CENTER FOR DIGITAL EDUCATION SPECIAL REPORT

PROTECTING STUDENTS & THEIR DATA

K-12 and higher education leaders need a comprehensive approach that outlines the latest policies, practices and technologies for physical safety and cybersecurity.

EMERGENCY MANAGEMENT
CENTER FOR DIGITAL EDUCATION

TABLE OF CONTENTS

INTRODUCTION

The primary role of educators — and the reasons why talented people enter the profession in the first place — is to teach, inspire and prepare students for life outside of classrooms. But the reality today is that educators must dedicate themselves to more than just education. Threats against our nation's schools are growing more numerous, sophisticated and serious. Leaders in school districts and on campuses must protect students and staff from physical incidents, while also guarding storehouses of digital data and IT systems.

Balancing these factors appears to become more challenging with the start of each new semester.

- A recent rise of violent acts on campuses threatens the physical security of students, faculty and staff. In the 2017-2018 school year, there were 279 incidents of violence, compared to 131 events in the 2016-2017 school year — an increase of 113 percent, according to the Educator's School Safety Network.[1]

- Weather is less predictable, bringing a higher likelihood of flood, fire and other natural disasters. In 2017, hurricanes Irma and Harvey led to school closures at six of the country's largest school districts, keeping 1.7 million K-12 students from attending classes.[2] This year, Hurricane Florence forced K-12 and higher education institutions to cancel classes on the Eastern Seaboard, including in the Carolinas and Virginia.

- Cybersecurity threats continue to increase in number and sophistication as cybercriminals find new avenues to exploit personally identifiable information (PII) and other sensitive data. There have been more than 375 cybersecurity incidents at

63%

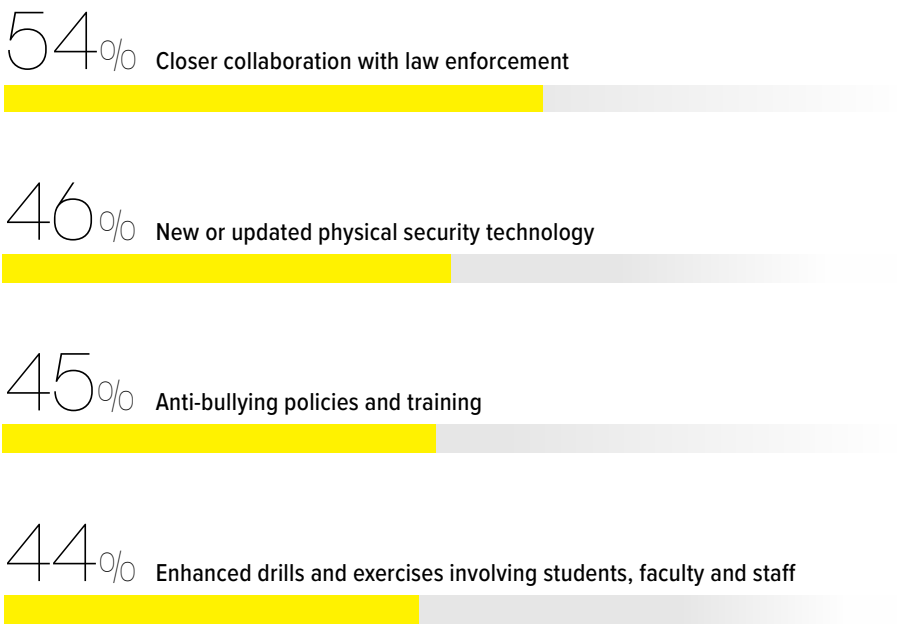
of K-12 school districts and

67%

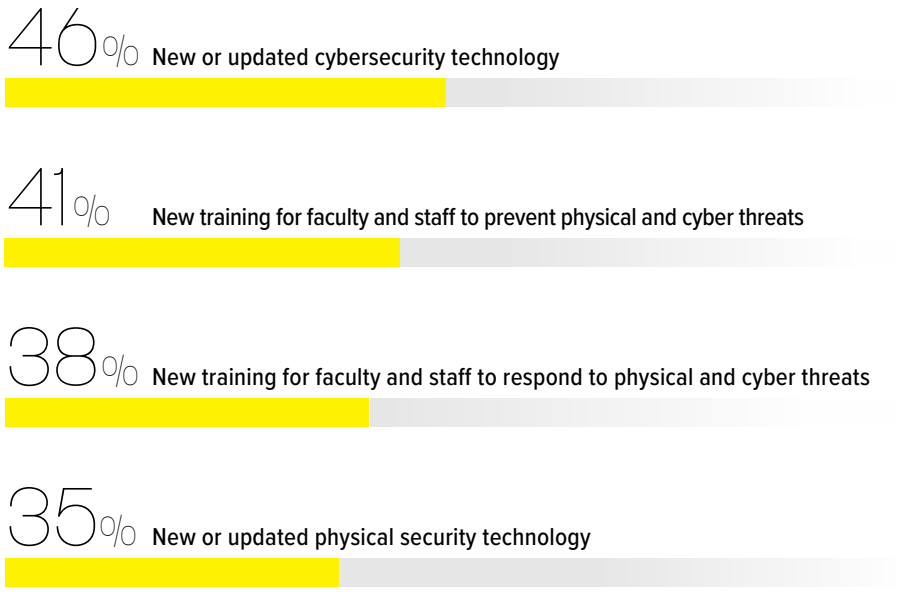
of higher education institutions say direct experience and news reports about physical and cybersecurity events have prompted them to significantly update security practices.

