TECH TACTICS

IT Mastery over the Remote Classroom

When going to school means going online, a new set of learning standards is required – calling for smart use of relief funds and a boundless approach to cybersecurity. These 10 do's and don'ts will help you target your planning.

AS EDUCATION EVOLVES IN 2021, adrenaline-charged scrambling is finally giving way to more thoughtful adaptation. New sources of government relief funding are providing schools and districts with the capacity to put in place more permanent technology solutions to enable anywhere teaching and learning for every student, not just those already outfitted with devices and connectivity. And the IT organization finally has the breathing room to figure out how to secure operations properly.

A big question to address is how to deal with the "upside-down" nature of cybersecurity, as Sony Kogin put it. Kogin senior manager for security vendor **SonicWall**, has dedicated his career to the network and IT security segment, and he said he has never seen anything like what transpired for organizations in 2020. "In the past when the majority of users were in one or two centralized locations – the castle – it was very easy to protect them," he explained. "But now we're in an inverted situation where the users are *outside*. That renders investment in traditional firewalls and other security devices useless. How do you protect when the users are outside? It requires a new approach to protection."

The answer is what he calls the "boundless cybersecurity model" – the idea that the security perimeter follows wherever students are learning and teachers are instructing and extends to wherever digital school assets reside, whether on the device, in the data center or in the cloud.

Before IT jumps in to say the district can't afford boundless *anything*, added Holly Davis, an E-rate expert running **Komplement Consulting**, it's important to make sure everyone understands the recent education relief funding provided by the U.S. government – $82 billion for K-12, made available through CARES Act ESSER I and ESSER II. These new grants aren't tied to the traditional buying cycles used for the federal E-Rate program; their purpose is to help schools support the purchase of remote learning technology.

PRESENTED BY: THE JOURNAL | SPONSORED BY: SONICWALL®

DO'S

Essential Do's and Dont's of Operating the Remote Learning Environment

SonicWall expert Sony Kogin and Komplement Consulting school funding expert Holly Davis share key dos and don'ts for funding and putting an IT security profile in place that will hold up under continued expansion and change.

1 DO tackle the homework gap once and for all.

PRE-PANDEMIC, SCHOOLS OFFERED PLACES WHERE students could get their homework done, primarily after-school programs and libraries. If students lacked internet at home and didn't have a computer, they could use the technology provided in those outlets. When that capability wasn't viable due to the pandemic, the real disparity of the "homework gap" came into focus (and is now better known as the "remote learning gap").

As Davis noted, "If students need or have to attend their classes at home, it's even more important to make sure that every child has equal opportunity to learn, which is one of the greatest challenges schools are facing during the pandemic. Suppose you don't have one-to-one device learning and you can't provide the student with the necessary collaboration applications on an internet connection that is safe and secure? That's a big challenge."

Davis strongly encouraged districts that suddenly have new sources of funding "just dropped into their lap" to address the technology gaps that have existed for a long time. Her advice: "Let's rip that bandage off. Now you have the chance to make sure all your students have connectivity at home, which is safe and secure. It may require thinking outside the box in researching innovative technology to upgrade the on-campus infrastructure and secure the connection to support off-campus traffic."

Only then will those students who in the past might have had to stay after school to complete their homework be able to head home and enjoy an authentic "homework" experience, creating "a fairer and more equitable learning environment."

2 DO become proactive about planning for remote learning.

NOW THAT THE EMERGENCY RESPONSE TO THE pandemic is starting to ease, schools are becoming more concerned about making the right choices long-term. In the case of public schools "we have to remember they're spending public funds," suggested Davis. School officials – including the superintendents and IT teams – can expect their actions to be examined based on how well they responded to the COVID-19 pandemic and used the funding available to them to set more permanent solutions in motion.

Even as kids return to school others will stay home to continue their learning remotely, she pointed out. The synchronous learning model isn't going away any time soon, and IT decision-makers will need to take that into account when designing their solutions.

Davis has advised schools to step back from their reactive activities and engage in long-term planning. What would that look like? "I'd want them to whiteboard a few things for me: the types of device they have their students learning on; the applications being used for collaboration; what's being done for students who don't have connectivity at home; and the capacity of technology they use today to support traffic for synchronous learning environments – just to see if they are looking holistically at what solutions are available to them."

Another big aspect of planning is to examine security, Davis said. "Are they doing anything for application security? How are the teachers who are not in the classroom getting onto the network for student/teacher communications and learning? How are all the endpoints being monitored? Is the firewall capacity sufficient to be able to capture everything that could possibly be an unknown risk? You have to have really good technology that can manage all of that."

Once IT accounts for what it has in place today and what the goals are for the future, Davis explained, they can prioritize the quick-fixes (A) and then set the long-term goals (B) to begin building "the bridge that will let them get from A to B."

3

DO adopt a zero-trust posture.

WHILE USERS WANT TO GET TO THE SCHOOL resources they require quickly and easily, effective IT oversight in the new normal has to cover the risks of mobile access. What it comes down to, asserted Kogin, is that students (along with teachers, staff and administrators) cannot be trusted to secure their own devices.

