SCHOOLS LEARN THEIR LESSONS ON RANSOMWARE

Several schools have already been hit with ransomware, so be ready.

Ransomware is becoming a major issue in the world of education. When BitSight issued its report in September 2016 declaring education the biggest target for ransomware, the news put school officials on notice that they were vulnerable to this form of cyberattack.

Ransomware currently comes in two flavors: encrypting and locker. MarsJoke is one example of encrypting ransomware. This locks user data with an AES 256 encryption algorithm. Winlocker is an example of the second variety. This locks the victim out of his or her computer. In both cases, the user is commanded to pay a bitcoin ransom in order to regain access. Some schools have already learned about ransomware from experience.

- Oxford School District in Missouri suffered a data lockdown in February after a phishing e-mail infected the school system's servers with malware, encrypted files and demanded a bitcoin ransom worth about $9,000 at the time.
- Horry County Schools in South Carolina also experienced a lockout during the same period, possibly when an out-of-date server running legacy applications became infected and spread the malware to dozens of other servers on the same network.
- In April, Follett Corp. learned schools running its software faced break-ins through unpatched versions of Destiny, the company's popular library management application. Cyber criminals took advantage of vulnerabilities in JBoss, Red Hat's middleware, to deliver the ransomware.

Unless your entire district staff is savvy to e-mail phishing, add this to your list of security concerns. The question becomes whether or not to shell out a ransom in these situations. The report hedges, mostly coming down on the side of agreeing with the FBI, which in April officially recommended not paying.

"Paying a ransom doesn't guarantee an organization that it will get its data back. We've seen cases where organizations never got a decryption key after having paid the ransom," says FBI Cyber Division Assistant Director James Trainor. "Paying a ransom not only emboldens current cyber criminals to target more organizations, it also offers an incentive for other criminals to get involved in this type of illegal activity. And finally, by paying a ransom, an organization might inadvertently be funding other illicit activity associated with criminals."

In other words, education technology leaders will have to decide for themselves on an appropriate response. While the South Carolina district paid a ransom of around $10,000, the Missouri district didn't. The difference was that Oxford was armed with a recent backup that allowed the IT organization to "wipe everything clean" and bring technology services back online for the district and its schools, according to published reports. Even then, though, some services were down for weeks.

As with most things cybersecurity-focused, hardened systems are the first line of defense. As the FBI emphasizes, prevention requires:

- Currently patched operating systems, software and firmware
- Use automatically updated anti-virus and anti-malware solutions
- Close oversight of privileged accounts
- Properly configure access controls
- Disable macro scripts from files transmitted through e-mail
- Perform regular backups with integrity checks
- Separate backups from the computers and networks they're protecting

User education is clearly at the top of the FBI list, above all other preventative measures. As malware sophistication increases, getting users trained to recognize the problem and take appropriate action is really your final defense.

Casa Grande Elementary School District, which has also experienced ransomware up close, appears to agree. In a staff memo dedicated to the topic, IT acknowledged "several" people within the Arizona school system had their computers infected. Then the district proceeded to help its users understand how to respond in the event of an infection with a step-by-step list of instructions and clear advice on how to recognize infected messages.

shutterstock.com

THE SMALL DISTRICT CHALLENGE

Smaller schools and districts face some unique challenges when it comes to defending against ransomware.

When the State Educational Technology Directors Association (SEDTA) issued its latest recommendations for broadband capacity, there was a major difference in the current report as compared to the 2012 report related to how it handles estimates based on district size. One particularly interesting note is how it considers smaller school systems.

In 2012, the State Education Technology Directors Association's original set of bandwidth goals offered a lone minimum. By the 2017-2018 academic year, every school should aspire to provide Internet access speeds of 1 Gigabit per second (Gbps) for every 1000 users; whether those were students, staff or guests.

In the report just issued, "The Broadband Imperative II: Equitable Access for Learning," SETDA re-examined their recommended capacity from the perspective of school size. While medium school districts (those with around 3,000 students) stayed the course at 1 Megabit per second (Mbps) per student for 2017-2018, smaller districts (fewer than 1,000 students) now have a target of at least 1.5 Mbps per user with a minimum of 100 Mbps for the district. Large school systems (those with more than 10,000 students) have a goal of at least 0.7 Gbps per 1,000 users.