SECURITY PRIORITIES FOR K-12 AND HIGHER EDUCATION

K-12



HIGHER EDUCATION



Source: CDE September 2018 Survey

K-12 public schools since January 2016, according to a tally by EdTech Strategies.[3] Doug Levin, president of the consulting firm, says he thinks his count underreports the scope of the security troubles.

Because of these threats, K-12 and higher education officials are stepping up their security efforts. Sixty-three percent of K-12 school districts and 67 percent of higher education institutions say direct experience and news reports about physical and cybersecurity events at schools have prompted them to significantly update security practices for the current academic year, according to a September 2018 Center for Digital Education (CDE) survey of 177 administrators and faculty staff, conducted for this report.[4]

Where exactly did K-12 and higher education officials focus these efforts? The answers show differing priorities between the two groups of educators (see "Security Priorities for K-12 and Higher Education" on the left). K-12 institutions are focusing on physical security and anti-bullying measures, while higher education officials are giving cybersecurity more attention. Both segments value increased training and drills.

Having a clear set of priorities is important, but that's only a start. K-12 and higher education organizations also need a comprehensive plan to achieve their mission of educating students, while also addressing physical and cybersecurity threats and budget realities. This special report from the Center for Digital Education outlines policies, practices and technologies that K-12 and higher education leaders can implement to ensure their students, faculty and staff are safe and their data and systems are secure.

Balance Security and Open Culture with Identity

While information security has become the top concern for higher education IT professionals, it is not their only priority. In fact, data protection remains juxtaposed with ensuring an open, collaborative culture and optimizing information access. There are reasons why this is such a challenge for colleges and universities.

Dynamic User Population and Needs: In higher education, IT administrators and data stewards must provide timely provisioning and deprovisioning for thousands of diverse users.

Regulatory Compliance: Because educational institutions manage sensitive data, they must comply with a host of regulations, including the Health Insurance Portability and Accountability Act (HIPAA), the Family Educational Rights and Privacy Act (FERPA), the General Data Protection Regulation (GDPR) and more.

Budget Scarcity: According to a recent study by The Tambellini Group, 69 percent of senior IT professionals allocate no more than 1/10th of their IT budget to cybersecurity.

Heterogeneous Applications: Within any educational institution, there is an array of applications deployed for a myriad of users and requirements. This diversity makes it challenging for IT to securely govern access to these applications.

SailPoint Identity Brings Balance to the Educational Universe

SailPoint's identity governance platforms are designed to balance the need for security with efficient, responsive and timely access to information to support an open and collaborative culture.

Improve Access Workflow: Enable self-service access, automated provisioning and deprovisioning, and password sync to drive efficiency and improve access workflow for thousands of students, faculty, staff and other users.

Mitigate Risk: Ensure users have the right access (based on their roles) to the right systems, applications and data files, whether the resource is in the cloud or on-premises.

Improve Compliance: Meet compliance demands through streamlined, business-friendly access reviews, and automate policy management to boost security through consistent policy enforcement. Also, demonstrate compliance through audit-trail logging and reporting.

Minimize Complexities: Reduce risk of inconsistent access governance for users that may have multiple personas or roles per identity through best practice approaches. Enable user-friendly, self-service access requests and password resets to reduce workloads and simplify time-consuming tasks.

SailPoint

Recognized by Gartner, Forrester and KuppingerCole as the leading authority in identity governance, SailPoint can help educational institutions properly leverage identity to balance security with an open collaborative culture. Contact SailPoint to learn more. **https://slpnt.co/2ORa0gA**

THE THREAT LANDSCAPE

School safety is multifaceted, touching on a range of physical and cyber risks, so it's best to consider the unique characteristics of each area. For example, discussions about physical threats often focus on a sobering series of violent events that have rightfully drawn widespread attention in recent years. But many types of non-fatal acts, ranging from physical altercations to bullying, can also severely wound victims and undermine the core mission of educators. According to the Centers for Disease Control and Prevention's (CDC) Youth Risk Behavior Survey, nearly eight percent of students had been in a physical fight on school property one or more times during the 12 months before the survey.[5]

Despite national attention and formal programs instituted by educational institutions, bullying continues to plague schools. According to the CDC, in 2015, about 21 percent of students ages 12 to 18 reported being bullied at school during the school year. The digital era expands opportunities for this pernicious behavior.

"Cyberbullying has been increasing because of the many ways elementary, high school and college students can communicate today," says Marc Meyer, chief marketing officer with the Digital Futures Initiative, which offers resources to address cyberbullying.

Schools not only need to worry about threats to students, but also threats to their digital data and systems.

CYBERCRIME ON THE RISE

The challenges that K-12 districts and college campuses face when securing digital resources mirror the problems encountered by government, commercial industry and individuals.

For example, some of the biggest and most tech-savvy commercial organizations also suffered disruptive exploits in recent years.