Typically, to prevent problems, users might have been required to log onto a virtual private network. When the infrastructure and users are local, the VPN approach can do the job, said Kogin. That's no longer the case though, he added, as people are migrating for health, sanity, financial need or other reasons. The limitation is that relying on VPN doesn't necessarily address the malware that makes its way into the server infrastructure through some other route.

Schools are finally realizing they need to adopt a "zero-trust" posture: Nobody gets onto the network until they've run the gauntlet. And even then, they can't roam free once they're inside the network, and all data remains "at rest."

In this scenario, "no data can be transferred from one place to the next, especially outside the infrastructure itself. If a user connects, what he or she is seeing on the screen is actually a picture. It's not because the data is being transferred to his local hard drive," said Kogin. "The manipulation of the data actually happens within the school data center itself. Nothing gets transferred. Zero trust is very secure."

For that reason, Kogin urged districts to choose a security vendor that can address the VPN requirements where that's sufficient along with more comprehensive solutions that guarantee zero-trust.

4

DO choose a security solution that will stop breaches at the edge.

TECH-ENABLED STUDENT LEARNING USED TO resemble the Clone army: Every child in a class or grade was outfitted with the same device, making for lockstep maintenance and security, simpler class management and stronger buying power. No more. Now, computing looks more like the Rebel Alliance, with a motley collection of district-issued laptops, Chromebooks and tablets – both old and new – and family-owned computers, ready to serve as called on.

As users switch on their devices and log in to begin the school day, it's important to make sure those computers are ready and aimed to blast down malware attacks at the edge rather than waiting until they get into the network. Without the right protection in place, Kogin said, "malware is going to roam free in the hard drive, jumping from one file to the next. The next day, when the student connects

to the school network to hand in homework, that same malware could find its way into a server in the data center."

Blocking that outcome requires a combination of advanced threat functionality, including:

- Machine learning to automate and speed up the decision-making
- Access to a network sandbox for inspecting dubious packets that may pose brand new threats not already covered by the device's anti-virus
- System rollback, for the recovery of files and OS functionality that have been encrypted through ransomware

Plus, added Kogin, the solution has to be "easy to use, even transparent for provisioning to students" and it has to have "the flexibility of being hosted off-site and on premise."

5

DO choose a company with broad experience in education and a complete product portfolio.

SOME CYBERSECURITY COMPANIES DO A GREAT job of addressing the needs of the enterprise. But K-12 isn't a multinational. Kogin advised IT organizations to choose a security vendor that specializes in addressing school requirements, where there's often network complexity for supporting quite diverse user groups, legacy systems from a variety of companies and, seemingly, never enough budget.

Likewise, Kogin urged districts to choose a vendor that "has a broad product portfolio," since that's the best way to make sure the various security components integrate and "are tested to play nicely together."

Essentials for Securing School IT

Putting a comprehensive security framework in place for K-12 requires a three-pronged approach: the use of endpoint management to secure users, secure access infrastructure and cloud application security. The SonicWall solution encompasses each:

SonicWall Capture Client

Protects the student device, ready to detect malware and perform URL filtering. When a threat is positively identified, the file is quarantined and removed. Where there's not a solid identification, because the threat is brand new, Capture Client goes to the SonicWall cloud engine for remediation. The program is agentless and protection extends to any operating system, including those running public browsers.

SonicWall Secure Mobile Access (SMA)

Resides in the data center and acts as a gateway, protecting applications and data across hybrid environments, serving both internal and remote users. Before a student device is allowed on the school network, for example, SMA makes sure the user is authenticated (including by user location) and the device complies with policies (such as the latest patches). While SMA works with the company's own Capture Client, it also supports many other anti-virus programs. SMA can be deployed as a physical appliance or as a virtualized appliance in a private cloud or public cloud.

SonicWall Cloud App Security (CAS)

Delivers the final blow to bad traffic by securing schools using software-as-a-service and cloud-based applications, such as G Suite for Education, Office 365, Zoom, Teams or Meet. Security covers email, anti-phishing, URL filtering, ransomware protection and account takeover.

DON'TS

1 DON'T confuse relief funding with E-rate.

DAVIS SAID SHE FINDS THERE IS A LOT OF CONFUSION about the difference between E-rate funding and CARES Act funding. E-rate, managed by FCC agency USAC, has been around for decades, with a focus on making sure districts have the on-campus connectivity they require for equality learning in the classroom. The percentage of discount a school may receive from the government is determined by how many students participate in the national school lunch program. The program discounts range from 20 percent to 90 percent of the costs of eligible services.

CARES Act funding was, of course, put in place in 2020, then expanded for 2021. For K-12, it's ultimately managed by the U.S. Department of Education and directly through individual states grant portals. It includes several buckets of funding for K-12 to include, 1) Emergency education relief grants managed by governors, based on what they identify as the greatest needs in their states; and 2) ESSER I and II funds, dedicated to elementary and secondary schools, awarded by the U.S. Department of Education for management by state education agencies.

