Keep Schools Secure to Keep Learning

A robust IT security system can prevent cyberattacks, meet federal and state regulations, and protect student and faculty information.

Security experts estimate 15 percent of all data breaches happen at educational institutions. "Today's constant cyberthreats have devastating, crippling effects on our school systems," says Keith Krueger, CEO of the Consortium for School Networking (CoSN). "Only a robust, current IT security system can help safeguard against cyberthreats to a school's technology infrastructure and data assets."

A data breach is defined as when sensitive, protected, or confidential data is lost, stolen, or put at risk. A weak IT security system can leave the door open for malware and viruses, distributed denial of services (DDoS) attacks, criminal and "recreational" hacking and more. "It's not a matter of if you're going to get breached. It's a matter of when," says Peter Streips, president of Network Security Group.

Since 2005, The Privacy Rights Clearing House's Chronology of Data Breaches has tracked more than 10 million education records that have been compromised, either through "unintended disclosure" (sensitive information posted publicly on a website or sent to the wrong party) or "hacking or malware" (electronic entry by an outside party, malware and spyware). Yet this is just "the tip of the iceberg" when it comes to data breaches, says Beth Givens, Executive Director of Privacy Rights Clearinghouse.

Here are several recent examples of data breaches in K-12:

- **May 2015**: Unauthorized individuals gained access to the student information system at San Dimas High School, San Dimas, CA, and changed the grades of several students. The suspects also downloaded personal student information, including social security numbers, birthdates, and medical information.
- **July 2014**: The Park Hill School District in Kansas City, MO, notified parents and faculty a data breach had potentially compromised personal information of more than 10,000 students and district employees, including social security numbers, student records and employee evaluations.
- **November 2015**: The Salt Lake City School district experienced a DDoS attack. These are designed to disrupt or disable the district's information network (as opposed to actually accessing information about students or employees). A similar cyberattack on the Kentucky Department of Education's Infinite Campus information network in August 2013 tricked hundreds of thousands of computers around the world into sending signals to the Infinite Campus portal, jamming up the firewalls.

Such attacks on school district networks aren't unusual. Jeremy Cox, an information security officer with the Washington County School District in Utah, the only district in the state with full-time cyber security personnel, says their district's systems are being attacked "all the time."

THE TRUE COST OF A DATA BREACH: ECONOMIC, MORAL, AND LEGAL

The cost for school districts to fully recover from a data breach can run into tens of thousands of dollars, not to mention the cost of network downtime. Those costs include working with experts to remove viruses or malware, as well as the cost of notifying students and parents about the breach. According to a 2014 study, the education sector

(including higher education) has the second highest per capita cost of cleaning up from a data breach, estimated at $294.

At colleges and universities, the costs of a data breach can reach astronomical proportions. The Maricopa County Community College District in Maricopa County, Arizona, is one the of the largest community college districts in the United States, serving more than 128,000 students. A 2013 breach there ended up costing a whopping $18 million dollars for repair of the security system and notifying 2.3 million current and former students, staff and vendors that their social security numbers and other sensitive data may have been exposed.

THE LEGAL SIDE

Given those statistics, data security in education is clearly an economic necessity. However, it's also a moral and legal responsibility. "These days, schools across the country are being held to a rigorous legal standard for data security—one that leaves little room for error, but substantial room for legal liability," according to a published report in THE Journal.

Over the last twenty years, the federal government has enacted several laws in an effort to protect student privacy and information. That's understandable given the fact that some security experts say educational institutions, including higher ed and K-12, present "the most attractive targets for data privacy crimes." In fact, one estimate suggests more than 140,000 children are victims of identity theft each year.

Federal regulations include the Family Educational Rights and Privacy Act (FERPA) that protects the privacy of student education records from unauthorized disclosure and the Children's Online Privacy Protection Act (COPPA). That requires operators of online sites and services directed at children under the age of 13 to provide notice and obtain permission from a child's parents before collecting personal information from that child.

Perhaps chief among the federal regulations, however, is the Children's Internet Protection Act (CIPA). This was enacted by Congress in 2000 to "address concerns about children's access to obscene or harmful content over the Internet."

Part of that legislation, which was updated in 2011, specifically precludes schools and libraries from receiving discounts offered by the E-rate program unless they certify they have Internet safety measures in place that block or filter obscene or harmful content over the Internet. Internet safety policies must also include the monitoring minors' online activities.

It's not just federal laws that present Internet security challenges to school districts. School officials must also be aware of their own state laws regarding data security and breach reporting requirements. As of January 2015, only three states—Alabama, New Mexico, and South Dakota—have no laws related to security breach notification.

Why are these state laws so important? A recent Massachusetts Superior Court decision stated a plaintiff could sue for financial damages based on "the mere exposure of plaintiff's private information." This is regardless of whether that information was ever used for nefarious purposes. While this case pertained to medical records (not school records) that were "inadvertently made accessible to the public," it foretells the potential for similar education-related lawsuits in the future.