- ☑ The credit-reporting agency Equifax revealed in 2017 that hackers accessed financial data in more than 145 million accounts.[6]
- ☑ The ride-sharing company Uber reported in late 2017 that 57 million customers and drivers had personal information purloined by cyberthieves. The company reportedly paid a $100,000 ransom to keep the information from being made public.[7]
- ☑ Even the nation's National Security Administration (NSA) isn't immune to hackers. Nation-state attackers used stolen NSA cyber-weapons to fuel a global ransomware outbreak in 2017.[8]

Education-related incidents mirror the rise of exploits in commercial industry, and there are signs that hackers are singling out schools — and have been for some time. Between 2005 and 2016, higher education institutions were the victim of 539 breaches involving 13 million known records.[9] More recently, according to the September CDE survey, 18 percent of K-12 schools and 29 percent of higher education institutions suffered a data-loss breach or ransomware disruption during the 2017-2018 school year.

Why are hackers focusing on education? The end game isn't a surprise.

"The bottom line is the bottom line," says Sean Wiese, chief information security officer (CISO) for the state of North Dakota. "They're looking to make money through ransomware or confiscate personal information, such as financial data they can use or sell to others."

18%

of K-12 schools and

29%

of higher education institutions suffered a data-loss breach or ransomware disruption during the 2017-2018 school year.

What sets education apart from other sectors are resource constraints, which lead hackers to think of these institutions as soft targets.

"In many K-12 schools, it may be a math teacher who is acting as the IT administrator on the side," Wiese says.

North Dakota came face-to-face with the problem in February when one-third of its K-12 schools were hit by DoublePulsar, malware that evolved from the leaked NSA tools. Fortunately, quick identification and help from the state's cybersecurity staff addressed the exploit before any data was lost, Wiese says.

Ransomware remains a significant threat to schools, even though the overall number of ransomware attacks has fallen since the 2017 peak when the global WannaCry outbreak infected a range of industries. For example, reports of ransomware dropped 20 percent in the first half of 2018 compared to the previous year.[10]

But ransomware problems continue. Leominster Public Schools in Massachusetts learned this lesson the hard way in April 2018 when hackers disrupted the district's IT resources and demanded $10,000 in bitcoin to recover the systems.[11] According to a press report, the school didn't have a comprehensive backup strategy in place to wipe the infected computers and return to normal IT operations. As a result, city officials acquiesced and paid the ransom.

Ransomware attacks are just one of many types of cybercrimes that schools must guard against. Identity theft also deserves close attention. According to a report by Carnegie Mellon University's CyLab, the rate of identity theft for children is 51 times higher than that of adults.[12] This means institutions charged with protecting student data are high-value targets. A recent report found education data breaches doubled in the first half of 2017 (compared to the last half of 2016), with education institutions experiencing 118 successful attacks.[13]

Cybersecurity experts say "crypto-mining" is another insidious trend hitting schools. Cybercriminals infect IT systems with stealthy malware that quietly uses the processing power of the institution's on-premises IT systems and cloud servers to run computationally demanding algorithms that verify bitcoins and other crypto-currencies. In return, the digital miners receive payments for each transaction they help process from the currency networks. Months may go by before school officials realize the digital parasites are feeding off school resources. In the meantime, schools can't access all the processing power they have paid for, and they unwittingly help cybercriminals stay in business. One cybersecurity company estimates that crypto-mining incidents rose 8,500 percent in 2017.[14]

One cybersecurity company estimates that crypto-mining incidents rose

8,500%

in 2017.

Of course, hackers continue to use a variety of tried-and-true exploits along with these more recent threats to breach K-12 and higher education networks. These include phishing and spear-phishing attacks that employ clever tactics to trick people to click. One avenue of attack is exploiting students with aid packages.

"Criminals send emails to students purportedly from legitimate lending organizations or federal grant programs," says Dr. Mary Ann Hoppa, associate professor at Norfolk State University and co-principle investigator at the school's Cybersecurity Center of Excellence. "The attackers try to obtain personal information by saying they need to check student credentials."

Unfortunately, outside hackers aren't the only threats schools must guard against. During the 2017-2018 academic year, 10 states acknowledged that young people hacked into student information systems (SISs) and other platforms, usually to alter grades.[15] Industry observers note the exploits began with stolen passwords and login information, highlighting the need for basic security best practices, such as requiring faculty and staff to regularly change their passwords.

// Ransomware remains a significant threat. In April 2018, hackers disrupted the IT resources of Leominster Public Schools in Massachusetts and demanded $10,000 in bitcoin to recover the systems.

Maximize K-20 Security with an End-to-End Solution

The combination of endpoint, network and physical security provides Reading School District and Illinois College with a powerful, end-to-end security solution that keeps students and educators safe.

IT teams at K-12 schools and higher education institutions are tasked with keeping the network secure, from guarding against sophisticated cyber threats to blocking harmful content and protecting student data privacy. At the same time, they must protect end-user devices and ensure the physical safety of students and staff. Accomplishing all of this is challenging, especially when IT teams must manage numerous solutions across multiple vendors with limited resources. How do you protect endpoints, networks and students, all at the same time?

