MFA ✓

To-Do

Because passwords can be compromised so easily, education institutions should implement MFA (multi-factor authentication) alongside any BYOD programs. WatchGuard's MFA solution AuthPoint is ideal for staff and students who bring in their own devices, with an easy-to-use app that enables authentication right from their own phone after a simple install and activation.

TUESDAY

IMPLEMENT SECURE WI-FI SOLUTIONS ✓

To-Do

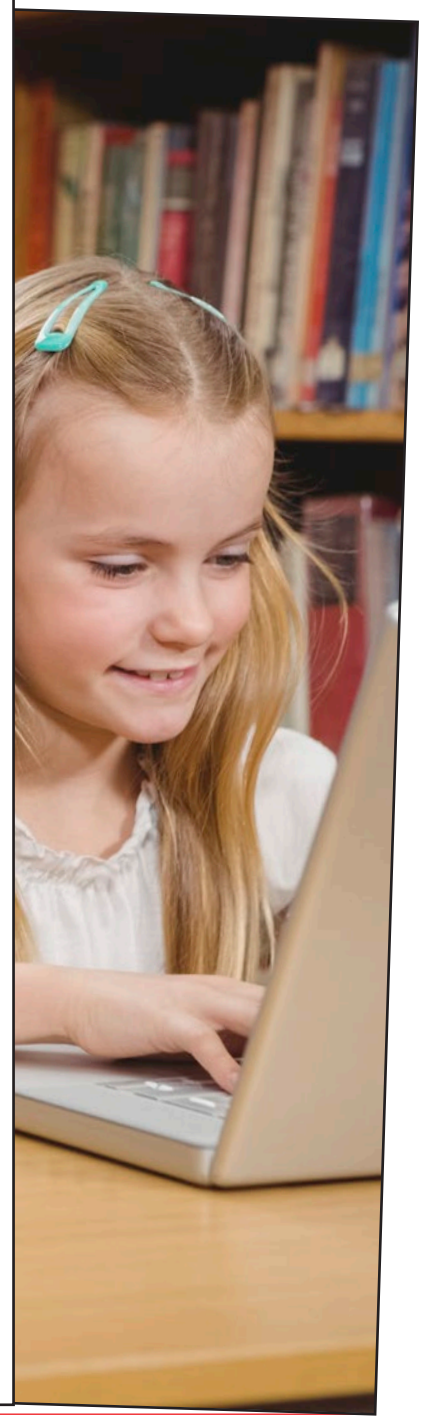
WatchGuard Cloud-Managed Access Points have been architected from the ground up to support ease of deployment and administration, simplifying even the most complex aspects of Wi-Fi management. Wi-Fi Cloud also offers Google for Education integration, working together with popular applications and services of Google for EDU to ensure that only authorized devices connect to the network. And now, with AP327X, WatchGuard brings the best Wi-Fi security and performance for faculty that require Wi-Fi outside, enabling a modern education experience.

WEDNESDAY

OUTSOURCE IT RESOURCES ✓

To-Do

BYOD, with all its myriad benefits, can also introduce resource challenges for your IT department; after all, your IT staff is greatly outnumbered by students and faculty. A managed security service provider (MSSP) 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.



KEY CHALLENGE:

Funding for Cyber Security

Educational institutions can't afford NOT to invest in network security. Though even small districts have multi-million dollar budgets, cyber security provisions are often limited, making schools an easy target. Cyber criminals 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.

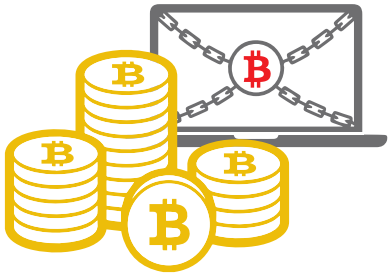
Recently, an entire US school district shut down for three days after hackers broke into multiple school servers and stole personal information on students and staff. Following the data breach, the hackers began sending text message threats to parents and promising to release students', teachers' and school administrators' personal information unless a ransom ($150,000 in bitcoin) was paid. The disruption affected more than 30 schools across the district.

