WHITE PAPER

A SECURITY ROADMAP FOR EDUCATION: How to protect students, educators and systems

SECURITY BREACHES HAVE BECOME A PART OF EVERYDAY LIFE FOR PUBLIC SECTOR ORGANIZATIONS, as cyberattackers continuously change their tactics to target systems and gain access to data. Schools are not immune to this disturbing trend: For years, K-12 institutions have increasingly relied on technology tools for everything from teaching and learning to communications, administration, and operations. These days, the COVID-19 crisis has also forced districts across the country to transition to cloud-based remote learning platforms and off-site devices, creating additional technology challenges.

As a result of this transformation, schools are at a greater risk for cybersecurity incidents than ever. According to EdTech Strategies' *K-12 Cybersecurity: 2019 Year in Review*,[1] the frequency and severity of school cybersecurity incidents increased significantly over the past year: During 2019, the report cataloged 348 publicly disclosed school incidents, including: student and staff data breaches; ransomware and other malware outbreaks; phishing attacks and other social engineering scams; and denial-of-service attacks. This is nearly three times as many incidents as were publicly disclosed during 2018.

verizon✓

SPONSORED CONTENT
IDG

The attacks, ranging from personal information theft and ransomware strikes to financial fraud, can lead to striking impacts including downed systems, data loss, and the sale of student information on the dark web. Student data was included in more than 60% of K-12 data breaches in 2018, and 46% of all K-12 digital data breaches included data (such as payroll or other personnel records) about current and former school staff.[2]

The question is, what can school administrators and IT officials do to mitigate or reduce those risks? The key is to take a high-level, holistic view in order to assess a school's cybersecurity needs and develop a roadmap that includes critical steps to protect students, educators, and systems, says David Grady, manager of security marketing and chief security evangelist at Verizon.

"It can be very challenging to wrap your arms around all the devices and technology the school has in place, particularly if someone comes in new or the school system is looking to make a big transformation," he says. "To maintain that high-level view, it's important to take a step back and understand the most likely things that could happen to you from a cybersecurity and cybercrime perspective."

Tackling Security Challenges in K-12 Education

The rate of technology adoption by K-12 schools in the U.S. has been on a steep, upward climb. The number of students with access to broadband at school grew from a mere 4 million in 2013 to 46.3 million in 2019.[3] Millions of mobile devices have been purchased for student and teacher use.[4] Meanwhile infrastructure operations are also going digital with Internet of Things, VoIP phones, cafeteria POS systems, HVAC and lighting controls with IP networks, online portals for HR, and much more. Not to mention the lack of a coherent security scheme for disparate devices.

With this rise in technology use, comes a rise in risk exposure. Over the past year, bad actors have targeted schools for personally identifiable information or to knock systems offline with DDOS attacks. Not all the threats come from the outside through malware, ransomware and the like. According to Verizon's 2020 Data Breach Investigations Report, while 67% of threat actors are external, human error by staff, parents or students is at the heart of more than a third of security breaches in K-12 public schools.[5] These miscellaneous examples often result from poor security hygiene including misdirected emails, sending files to the wrong people, or insufficient password protection. Web application attacks comprise around a quarter of breaches in the education vertical, mostly due to compromised cloud-based email services with phishing links to phony pages.

DURING 2019, **THE REPORT CATALOGED 348 PUBLICLY DISCLOSED SCHOOL INCIDENTS**, INCLUDING: STUDENT AND STAFF DATA BREACHES; RANSOMWARE AND OTHER MALWARE OUTBREAKS; PHISHING ATTACKS AND OTHER SOCIAL ENGINEERING SCAMS; AND DENIAL-OF-SERVICE ATTACKS.

Another challenge facing IT and security leaders is that many school cybersecurity systems are outdated, with large investments in legacy systems and policies that are no longer up to the task. No longer can a school's security focus be simply on the perimeter — that is, keeping the "walls of the castle" strong. In an age of cloud and mobile applications, there is no perimeter. This means that tools schools bought five years ago to manage antivirus or other elements of security are no longer how students, teachers, and other education stakeholders connect to the network, access data, store data, and move data around.

Meanwhile, remote learning creates a different kind of challenge for security leaders, says Grady. "There is no longer the same direct visibility into the activity between different users as there was when people were working on-premises and using school-supported tools," he says. "Now, security leaders need to work closely with IT to examine data access, availability, and confidentiality."

Priorities will depend on what level of service the school is trying to maintain for teachers, students, and parents, he explains. Is there a platform where students learn? Is it Google Classroom, or a portal that is maintained? Is there sensitive, private information being shared through email? If the school relies on cloud services such as Office 365, is there the right security in place to make sure the data going from the school and the network to the cloud and out to the end users is actually safe?

A Roadmap for Successful Cybersecurity in K-12 Schools

With so much at stake, from student safety to expensive breaches, developing a cybersecurity roadmap that leads to an improved security posture is essential. The primary goals of any good roadmap are to:

- Identify the biggest cybersecurity risks
- Reduce vulnerabilities to systems and critical infrastructure across systems
- Mitigate consequences if and when incidents do occur
- Strengthen security and ensure the resilience of the system

An excellent benchmark for planning a roadmap is the NIST (National Institute of Standards and Technology) Cybersecurity Framework.[6] It includes these five essential security steps organizations, including schools, should take to make sure they understand where they are today, where they need to go to meet their goals, and what plan needs to be put in place to get there:

1. **Conduct an assessment to identify managed assets and policies.**
   The first step is to identify how big a threat landscape needs to be protected and what critical business processes IT supports. The more you understand the risks your school faces, the better-positioned the organization will be to handle a potential breach. This begins with a security assessment that includes identifying managed assets and policies currently in place.