Reading School District in southeastern Pennsylvania is committed to providing reliable wireless, securing endpoints, keeping data protected and ensuring the physical safety of students and teachers. But using a different vendor for wireless, switching and security, with no centralized management, led to a complex IT environment. To combat this challenge, district leaders deployed an end-to end cloud-managed security solution, allowing the IT team to block harmful content on student devices, stop malicious files and viruses, and mitigate physical security threats with high-quality video footage and easy search capabilities — all from the same web-based dashboard.

Illinois College realized it could not continue to manage its complex networking infrastructure with its small staff and limited budgets, while also protecting students and devices. By deploying endpoint management, security appliances and smart security cameras, the IT team can keep students and faculty safer across campus. With built-in malware protection, automatic firmware upgrades and content filtering, the number of students with viruses on their computers has drastically decreased. Plus, with motion search and motion alert features on security cameras, the IT team can quickly identify security incidents and respond accordingly.

The combination of endpoint, network and physical security provides Reading School District and Illinois College with a powerful, end-to-end security solution that helps keep students and educators safe. By managing all security solutions from a single, web-based dashboard, schools can make remote configurations, view video footage and deploy applications from anywhere, in just a couple of clicks. Meraki keeps devices protected, data encrypted and students safe, while enabling the IT department to spend more time on impactful projects and less time managing and troubleshooting security solutions.

To find out more about how you can simplify and secure your K-20 environment, visit: www.meraki.com/edusecurity

cisco Meraki

REGULATIONS, COMPLIANCE AND GRANT REQUIREMENTS: WHAT YOU NEED TO KNOW

Instructors at Norfolk State University recently got a lesson in the challenges of meeting federal regulations designed to protect student information. A re-reading of the Family Educational Rights and Privacy Act (FERPA) led the university's legal staff to ban broadcast emails that list the addresses of multiple students.

"Professors can't reveal student email addresses when we send a message to the entire class or to create small workgroups," says Hoppa. "We all understand why it's important to safeguard student information, but the pendulum is swinging to an extreme. Not only are we not allowed to share information with parents or others outside the university, we're no longer able to share contact information among the students themselves."

Of course, FERPA is just one law with which K-12 and college officials must comply. The list also includes the Protection of Pupil Rights Amendment (PPRA), the Children's Online Privacy Protection Act (COPPA), the Children's Internet Protection Act (CIPA), the Education Sciences Reform Act (ESRA) and more. In fact, The Future of Privacy Forum estimates that states have instituted 125 new student privacy rules over the past five years.[16]

The volume of laws isn't the only challenge. School faculty and staff also grapple with sometimes conflicting requirements within various regulations.

"One regulation may require schools to retain data for 'X' amount of time, while it's 'X minus 2' for another one," says Hoppa. "Those differences can make compliance time consuming and prone to error. Adding to the challenge is the tediousness of having to go through all of the regulatory audits."

Security gaps only intensify the difficulties. For example, if hackers breach a school network and steal student information, the institution faces stiff penalties if any of that data is made public. An Iowa school system faced this issue in late 2017 when the group Dark Overlord published student names and contact information online.[17]

THE PAIN OF NON-COMPLIANCE

Lack of compliance may carry significant financial consequences. For example, when schools fail to meet FERPA rules, they jeopardize their ability to obtain federal grants and other financial resources.

Organizations may also face legal consequences. A report by the Consortium for School Networking (CoSN), a professional association for school technology officials, concludes that schools may be liable for problems stemming from network breaches.[18]

"The costs of these incidents can be extremely high and can include the cost of determining the cause, the cost of preventing future breaches, the cost of legal counsel, the cost of public relations to regain trust and the cost of remediation," the report adds. "District tech leaders as individuals may be sued by families whose data was compromised by a security breach."

How can K-12 and higher education institutions protect sensitive data to remain in compliance with federal and state laws? To start, officials should follow the policies, practices and technology guidelines outlined in the section "Keeping Data and IT Systems Secure" on page 18. In addition, the U.S. Department of Education's Office of Student Financial Aid offers a list of tools that aid in regulatory compliance at https://ifap.ed.gov/eannouncements/Cyber.html.

MORE REGULATIONS?

Given the long list of existing rules, it may sound counter-intuitive to advocate for more requirements. But some observers see the need to expand the focus of the current laws.

"While regulators have given attention to student data, they've been relatively silent on the issue of security," says EdTech Strategies' Levin. "Privacy laws presume that schools are fulfilling their obligation to keep data from unauthorized persons. But I'm seeing mounting evidence that security is a challenge for schools, and they may need more specific guidance around cybersecurity practices. As we look to modernize our practices and privacy rules in schools, they need a clear set of standards against which they will be measured."

What Do You Want From **THE CLOUD?**

A Anytime, anywhere access to digital content. My students and staff have high expectations.

B Ease of maintenance. My IT staff is already stretched to the limit.

C Lower costs. I am (perpetually) short on capital for expensive IT investments.

D I need to roll out new applications quickly and scale up capacity when needed.

Why not: "All of the above?"

According to the Center for Digital Education's recent cloud survey, education leaders see these as the top four benefits of using cloud-based technologies.

Pure Storage helps education institutions reach these goals. Pure Storage provides flash storage solutions – a software-driven technology that is transforming IT operations through dramatic increases in performance and efficiency at lower costs. Whether you leverage all-flash for your private cloud or keep your solution on-premises, Pure Storage allows you to take advantage of everything to love about cloud – speed, reliability, and simplicity.