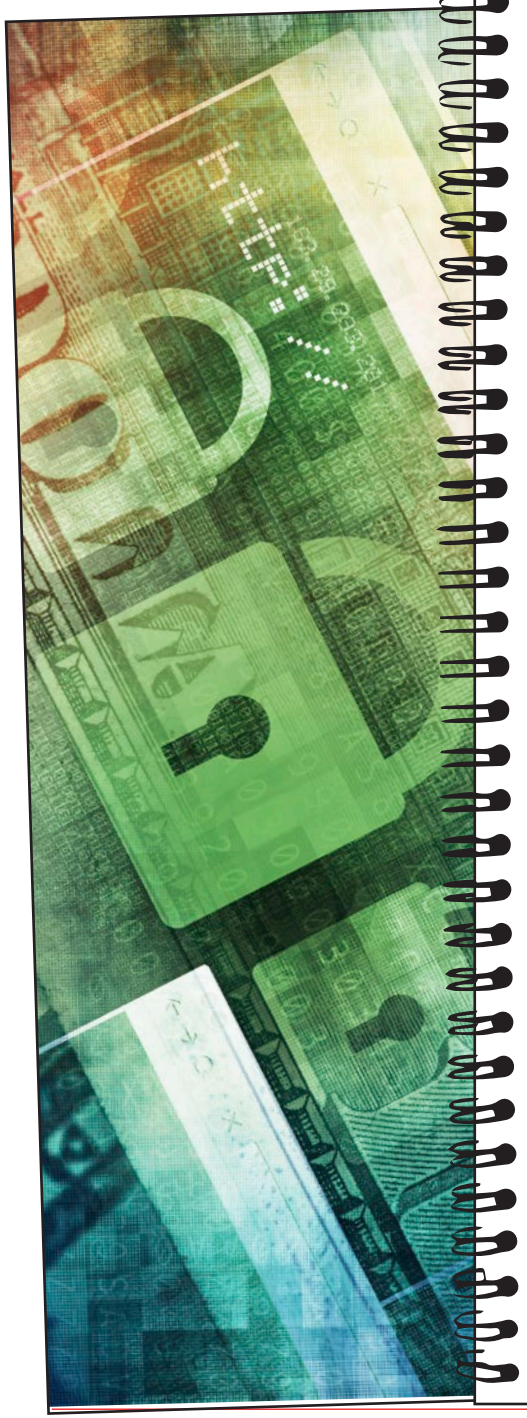
The implications of such attacks on schools can be considerable, resulting in major financial losses, stolen data, hardware rendered useless and educational institutions faced with prosecution or even lawsuits. In many cases, schools have been forced to turn students away while they work to resolve the issue and bring their systems back online. The Department of Education has stated that cyber criminals are likely targeting districts "with weak data security, or well-known vulnerabilities that enable the attackers to gain access to sensitive data."

The good news is that these attacks can be mitigated and their effects greatly diminished with a dedicated cyber security front, for which schools have numerous funding opportunities available to them.

WatchGuard

A US school district was hacked, and the hackers threatened to release the **personal information** of students, teachers and school administrators unless a ransom of **$150,000 in bitcoin** was paid.





Solutions:

MONDAY

E-RATE ✔

To-Do

Many schools take advantage of the E-Rate program in the United States to purchase technology at a discount, making it more affordable to provide a safe learning environment. WatchGuard products and services are eligible under the FCC's E-Rate program – it's the best way to save your budget dollars and secure your network with WatchGuard's enterprise-grade solutions.

TUESDAY

GRANTS ✔

To-Do

As with other needs that may not be addressed in the regular school or district budget, grants offer a chance to fund cyber security projects. A good first stop for cyber security grants is to visit government-regulated websites – such as grants.gov, which offers an extensive collection of grant opportunities. One such example, the Training-Based Workforce Development for Advanced Cyberinfrastructure opportunity, is specifically for developing school cyber security, and can pay for the technology needed to implement cyber security.

WEDNESDAY

PTA FUNDRAISING ✔

To-Do

PTA fundraising has come a long way since the days of selling wrapping paper and candy. Though classic methods like those are still viable options, online fundraising is a great alternative or supplemental method. Online fundraising sites make it easy to start a campaign for, manage, and accept funds to support an institution's cyber security goals.