A big difference, according to Davis, is this: While the relief funding could cover anything to help schools continue their operations, including delivering remote instruction and preparing for a return to in-person classes, E-rate pays only for on-campus technology infrastructure. It doesn't cover anything that happens off-campus. E-rate is useful for funding internet service for the classroom and also supports the technology infrastructure to support an e-learning environment, such as wireless, firewall cybersecurity hardware/software, switch, and routers, cabling and licenses for support.

While those elements are important, in a remote learning scenario other components also come to the forefront: computing devices, internet access to homes, virtual private networks, security not built into the internet provisioning and other hardware and software needed to harden all of those devices and address mandates such as content filtering.

One expectation Davis has is that E-rate funds will generate a "lot of network refreshes" in the next five years, with relief funding being used to make sure students have devices and connectivity which have been properly secured. Put in the broadest terms, according to Davis: "Use CARES funding for anything off campus. And for infrastructure on campus, use E-rate."

2 DON'T assume digital natives are security experts too.

THE REALITY ABOUT K-12 STUDENTS IS THAT they're at their peak of curiosity, have undisciplined browsing habits that lead to undesirable destinations and can be naïve about cyberthreats. "They'll visit a website that recognizes they're a new target and send them some inviting message. Without thinking very deeply, the student will most likely click on it," said Kogin. Too often, he noted, it turns out to be a phishing ploy that leads to the activation of malware. There's only so much cybersecurity training students can absorb, and much of it flies out the window when they're invited by online friends – real or otherwise – to try out a game or view a video.

Schools need to keep that in mind as they're mapping out security. "IT administrators not only have to understand technology choices, but they also have to understand the psychology and the usage behavior of the people they're serving, and that would be the students. Don't underestimate its importance."

3 DON'T believe that because students are learning from home, their security needs don't belong to school IT.

"EVERY SCHOOL IS RESPONSIBLE FOR THE SAFETY of the children while they're on the school's network when they're sitting at their desks in a classroom," observed Davis. Now that they may be learning in their own home environments, the same IT responsibility applies, she said, even if the same controls aren't available.

Davis likened the situation to a young person with a learner's permit. "As the parent, you have control on where they drive and what they do, because they can't go anywhere without you. But as soon as they get their driver's license, they're now out there driving around and there's no control, unless you put some kind of tracker on the car or the phone. It's really hard to control where they're going and what they're doing, unless you secure it."

In the case of remote learning, that includes imposing the same level of content filtering when the student is using school resources, making sure they adhere to the rules before they gain access to the network and ensuring their student data is protected from misuse, no matter where it resides.

4 DON'T assume cloud apps are already secured.

WHILE CLOUD HAS BECOME THE ESSENTIAL ingredient for delivering anywhere education, cloud providers consider security a "shared responsibility," asserted Kogin. "They will not provide the complete protection needed by schools." Anything that's added on top of the cloud foundation – collaboration, communications, file sharing, or any of hundreds of other SaaS-based ed tech applications – becomes the district's security burden.

Dedicated cloud application security is a breed of software that analyzes real-time traffic and compares it to historic patterns to detect anomalies and stop further action. A best-of-breed solution will provide native APIs that deliver dual benefits: 1) protecting email, messaging, data and user credentials without adding latency or extra overhead to the security process; and monitoring for and

stopping targeted phishing, impersonation and account takeover attacks in applications such as Office 365 and G Suite for Education.

5 DON'T keep throwing out hotspots or consider LTE the answer.

IN FALL 2020, SOME 3.7 MILLION AMERICAN households with school-age children still lacked regular internet connectivity, according to an **analysis of Census data by USAFacts**. When schools shifted to online learning, they found that oftentimes connectivity was being supplied by parents' smartphones serving as hotspots. When the adults headed to work, access to the internet went with them. As a stopgap measure, a lot of districts took relief funding and quickly issued portable hotspots to families, enabling them to gain connectivity at school expense. These are small routers that can connect to a cellular network to provide internet access to multiple devices.

"But what a nightmare that has proven to be," observed Davis. One problem: It's not a long-term solution, she said. "It's a recurring cost that's going to be a budget constraint for them in the future." Another problem: It's difficult to control who uses the limited bandwidth made available. And finally, schools are facing challenges in properly securing student devices relying on this form of access.

Similarly, Davis has detected a trend among the largest school districts to consider building private LTE networks, taking advantage of the Citizen Band Radio Service (CBRS) spectrum. This has become especially popular for districts serving large rural areas. Her take: "In many instances this could prove cost-prohibitive for the school district."

Davis' advice is to evaluate "new, innovative technology" that can meet the objective of providing connectivity to the school community. "Don't rely on outdated technologies or approaches. There are really great new ways to solve this," she said. " IT and administrators need to talk with their vendors and manufacturers to trial the technology and do the research. They can help to identify and aid in designing really unique solutions."

Boundless Thinking

AS THE YEAR UNFOLDS, SCHOOL ENVIRONMENTS will continue adapting. The definition of the "edge" could expand and shrink and expand again. What's important is to lay the groundwork now for boundless learning protected by boundless cybersecurity. That's the best way to ensure that wherever the learning takes place, IT has shown itself to be forward-thinking for tomorrow's challenges while still effective for today's surprises.