ANYTIME, ANYWHERE ACCESS TO CONTENT Pure Storage excels in virtualization scenarios, allowing schools to offer mobility and BYOD at scale without performance issues. All-flash enables seamless, ubiquitous access to digital learning.

EASE OF MAINTENANCE Pure Storage takes the headaches out of storage from the moment it comes out of the box. With the Evergreen™ Storage model, both controller hardware and software are non-disruptively upgraded with each three-year maintenance renewal. Say goodbye to forklift upgrades and the hassles that come with them.

LOWER COSTS With a low upfront price, flat annual maintenance fees and an investment that stays modern through Evergreen Storage, there is no better total cost of ownership in the storage industry. Low, predictable payments have finally arrived.

AGILITY Pure Storage allows you to grow capacity and performance where and when they are needed, with no downtime. With automatic resource provisioning, you can add more services whenever you need to.

Learn more about Pure Storage and the customers they've served in education: ***purestorage.com/education***

PURESTORAGE®


EMERGENCY
911

KEEPING PEOPLE SAFE

Given the recent rise in violent on-campus incidents, education officials are strengthening physical security using a variety of approaches.

Security professionals at the University of Virginia advocate approaching physical security as a public health issue. It starts with expanding efforts to create positive climates that help all students succeed in school, said Dewey Cornell, forensic clinical psychologist and professor of education at the university, in testimony on Capitol Hill last spring.[19]

Noting that incidents of mass violence in schools and communities often stem from bullying, harassment and discrimination experienced at school, Cornell told lawmakers that timely intervention is needed.

"Put an armed guard in a school and you might prevent one shooting in one building," he said. "Put a counselor or psychologist in a school and you have the potential to prevent shootings in any building anywhere in your community."

The university's Virginia Student Threat Assessment Guidelines (VSTAG) outline steps to identify and then intervene when students appear to be moving toward violence. The program is designed to not only assess individual students, but also reveal systemic problems at an institution, such as bullying, that require attention.

Researchers at the university say threat assessments yield significant safety-related benefits. They cite studies that compare middle schools that conducted VSTAG assessments with ones that hadn't. The conclusion: The number of years a school used the [guidelines] was associated with lower long-term suspension rates, lower levels of general victimization, higher student reports of fairer discipline and higher teacher perceptions of school safety.[20]

TECHNOLOGY FOR SAFER SCHOOLS

In the wake of numerous natural and human-initiated disasters, school officials are relying more heavily on technology to keep students and staff safe this year. When the September 2018 survey asked administrators about the various steps they've taken to enhance overall security practices, the leading response, at 41 percent, was added or enhanced physical security technology.

Where did schools focus their spending this year? Much of the money went to tried-and-true technology. Fifty-eight percent of survey respondents said they invested most heavily in video surveillance, followed closely at 55 percent by campus emergency alert systems that broadcast warnings about active shooters and other significant threats.

It's clear why officials value surveillance systems so highly. Real-time video feeds show security staff who's entering campuses and buildings throughout the day and night. Officials can immediately see suspicious and unauthorized visitors. Video records also help provide important forensic information after an event, which can bolster future security practices. The prominent display of video systems around campus may also reduce physical assaults and other criminal activity by deterring people who fear being apprehended.

Compared to this important but more traditional technology, respondents are giving a lower priority to some new digital tools, such as the Internet of Things (IoT) and artificial intelligence (AI). But that may change, given their impact on the security market. For example, Grand View Research called out integration of IoT as one of the factors fueling significant growth in physical security spending across industries through 2025.[21]

Platforms for IoT and AI contribute complementary capabilities for school safety. IoT connects

// Security professionals at the University of Virginia advocate approaching physical security as a public health issue.

hundreds or perhaps thousands of small, digital sensors installed across campuses to collect an array of data. Security officers can use IoT to monitor video feeds from wireless cameras or capture information scanned from identification cards as people access school facilities. But not all of these data points necessarily indicate a security threat. To guard against an impending risk getting lost in the flood of information, AI applies advanced pattern-matching techniques to alert security personnel to suspicious activity — on the campus itself or in social media conversations that discuss plans for a shooting, for example.

IoT and AI also provide the underpinnings of smart campuses by monitoring and automating facility resources. During non-emergencies, this includes keeping HVAC systems set at predetermined levels for optimum energy management and occupant comfort. But when a disaster is unfolding, smart campus infrastructure can be set to act. For example, the platform may automatically lock down certain areas based on the school's emergency response plan. In addition, a smart campus system could post warnings and emergency instructions on digital signage or turn up campus lighting to aid first responders.

THREATS THAT SPAN TWO WORLDS

Safe internet practices straddle the physical and cyber worlds, which means that safety strategies require special instruction. The Digital Futures Initiative's Meyer says schools and parents must educate students about internet dangers, such as human trafficking and threats from adults who lurk on sites frequented by young people.

"Students need to understand how adults may approach them and try to groom them as the next victim," he says. "The whole goal is to give kids a fighting chance to stay safe by ensuring they have a clue about what's out there before they fire up a phone, laptop or iPad."

Digital systems may also foster cyberbullying that preys on the natural desires of young people to validate themselves by comparing themselves with others.