   For example, there may be Chromebooks given to students, desktop computers in labs, mobile phones given to teachers, internet connections, payment systems, and VoIP phone systems. Schools need to assess where data is, what kind of data it is (personally identifiable information? health information?), where it is stored, and how access is controlled. By conducting this initial assessment, schools can begin to understand where data flows through the organization and identify security gaps. They can also identify the legal and regulatory requirements related to cybersecurity, such as PCI compliance with payment systems or the Family Educational Rights and Privacy Act (FERPA), which requires the use of "reasonable methods" to safeguard student records.[7]

2. **Plan and prepare a program of protection for cybersecurity incidents.**
   Planning is crucial when developing an effective response to any cybersecurity incident, to make sure appropriate safeguards are in place to contain the impact and ensure critical infrastructure services can be delivered. Once assets are identified, the school can build out a program to address the biggest risks, such as phishing, web application attacks, and internal human errors due to poor security hygiene.

   These planning efforts may include protections for identity management and access control, including physical and remote access; user training for personnel; establishing and maintaining security policies, processes and procedures for critical data and systems; careful maintenance; and managing protective technology to ensure system security and resilience.[8]

3. **Leverage resources to implement incident detection tools.**
   Assessment and planning are important preparations, but the best response efforts include detecting and classifying incidents in as timely a way and as early in the process as possible. The problem is, the continuous monitoring detection tools required to provide awareness of anomalous events tend to be labor-intensive and expensive, which may be too big a spend for a school's small IT budget.

   However, schools may be part of a larger community of networks such as a bigger municipality or county/regional IT infrastructure. Perhaps those entities have resources that can be leveraged.

4. **Develop responses to contain cybersecurity threats and minimize damage.**
   What actions will be taken once a cybersecurity incident is detected? The good news is, there are coordinated response plans and activities schools can put in place in advance to make sure their response to a detected threat is timely and effective.

   These include making sure previously created response procedures are followed; that there is proper communication to ensure that internal and external stakeholders understand their response roles; that data is shared with stakeholders to encourage a consistent response; and that policies are implemented to contain the incident and prevent it from spreading.[9]

THERE ARE **COORDINATED RESPONSE PLANS AND ACTIVITIES SCHOOLS CAN PUT IN PLACE** IN ADVANCE TO MAKE SURE THEIR RESPONSE TO A DETECTED THREAT IS TIMELY AND EFFECTIVE.

5. **Identify how you will maintain resilience and restore capabilities and functions.**
Finally, no security roadmap is complete without a focus on recovering and restoring normal operations, as well as maintaining future resilience. A recovery plan should include restoring any systems or platforms affected by the incident, in as timely a manner as possible — as well as noting lessons learned from the incident and coordinating efforts with internal and external stakeholders.

There is no doubt this is easier said than done — according to the 2019 Verizon Incident Preparedness and Response Report, less than half (45%) of those with assessed incident response plans had fully specified recovery measures in place.[10] But schools that embark on the journey of a cybersecurity roadmap should prioritize their focus on recovery, to make sure that they can recover from an attack swiftly and with renewed strength.

A Security Roadmap Protects Public School Data and Privacy

Every K-12 school needs to protect its data and privacy as cyber threats and incidents continue to increase throughout public school systems. It is clear that security teams, IT leaders, and administrators must come together to formulate a holistic security strategy that deals with hardware, networks, applications, data, endpoints, and cloud. A step-by-step approach guided by a security roadmap can help protect data and privacy in all of these areas, for all stakeholders.

In education, many breaches are a result of poor security hygiene and a lack of attention to detail, so schools should particularly focus on reducing human error and then establishing a baseline level of security (that includes two-factor authentication) around internet-facing assets such as web servers. But that is only one part of a larger transformational journey that IT decision-makers need to take as they try to stay one step ahead of cyber thieves that try to get access to private student information and other school data.

"Everybody in the community of the school — from IT staff, to school leaders and teachers, to students and parents — needs to recognize that they play a role in building and implementing an effective cybersecurity program; it's not somebody else's job," says Grady. "That's where the right roadmap, used by all stakeholders, can help set schools on a path to security success."

CLICK HERE FOR MORE INFORMATION FROM VERIZON

CLICK HERE TO REQUEST MORE INFORMATION FROM AN EXPERT.

[1] "K-12 Cybersecurity: 2019 Year in Review"
[2] https://edtechmagazine.com/k12/article/2019/10/cybersecurity-threats-keep-k-12-cios-night
[3] https://s3-us-west-1.amazonaws.com/esh-sots-pdfs/2019%20State%20of%20the%20States.pdf
[4] "Global Demand for Mobile Computing Devices in K-12 Grows, Powered by U.S. Market"
[5] Verizon's 2020 Data Breach Investigations Report (DBIR)
[6] https://www.nist.gov/cyberframework
[7] https://studentprivacy.ed.gov/Security
[8] https://www.nist.gov/cyberframework/online-learning/five-functions
[9] https://www.nist.gov/cyberframework/online-learning/five-functions
[10] https://enterprise.verizon.com/resources/reports/vipr/vipr-exec-summary.pdf