As more student data is collected and stored, parents are becoming more concerned and questioning the necessity of collecting such student data, especially when only an estimated half of K-12 schools use encryption to scramble sensitive and private data. A data breach at a school in Nashville, for example, exposed the Social Security numbers of more than 18,000 students. As one parent noted at the time, "If schools want that information, there should be some sort of penalty paid if they don't guard it with their lives."

Amelia Vance, director of education data and technology for the National Association of State Boards of Education, agrees with that sentiment, yet also takes a realistic view. "Parents want to know the data that schools have can be protected," she says, "but when you're dealing with data, there's always a level of danger."

"Parents want to know data schools have can be protected, but when you're dealing with data, there's always a level of danger."
—Amelia Vance, director of education data and technology, NASBE

To help educational institutions understand the complexities of data privacy, confidentiality, and security practices, the U.S. department of Education created the Privacy Technical Assistance Center (PTAC). This is a "one-stop" resource for education stakeholders to learn about data privacy, confidentiality, and network security. Among its other services,

the PTAC recently released a security checklist designed to help school districts develop privacy programs.

CYBERSECURITY: A TOP PRIORITY

Given the growing threat to school district networks, the potential costs of cleaning up cyberattacks, federal and state privacy regulations, and the potential legal liability a district might face in a data breach, it's no wonder that cybersecurity has become a top priority in K-12 education. IT professionals and other district officials are demanding network security tools to mitigate risks, including appliances that can support deep visibility into network activity, integrate security policies for multiple outside devices, and maintain detailed recording-keeping.

Next-generation firewalls (NGFWs) and unified management solutions provide the best defense for protecting a district's network. "Next generation firewalls are very efficient at monitoring and properly protecting an organization's network," says Dr. Eric Cole, a faculty member at the SANS institute, a research and education organization.

NGFWs offer advanced capabilities for catching threats and combining multiple functions into a single device, including:

- **Deep packet inspection**: This targets traffic irregularities or encrypted malware.
- **Integrated intrusion detection and prevention capabilities**: These ensure that traffic doesn't have to pass through separate security layers and performance doesn't suffer.
- **Content filtering**: This distinguishes good traffic from bad, a critical function for CIPA compliance, not only in school but at home when students use school-issued device to connect to the Internet.
- **Application control**: This allows, for example, YouTube for Schools, but blocks its recreational use. At a public school outside of Boston, for example, IT officials discovered the second most used app by students was a streaming music service. Next-generation firewall technology eliminated student access to the streaming music service.
- **Bandwidth management**: This controls ingress and egress traffic, helps prioritize traffic, and can ensure key services don't suffer from slowdowns.
- **Central management**: This helps you manage multiple network security devices and applications. Centralized management not only simplifies the process, but also controls costs.

After deploying NGFWs, IT officials and other education stakeholders can feel confident their infrastructure will provide a safe and secure digital learning environment for all students. At schools throughout the country, educators are striving to meet the demands of providing students with 21st century learning and skills through technology, whether for collaborative and/or personalized learning, Web-based applications, Internet research, or online testing and assessments.

The primary challenge here is to harness the technology while staying ahead of the ever-present, ever-evolving threat of a data breach or cyberattack. To accomplish that objective, K-12 IT administrators are looking for scalable solutions that provide threat prevention for both wired and wireless network, filtering of objectionable content and Web sites, and easy management.

The first step in achieving that goal, says CoSN's CEO Krueger, is to analyze the security systems a district currently has in place and assess how those systems can be improved to mitigate dangers. For many school districts, their network infrastructure has developed over time—almost haphazardly—creating a heterogeneous mix of non-standardized systems. At the same time, school districts have had their firewalls in place for a long time, even though state-of-the-art in firewall protection has developed substantially over the last few years.

Next generation firewalls can help school districts strengthen and secure their network, meet requirements for CIPA and other regulations, and ultimately help expand and enhance teaching and learning. But schools can only achieve those goals when all education stakeholders take an active role in helping schools secure their networks.

"Security in an organization is not specifically an IT responsibility. It's everyone's responsibility."
—Ed Kelty, CIO, Maricopa County Community College District

As Ed Kelty, chief information officer at the Maricopa County Community College District, puts it, "Security in an organization is not specifically an IT responsibility. It's everyone's responsibility."

Security

Improve your school district's network security with eRate

The federal eRate program makes it possible for you to significantly upgrade your school district's network security and connectivity - at a price that fits your budget.

Dell Security solutions can help you:

- **Put the latest in secure firewalls and content filtering in place**
- **Clean up your wireless infrastructure and maximize performance through WAN acceleration**
- **Reduce administrative overhead with consolidated network management**

Dell SonicWALL scalable, CIPA-compliant network security solutions are available at discount through eRate. For the complete portfolio of eRate available products and services, visit **dell.com/eRate**