"Those comparisons are now happening at hyper speed, among students who have a low emotional intelligence quotient because their brains aren't developed enough to handle this," Meyer says.

Parents may miss warning signs that reveal bullying, he adds.

"They take the stance that John is over there in the corner looking at his phone. I can see him, so everything must be fine. They have no idea what sites their child is on, what they're posting, saying, reading," Meyer says.

Adding to the challenge of stopping cyber-stalking and cyberbullying is the fact that today's students are digital natives, while many school officials and parents are digital immigrants who must simultaneously learn and teach internet best practices.

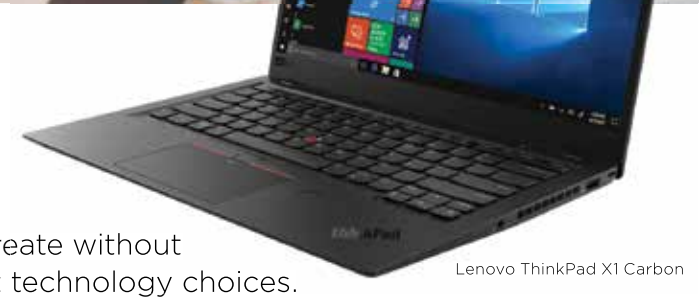
"Our approach is to impart onto students the idea of creating a balance between real and digital life," Meyer says. "At the same time, most adults need to be more vigilant. Look at what's on the phones of minors, look at what they're saying and what others are saying to them."

He advises school officials to investigate internet tools that monitor web activity, browser histories and conversations on social media sites. Resources like these can flag discussions that may require further investigation, such as ones that include talk of guns, drugs or other topics that may negatively impact school safety.

// Our approach is to impart onto students the idea of creating a balance between real and digital life. At the same time, most adults need to be more vigilant. Look at what's on the phones of minors, look at what they're saying and what others are saying to them.

Marc Meyer, Chief Marketing Officer, Digital Futures Initiative

Tomorrow Belongs to Risk-Takers.



Lenovo ThinkPad X1 Carbon

EMPOWER NEW IDEAS WHILE STAYING PROTECTED.

Users must be allowed to explore, collaborate and create without compromising security, and that starts with the right technology choices.

Lenovo™ is committed to mobile solutions that keep faculty and students productive and protected on and off campus. It starts with a security-first culture that inspires our ThinkPad® engineers to deliver unparalleled protection and privacy, from advanced encryption and authentication to meaningful features like built-in camera privacy shutters.

Delivered with a Windows 10 Pro experience that carefully balances user convenience and the most comprehensive information security, Lenovo gives higher education institutions technology that delivers secure collaboration and creativity on campus and beyond.

For more information about Lenovo and Windows 10 Pro products for education, please visit www.solutions.lenovo.com/higher-education.

Education

Lenovo™

Windows 10 Pro

Windows 10 Pro means business.

KEEPING DATA & IT SYSTEMS SECURE

School security staffs have more choices than ever when it comes to cybersecurity tools and services to protect student information and IT systems from hackers. But experts warn against the trap of thinking the latest and greatest security technology alone will keep institutions secure. Before making plans to update and expand security toolsets, officials should first redouble their efforts to ensure they have a comprehensive security strategy that incorporates effective policies and practices. This requires a spectrum of school officials.

"It is important for superintendents and school boards to not view cybersecurity as something that begins and ends with the IT department," says Levin. "These two groups should be engaged in discussions about risk management, including which risks they will accept, which ones they will manage through controls and policies, and which ones they'll insure against. It's also important these officials are part of conversations about incident response. The worst time to think about this issue is during a breach."

The need for comprehensive plans that give schools a strong cybersecurity foundation was highlighted last fall when the U.S. Department of Education issued an alert that spelled out an underlying vulnerability common to the victims of the ransomware attack that used NSA tools. The attackers targeted districts with weak data security or well-known vulnerabilities, according to the department.[22]

// Before making plans to update and expand security toolsets, officials should first redouble their efforts to ensure they have a comprehensive security strategy that incorporates effective policies and practices.

// In industry, we had basic cyber-hygiene drummed into our heads. For example, you don't walk away from your workstation without securing the keyboard. Those kinds of habits have not been ingrained in academia to the same extent.

Dr. Mary Ann Hoppa, Co-Principle Investigator, Cybersecurity Center of Excellence, Norfolk State University

Norfolk State University's Hoppa says she isn't surprised that some schools aren't adequately addressing cybersecurity fundamentals.

"When I compare my previous experience in industry to academia, I find the latter is a much more trusting environment," she says. "In industry, we had basic cyber-hygiene drummed into our heads. For example, you don't walk away from your workstation without securing the keyboard. Those kinds of habits have not been ingrained in academia to the same extent."

As a result, cybercriminals may consider academic institutions to be soft targets vulnerable to social engineering attacks and "scareware," the pop-ups that say a problem was detected on an individual's computer and that clicking on an accompanying link will start the process of fixing it. Unfortunately, by responding to a phantom problem, end users install malware that creates a real threat.

BEST PRACTICES FOR CYBERSECURITY

To fill cybersecurity gaps, schools should undergo an audit designed to reveal the strengths and flaws in the organization's current security posture. The goal is to do more than just bring anti-malware and security patches up to date or to scour network logs for unusual activity. An underlying framework should be in place to make certain that ongoing updates and reviews happen as quickly as possible. To do this, school officials can look to the federal government and commercial organizations for guidance.