SETDA bases its recommendations on "research, analysis of data sets from districts across eight states regarding both capacity and usage, and consultation with experts in the field." The report emphasizes, "some districts will need more than the recommendations depending upon their digital learning environments."

Study the math for a moment, though, and you'll quickly realize that smaller districts are actually being pushed to have more capacity per user than mid-sized and large districts. "Basic administrative and automation functions" consume a larger proportion of the overall network usage. That actually increases the per-user bandwidth requirement.

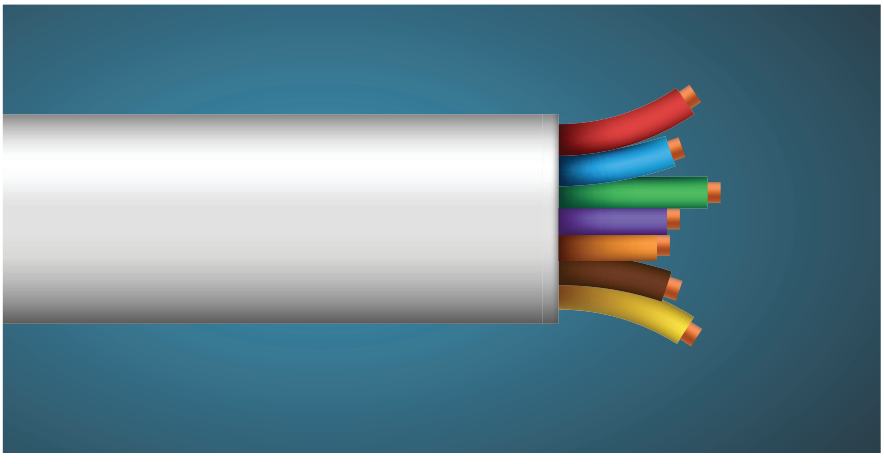
For example, the report states, "an extremely small school with 15 students and a 1.5 Mbps per user connection technically meets the current connectivity requirement, but they don't have enough bandwidth for more than a few intensive bandwidth activities at the same time." On top of the stack of student uses are those school overhead functions, such as state reporting, student information system usage, and security functionality.

If there are 50 students in a district, a quick calculation suggests bandwidth capacity of 75 Mbps (or 50 x 1.5 Mbps). But because that's below the minimum threshold of 100 Mbps for the district, the recommendation would be to contract for at least 100 Mbps. The targets rise across the board for 2020-2021. At that point, small districts are encouraged to have at least 4.3 Mbps per use with a minimum of 300 Mbps for the district.

Along with internet bandwidth IT organizations at small districts also need to consider the wide area network (WAN) capacity. As the report advises, it's "important to ensure that the individual school site has a connection from the core network that is at least as large as the recommended target." As a starting point, SETDA advises at least 10 Gbps per 1000 users for WAN access in the 2017-2018 timeframe.

That's not expected to change for the 2020-2021 school year. Virtualization efforts will shift the capacity burden from the WAN to the internet service provider. As a result, however, districts will want to choose networking components that can keep up with the pace of future requirements.

As CoSN's Smart Education Networks by Design (SEND) initiative advises, districts struggling to figure out how to right-size their infrastructure to support a digital transformation in learning shouldn't try to do so alone. "Learn from other districts [that] have been where you are. Aggregate purchasing, design, implementation and network management in order to get top performing networks affordably," district technology leaders told the Consortium for School Networking. "Work with your vendors as partners rather than as commodity vendors in order to create service level agreements and learn together."



shutterstock.com

GameChanger

AVERT THE HIGH PRICE OF SECURITY

Keeping your district network safe from intruders doesn't have to gut your IT budget.

Schools suffer two major disadvantages when it comes to security. First, while they may be aware of potential vulnerabilities and attacks, they're not necessarily in the same position as private industry to hire and retain deep security expertise. Second, spending on IT infrastructure isn't the first priority for district budgets.

