SONICWALL | CAMPUS TECHNOLOGY

EDUCATION LEADERS ON...

Supporting Safe and Effective Digital Learning

SONICWALL | CAMPUS TECHNOLOGY

INSIGHT SERIES: EDUCATION LEADERS ON...

What Are They Thinking?

Leadership Insights on Issues in Educational Technology

CONTRIBUTORS:

Matt Morton, security project consultant, University of Nebraska at Omaha

Kyle Bowen, director of informatics for information technology, Purdue University

Joy Hatch, vice chancellor, Information Technology Services, Virginia Community College System

Dr. Richard Sebastian, director of teaching and learning technologies, Virginia Community College System

SUPPORTING SAFE AND EFFECTIVE DIGITAL LEARNING

The proliferation of mobile devices and the push toward collaborative learning in today's universities has presented new security challenges for IT departments. How do universities ensure the security of their infrastructure while fulfilling the needs of new learning initiatives? *Campus Technology* spoke with three universities and security vendor SonicWALL to get their insight.

SONICWALL | CAMPUS TECHNOLOGY

INSIGHT SERIES: EDUCATION LEADERS ON...

What does collaboration mean for today's digital learner and why is it important?

MATT MORTON: Today's learners, more than ever, use collaboration tools to complete assignments and work on projects. This is also a key skill required for the workforce. Being able to understand the tools and use them is part of the digital literacy that is sorely needed. Tools like web conferencing, Skype, IM, and e-mail are all key technologies that today's learners should be coming to college with. Collaboration is one of the three C's of digital literacy, content, convenience, and collaboration.

KYLE BOWEN: Collaboration is a key aspect of any student's academic success. Activities such as discussing coursework outside of class and working with other students on projects are correlated with academic performance. Nearly every student uses social networking websites as a way to engage and communicate with their friends, and increasingly they have been turning to these tools as a means to communicate with classmates about course related topics. In many ways the same tools students use to manage their social life are used to administer their own learning experience.

Because students come to social tools on their own, they are left to find creative ways to bridge the divide between their own personal learning environment and the institution. The widespread adoption and use of social networks creates an opportunity to improve student success by establishing learning environments that help students build a support network, allowing people to connect and share content from their courses, learning communities, and friends.

JOY HATCH / RICHARD SEBASTIAN: Collaboration is vitally important for today's "digital learners," a term that now applies to all learners. Learning is slowly making a fundamental shift away from the "content delivery" model—still found in college lecture halls—to one that engages learners more deeply with content by asking them to solve messy problems, work on teams, and develop their own firsthand understanding of course material. This shift has been caused by rapid innovations in technology; especially the Internet and more recently social media networks, with these same technologies also providing the solutions.

shutterstock.com

Now, learners can not only read an important text, but also discuss it with the author via Skype. They can group-author a paper using Google Docs anywhere an Internet connection is accessible. And, after writing the paper, they can share it publicly by posting it to a blog or wiki, annotated with images and videos they created with the sophisticated digital media tools they carry around in their pockets. A learner's understanding can now be easily demonstrated through the creation and sharing of digital artifacts, as well as by the number of correct answers on a multiple choice test.

TECHNOLOGY INSIGHT FROM SONICWALL: With the ever increasing volume of traffic driven by user collaboration—including large media file attachments and links to streaming content—throughput is now a major consideration in evaluating security equipment. The closer to line speed a security measure performs, the better. Some organizations seek to address the issue with increased bandwidth and an increased number of switches accessing the network, each with their attendant security measures with load-balancing solutions often in front of it all.

This can get expensive and complex. And any piece of equipment through which traffic passes can become a chokepoint. Underpowered processors or store-and-forward architectures in the appliances can introduce latency into the flow. When threats are detected, remediation can further slow traffic. Fewer, faster systems can assure better performance and lower costs.

What is the role of anytime, anywhere learning in higher education?

MATT MORTON: Being able to access the content required for learning at anytime shifts the student from a synchronous environment to an asynchronous one. As students move towards this convenience of anytime, anywhere content, faculty will need to adapt their styles to meet the demand. There is still a place for synchronous education. However, as incoming students rely more heavily on asynchronous methods due to time restrictions, it becomes more of a "learn at your own pace" model. With that said though, in my opinion, the time for "knowledge activation" on a particular subject will still take the same amount of time for the individual no matter what method is applied.

KYLE BOWEN: The pervasiveness of mobile devices offers new capabilities for changing when and where the moment of learning takes place. For many students, mobile devices and social networks are their native environment—where they live their digital lives.

The benefits of mobile devices, such as smartphones and tablets, go well beyond access to digital content in the classroom, laboratory, or field. Mobile devices enable connections between students both inside and outside of the classroom. Within the classroom, they can create a backchannel of discussion between students—adding additional layers of interaction where learning was already happening. This same technology can also enable students to reach out beyond the classroom and the class to find new ideas that can further extend the classroom discussion. This virtual discussion medium also makes it possible to ask stupid questions, comment on taboo topics, or help introverted students find their voice in a larger group.