"Some of the more mature schools in terms of cybersecurity have adopted one of several cybersecurity risk management frameworks," Levin says. "Frameworks help schools organize and manage their work, measure the results of these efforts, and then use this data to drive conversations about budget and investments with district leadership."

For example, the Center for Internet Security (CIS) offers a three-tier set of 20 steps that guide organizations from basic to foundational to organizational levels of cybersecurity.[23]

"I've seen the CIS Controls gain a lot of traction within education," Levin says.

In addition to having underlying processes in place for tighter security, schools should also ensure faculty, staff and students understand the latest threats and how to respond.

"Training, training, training — that's critical for guarding against breaches," says Marie Bjerede, the principal for leadership initiatives at CoSN. "Make sure everyone is trained and knows how to keep their passwords secure, how to recognize phishing attempts and to avoid clicking on suspicious Web links."

Some institutions use training sessions to condition people to assume all incoming email carries malware, no matter how legitimate it looks. They teach employees and students to study the body of the message for typos or awkward phrasing that may tip them off to a phishing scam. They also use anti-virus applications to scan attachments for viruses before opening them. Vendors of security software also offer tools that analyze Web links to determine their safety. Campus IT departments may launch simulated phishing attacks to test the security skills of end users and remind "victims" about email best practices.

Dovetailing with these training techniques are tabletop exercises that take participants through various data breach scenarios.

"These exercises give people practice and experience so they know how to respond in an actual emergency," Bjerede says.

Communications is a component of these activities so officials are prepared to speak with parents, the outside community, the press, law enforcement and others in the aftermath of an attack, she adds.

Consolidating IT resources is another effective, if ambitious, practice that can bolster security. For example, many large school districts and universities use separate IT staffs to manage IT in individual departments or facilities. These schools should consider the benefits of having a single IT department centrally manage and oversee IT operations and network traffic.

North Dakota is taking this approach with STAGEnet, a statewide network that provides broadband connections to the internet for K-12 schools, public colleges and universities, all government departments and the legislative and judicial branches, as well as cities and counties. Schools still manage their local IT operations; the statewide connection to the internet means each facility doesn't need to contract with local service providers. This enables the security staff within the state's Information Technology Department to monitor network activity and act quickly if it spots an emerging malware outbreak.

"Because all the traffic information funnels through us at the state IT department, we can watch it for signs of trouble and act on problems in a common way," CISO Wiese says. "That puts us in a better defense posture."

Centralization also helps the state optimize scarce public sector resources by eliminating duplicate security tools and staff, he adds.

The value of centralization for cybersecurity hit home last winter when the malware outbreak hit one-third of North Dakota's school districts.

"We could see a large spike in the volume of traffic — it was just off the charts," Wiese says. "That's because the malware was quickly scanning networks, trying to infect as many systems as possible."

Thanks to its consolidated overview of network activity, the state IT staff quickly identified the outbreak and recognized the patterns of behavior as those associated with DoublePulsar, the misappropriated NSA tool.

"We then worked with the people who handle security at individual schools and districts to contain the outbreak" Wiese says. "The trick was to identify all the systems that may have been infected by the malware, which could run the gamut from a workstation used by a teacher to an HVAC system."

While it took nearly 45 days for everyone to be satisfied the virus was fully eradicated, the ability to quickly see the outbreak and take corrective measures minimized the damage. Wiese says none of the schools lost data.

TECHNOLOGY FOR TIGHTER SECURITY

Once schools have a solid foundation in policies and practices, they'll be better equipped to evaluate how technology can secure their organizations. Start with table-stakes tools, such as systems for securing emails, the delivery mechanism for

43%

of K-12 districts and

66%

of colleges earmarked the highest percentages of current-year cybersecurity investments to secure email systems.

phishing and spear-phishing attacks. According to the CDE survey, 43 percent of K-12 districts and 66 percent of colleges and universities earmarked the highest percentages of current-year cybersecurity investments to secure email systems.

Closely aligned with this are anti-malware applications, which are becoming more sophisticated to keep pace with new assaults from resourceful hackers. Today's malware safeguards incorporate AI and machine learning algorithms that look for signs of unusual behavior in applications that may tip off an infection. This adds an extra dimension beyond traditional anti-virus software that tries to spot the digital fingerprints of known viruses, which hackers can easily disguise.

Firewall technology is also getting a makeover. Next-generation firewalls (NGFs) evaluate network traffic as it flows across on-premises and cloud communications links. They, too, try to spot unusual behavior that may signal the presence of hackers. If warning signs appear, NGFs can segment potentially problematic code to a test area that's walled-off from production systems, where it can be evaluated by the security staff.

"Technology can assist schools in managing logins and passwords for authenticating staff and students," Levin says. "These are areas of weakness that are routinely exploited by cybercriminals."

A couple of technologies do a very good job protecting log-in data. The first is enterprise-quality password managers that enforce unique passwords, and ensure people can access only the accounts they're authorized to view, and that accounts can easily be deprovisioned when someone leaves the district. The second highly effective tool is two-factor authentication, which requires users to provide a password as well as a time-based software token like a verification code or a physical token.