To get around both those obstacles, savvy IT leaders are trying an end-run that utilizes a new service delivery model. It's probably no surprise to any IT hiring manager the information security talent gap is widening. More than six in 10 survey respondents (62 percent) told (ISC)² their organizations have too few information security professionals. Another study by ISACA found there aren't enough qualified security job candidates, and those individuals worth hiring may command salaries beyond the scope of the typical school district budget.

Given that scenario, it's no wonder school districts have a hard time attracting top security talent, says Dan Sell, who manages Security-as-a-Service (SECaaS) for security company SonicWall. "No disrespect meant to school districts, but if you're a hotshot security person, you're going to go work for a bank or some other industry that has cachet."

There's also the recurring challenge of ever-growing Internet requirements. Consortium for School Networking (CoSN) named broadband and network capacity the top priority in 2016 for IT leaders. Buying a firewall appliance can be a major investment. In a high-growth scenario, however, that doesn't always work to the district's advantage. Driven by a dramatic rise in the use of student devices, the growth in digital content and the arrival of online assessments, school IT organizations are grasping to keep up with the pace of broadband connectivity.

"All those factors are making people blow through their firewalls," Sell says. "When you've used capex, and you're hoping to get five years out of the firewall, you may have a big 'Oh, shoot!' moment when you realize at 18 months that all of a sudden it's not the right model anymore."

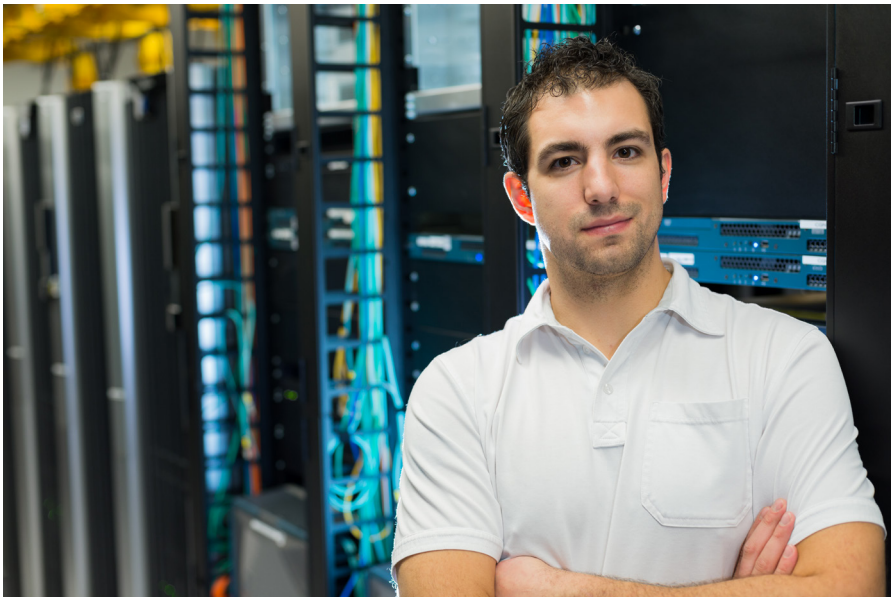
One new approach can address both those challenges of hiring and acquiring right-sized security appliances: "Security-as-a-Service" (SECaaS). This delivers security as a subscription, covering baseline security operations every school requires: intrusion detection, web content filtering and anti-virus and anti-malware coverage.

SECaaS works like this:

1. You hire a local SonicWall partner with certified security experts to provide the cybersecurity your district needs.
2. Security staff provides all equipment needed for your specific computing environment, sets it up, and performs all configuration tasks. The firewall appliance runs the same security management system the largest enterprise customers rely on to protect their assets.
3. Those security experts handle the cybersecurity monitoring and reporting from their facility and keep you informed at the level you choose.

As part of your annual IT planning, you assess when you need to upgrade, swap out or return the physical security gear. Managed Internal Broadband Services are E-rate eligible, so schools can build the annual subscription fee for SECaaS into Category Two funding requests.

The SECaaS approach fits perfectly into the annual budget mindset of most school districts, says Sell. "If you have capital constraints—and almost all schools do—the whole premise is you have no upfront cost, you work with a local security expert, you pay a monthly subscription price, and you get flexibility to return or upgrade the gear. That's a pretty straightforward value prop."



shutterstock.com