Mobile technology also enables students and instructors alike to easily create new digital media in the way of video, audio, or still images that can be used for learning and assessment. Rich media is found in nearly every part of our everyday lives. Instructors are weaving media creation into their course assignments—for some students, the first time they create a digital video for someone other than themselves may be for an assignment in their Science, Personal Finance, or American Sign Language class.

shutterstock.com

JOY HATCH / RICHARD SEBASTIAN: Thanks to the growing ubiquity of "always-on" broadband connections as well as smartphones and tablets, and an increase in informal and open learning, learners now expect to be able to login to their classes and communicate with their instructors and classmates whenever they want. Institutions of higher education are feeling the pressure to offer more online courses and programs, as well as develop and implement robust mobile learning solutions. The campus is moving away from being the location of learning, to being a place that provides the services that mediate the act of learning.

This is of significant importance to higher education because these new demands from learners suggest a need to retrofit some of the traditional structures of higher education for the digital age: the college semester, the classroom, seat time, and the college degree, to name just a few. Institutions slow to adapt to these changes are going to find their students looking elsewhere for an education.

SONICWALL | CAMPUS TECHNOLOGY

INSIGHT SERIES: EDUCATION LEADERS ON...

TECHNOLOGY INSIGHT FROM SONICWALL: Secure Remote Access (SRA) has moved from a small, precious component of the network for a core constituency to becoming the vast outer ring of the network serving many—if not all—users. Of course, users can fall into several different groups, each of which has its own needs and permissions. The smarter the remote access solution, the better the user experience and the easier it is to manage.

Trusted users can be expected to gain access via devices with client controls in place. Casual users cannot, especially with the proliferation of various endpoints like tablets and smartphones. Intelligent SRA can recognize the different levels of control required, prioritize traffic accordingly (including latency-sensitive streams like VoIP and video), and integrate with intelligent security appliances to enforce centrally managed policies.

What are the top three challenges facing colleges and universities that are trying to implement an effective, safe, and secure 21st century learning environment?

MATT MORTON: Information Security. Besides the obvious issues surrounding privacy and data security, the integrity of the IHE's academic data, including collaboration platforms, must also be secured. That means looking at the learning management systems (LMS), conferencing solutions, and other data sources that support the learning process and ensuring that those are safe from attack or abuse.

Bandwidth to support "on-demand" environments.

Data analytics to measure what is working and what isn't, as well as, providing a view into how the content is being used (or not used). Feedback on whether or not students are actually getting the material, or are actually putting forth effort, will help ensure that this "anytime, anywhere" model is successful.

KYLE BOWEN: Access is the key challenge—that is providing students with the connectivity to engage with instructors and fellow students, create digital media, or consume learning content—presented in a way that is universally accessible to all students no matter the disability or preference of device. Even the content itself should be designed for greatest elasticity—not just for online delivery, but also for the smallest of screens. Students are carrying new technology into the classroom at an unprecedented rate. For any student sitting in the classroom, it is not unreasonable to think that they have a smartphone, laptop, and e-reader that are all connected to the network.

Tools. So much of the previous efforts for information technology groups have been focused on building the infrastructure to support learning environments. Now that traditional IT services, like networking, is a commodity service, and hosting is moving its way into the cloud, a new opportunity emerges to create learning technology where student success is the focus. A mainstream convergence of mobile and social technologies has made it easier than ever to connect with students in a robustly interactive learning environment that takes advantage of the tools most common to students. Technology groups should engage this trend, and begin to pioneer new technologies and services that exploit the school's existing infrastructure.

Awareness. Having the technology in place to maintain a secure environment is important, but the greater challenge is to help the university community become more aware of secure behaviors. Most kids are taught the simple life lessons of eating their vegetables and not talking to strangers—rarely are they taught not to open e-mail attachments or to consistently pick a strong password. These are the types of security lessons schools should teach their students in order to be safe when they go online.

JOY HATCH / RICHARD SEBASTIAN: This is a matter of reducing risk, not eliminating it. Any security solution used must minimize enough of the risk without affecting the creation of robust and vibrant learning communities or accessibility to online tools. It also needs to be responsive to rapid developments in instructional and information technology, providing flexibility to instructors and learners who are exploring new ways of communicating and learning.

shutterstock.com

Establishing appropriate rights and permissions for end-users is a challenge for all institutions. Employees are hired, they move to different areas on campus, or they leave for other opportunities on a continual basis. It is important to have procedures for granting and revoking privileges, changing access to systems, and terminating accounts as these changes occur. A yearly review of system access will ensure users have access to only required systems and information, thus ensuring a safe environment where the integrity of data is not compromised. The other major challenge, and the potential weak link in all of this, is the activity of the end-user. It is crucial that end-users have continual security awareness training to encourage them to stop and think about their actions, and the consequences of those actions. At Virginia's Community Colleges, all users must complete security awareness training on a yearly basis, or their system privileges will be revoked. This training helps us maintain the safe and secure environment that we need to create that effective learning environment.