Reliable systems for backing up data and applications are another must-have for K-12 and higher education.

"Having an effective backup system in place means even if ransomware infects the network, schools can say, 'Forget about you, attacker. I'm just going to wipe out my system and restore everything from the backup,'" Wiese says. "The hacker has spent a lot of time and effort trying to break in, but he has wasted his time thanks to the backup."

Once schools have a core set of security tools in place, they can begin to evaluate advanced capabilities, such as using big data and machine learning to enhance their cyber-defenses. Access to large data sets and advanced analytical programs to sift through all the information provides another way for organizations to spot abnormal network activity. These insights help schools keep hackers from breaching systems and minimize the damage of any successful intrusions. Because machine learning algorithms automate much of the monitoring activity, internal security staffs aren't burdened with wading through reams of network data trying to spot potential problems.

The expense and complexity of big data and machine learning may prompt organizations to contract with outside service providers for these capabilities. However, some schools, such as Norfolk State University, are researching ways to incorporate these technologies within their on-campus operations. Norfolk's Cybersecurity Center of Excellence has already implemented specialized hardware and software to support this area. In addition to using the resource for Norfolk's security operations, officials are evaluating ways to offer it to others in higher education, as well as to the commonwealth of Virginia, Hoppa says. Meanwhile, graduate research assistants are designing interfaces with simple menus to make it easier for people to use.

"Big data and machine learning tools are fresh out of the laboratory, so a lot of configuration is still required," Hoppa says. "This can be burdensome for some organizations. We're creating a user-friendly layer to shield people from this complexity, so they can focus on finding answers to their questions."

A PATH TO THE FUTURE

Administrators and faculty in K-12 and higher education are closely attuned to growing threats to physical safety and cybersecurity. Research by CDE and others shows school officials are taking steps through new investments in technology and other areas to address these risks. But technology alone can't fully protect people and sensitive data from malicious activity. What's needed is a comprehensive strategy that merges modern security technology with the latest policies and practices tailored for physical and cyber safety.

Resources are limited, and officials will need to make tough choices about how to allocate staff time and funding. But with a multifaceted plan in place, educators can draw closer to the ultimate goal: creating learning environments that support positive student outcomes.

ENDNOTES

1. http://eschoolsafety.org/violence/
2. https://www.businessinsider.com/hurricane-irma-schools-closed-millions-no-education-2017-9
3. https://k12cybersecure.com/map
4. The Center for Digital Education surveyed 177 K-12 and higher education leaders in September 2018.
5. https://www.cdc.gov/violenceprevention/youthviolence/schoolviolence/data_stats.html
6. https://www.washingtonpost.com/news/the-switch/wp/2018/05/08/every-type-of-personal-data-equifax-lost-to-hackers-by-the-numbers/?noredirect=on&utm_term=.50f0a3b256f1
7. https://www.nytimes.com/2018/01/12/technology/uber-hacker-payment-100000.html
8. https://www.nytimes.com/2017/11/12/us/nsa-shadow-brokers.html
9. https://www.universitybusiness.com/article/0816-wisp
10. https://media.erepublic.com/document/GT18_HANDBOOK_Palo_Alto_V.pdf
11. https://www.cyberscoop.com/leominster-ransomware-massachusetts-bitcoin/
12. https://www.cylab.cmu.edu/_files/pdfs/reports/2011/child-identity-theft.pdf
13. https://thejournal.com/articles/2017/09/20/education-data-breaches-double-in-first-half-of-2017.aspx
14. https://www.symantec.com/blogs/threat-intelligence/istr-23-cyber-security-threat-landscape
15. https://www.edweek.org/ew/articles/2018/06/13/student-hackings-highlight-weak-k-12-cybersecurity.html
16. https://ferpasherpa.org/state-laws/
17. https://www.desmoinesregister.com/story/news/2017/10/06/iowa-governments-vulnerable-johnston-like-cyber-attacks/741025001/
18. https://cosn.org/sites/default/files/Superintendents%20Initiative%20-%20Cybersecurity_0.pdf
19. https://theconversation.com/threat-assessments-crucial-to-prevent-school-shootings-93636
20. https://curry.virginia.edu/sites/default/files/images/YVP/VSTAG%20summary%206-18-18.pdf
21. https://www.grandviewresearch.com/industry-analysis/physical-security-market
22. https://ifap.ed.gov/eannouncements/101617ALERTCyberAdvisoryNewTypeCyberExtortionThreat.html
23. https://www.cisecurity.org/controls/

PRODUCED BY:

CENTER FOR DIGITAL EDUCATION

The Center for Digital Education is a national research and advisory institute specializing in K-12 and higher education technology trends, policy and funding. The Center provides education and industry leaders with decision support and actionable insight to help effectively incorporate new technologies in the 21st century.
www.centerdigitaled.com

EMERGENCY MANAGEMENT

Emergency Management brings together leaders who drive the nation's prevention, protection, response and recovery operations.

Emergency Management is a division of e.Republic, the nation's only media and research company focused exclusively on state and local government and education.
www.emergencymgmt.com

SPONSORED BY:

cisco Meraki

Lenovo Education

PURESTORAGE®

SailPoint

PHOTOS PROVIDED BY SHUTTERSTOCK.COM