KEY CHALLENGE:

Keeping Pace with Evolving Resources

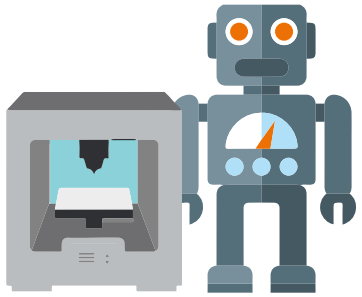
New EdTech (educational technology) is emerging every day, enabling both more engaged students and more effective teaching methods. In particular, the last few years have seen significant strides in science, technology, engineering and mathematics (STEM) learning – from the Computer Science for All initiative to the launch of new AP courses and online resources like Minecraft: Education Edition.

Makerspaces – collaborative spaces that utilize hands-on learning through building and design – continue to be an important tool in bringing STEM-related technology to the classroom. With makerspaces, (also known as "MakerLabs") there is no template or design to follow – districts have implemented technology of all kinds, from 3D printers to cardboard robots, and many educators believe that creative and engaging resources like these motivate students more than any pizza party ever could.

Not to be confined to designated areas, innovation in EdTech is moving out of makerspaces and into regular classrooms, with some English and language arts educators turning to STEM tools like robots to help students with critical thinking and empathy toward characters they're reading about. Smartboards have become wildly popular for schoolroom settings, marrying digital technology with a classic whiteboard format, and enabling the user to project computer images onto the board: this is the dry-erase board for the 21st century and beyond. Though certainly exciting, EdTech's ever-expanding reach introduces significant challenges, not least around network overload and user management.

WatchGuard

Makerspaces (or "MakerLabs") have a wide variety of technology, including **3D printers and cardboard robots**, to motivate students.



Solutions:

MONDAY

NETWORK SEGMENTATION ✓

To-Do

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.

TUESDAY

WIRELESS SITE SURVEY ✓

To-Do

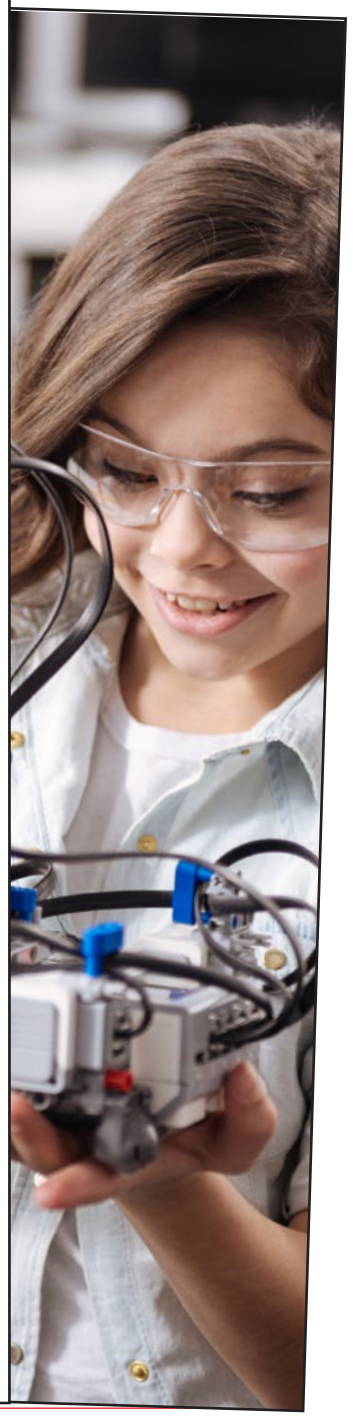
Wireless downtime can wreak havoc on your student's learning experience and be equally as frustrating for teachers and staff. Designed with the help of a WatchGuard-certified partner, a WatchGuard wireless site survey can help ensure your school has adequate, safe coverage for all authorized wireless devices.

WEDNESDAY

APPLICATION FILTERING ✓

To-Do

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 and when they can see it online. WatchGuard Application Control tightens security across your network and adds productivity safeguards, enabling administrators to monitor and control access to the Internet.



Managing the network infrastructure for any organization is hardly an "easy A," and educational institutions are certainly no exception. But with WatchGuard solutions that address the critical network challenges they face today, educational institutions get – and keep – high marks in security.

Global Headquarters
United States
Tel: +1.800.734.9905
Email: sales@watchguard.com

European Headquarters
The Netherlands
Tel: +31(0)70.711.20.85
Email: sales-benelux@watchguard.com

APAC & SEA Headquarters
Singapore
Tel: +65.6536.7717
Email: inquiry.sea@watchguard.com

WatchGuard