TECHNOLOGY INSIGHT FROM SONICWALL: The technical expression of how users are interacting with the network is on the application layer. The applications users are running are either permitted, or not. Inside the permitted group, some applications deserve higher priority than others. Next-Generation Firewalls supplying Application Intelligence, Control, and Visualization (AICV) enable granular scanning and filtering for the most targeted and intelligent security possible. This improves the quality of threat detection—especially the new web-borne application layer threats—and minimizes the disruption when threats are detected. It also gives IT administrators application-level controls for policy enforcement and traffic prioritization.

These capabilities can, in effect, free bandwidth and allocate it where it is most needed. They can automatically implement policy and prioritize flows by application type and user. And they can provide the analytics necessary to fine tune the network moving forward.

What are the biggest mistakes you've seen institutions make in securing their networks for digital learning?

MATT MORTON: Not allowing enough time or resources to ensure that the students have a safe online experience. Many times institutions don't work through a risk process at all for any aspect of their operation, let alone the digital infrastructure. It is time consuming, and most small- to mid-sized institutions don't have the luxury of a full staff of security experts.

shutterstock.com

KYLE BOWEN: The greatest mistake is believing that the technology can protect everyone from everyone. Being "secure" is something that requires constant vigilance, because the work of those seeking to do harm can outpace the work of those who seek to protect us. Despite this, it is critical that a digital learning environment be open and easy to use. Restricting how the network can be used or the devices it can be used with, is counter to the idea of providing this type of access at all. Collaborative learning environments require anywhere access to a wide range of tools that can be adopted at a moment's notice. Some of these web or mobile apps introduce new security or privacy concerns. This is why it is important to create an awareness of safe online behaviors.

JOY HATCH / RICHARD SEBASTIAN: An enthusiastic security team has several potential missteps that could be made if they do not understand the dynamics of learning in the digital age. Chief among these would be the introduction of too many procedures and controls to create a secure environment, and an inability to balance conflicting business risks. These processes could easily thwart efforts from the faculty and students to do creative things. Part of this problem is due to the disparity in the "language" spoken by the various constituents. This discrepancy can create an environment where the security team does not understand core business requirements, and therefore cannot create secure solutions to help meet these requirements.

TECHNOLOGY INSIGHT FROM SONICWALL: Aided by Application Intelligence and Control built into Next-Generation Firewalls, the right application controls are granular enough to enforce permissions by application, by user group (e.g., students vs. faculty) and even by individual users. The permissions can be modulated from "fully on" to "throttled" to "blocked"…even by time of day or point of origin. What's more, this Application Intelligence—knowing who is using what applications—is an invaluable tool for addressing regulatory compliance and budget planning.

This enables an optimization between real, important security issues and the best user experience possible. It also relieves users and administrators from struggling with human behaviors and focuses network management where it is most practical: how the network and applications behave.

What advice do you have for campuses wanting to create a secure infrastructure that will ensure safe and effective 21st century learning?

MATT MORTON: I am looking at managed security services (MSS) along with more edge devices to simplify the tasks of securing the network. Most institutions can't afford to hire the staff it takes to properly secure a network in today's environment. Economies of scale indicate that a provider like Dell Secureworks can help. This doesn't mean there isn't still a hardware requirement. Firewalls, like SonicWALL, and other edge protection devices are still necessary to ensure that the network is safe. MSS can assist in managing all of those devices and generating the proper reports from them to identify risk.

KYLE BOWEN: One key to securing a network is to know, and be honest with yourself, about where your own vulnerabilities are, and where your defenses are most critical. Part of this is to know what needs to be protected, and the consequences to exposing or losing this information. In addition to steps that IT can take to secure the network infrastructure, it is also important that they provide users with the tools to secure their own devices along with an understanding of how to use them.

JOY HATCH / RICHARD SEBASTIAN: Learning about the digital classroom environment is step one to providing a secure infrastructure for a college. With this background, the technology and security teams will be able to work collaboratively with faculty and staff to define sensitive data and understand where that data resides—both digitally and in paper form. This working group will also be able to create reasonable security controls that will enable the college to operate efficiently and effectively.

With this structure in place, the final step would be awareness, and ensuring that all constituents are aware of the issues, the risks, the controls, and how their actions will make the learning environment a more secure place.

TECHNOLOGY INSIGHT FROM SONICWALL: Security consolidation is the emerging approach to addressing multiple threat types and the attendant costs of defending against them. Intelligent security appliances have become platforms for multiple security applications running simultaneously, like intrusion detection and prevention, anti-virus, anti-malware, content filtering, and more. Single-pass security—provided it is robust enough—addresses several challenges: It minimizes or eliminates the latency that multiple devices can introduce into network flows; it eliminates the costs of multiple devices; and it simplifies network management. It also simplifies the forensics necessary for understanding network utilization, which is essential for informed provisioning of the network moving forward.