Securing The 21st Century Classroom

A World in Transition

Just as information technology has revolutionized the commercial sector, IT presents new challenges and opportunities for K-12 education. The very fact that the general population now relies on these technologies across their daily lives has changed the needs and expectations of students, families, and whole communities.

Virtually every occupation for which school prepares students involves some understanding of technology. And information systems are essential to improving academic performance with a constantly evolving curriculum. Despite these increased expectations—or, perhaps, because of them—the financial resources of schools are more constrained than ever. Given the annual nature of most school budgeting cycles, the long-term ROI benefits of IT investment cannot be as easily recognized or evaluated.

On the personnel front, increasing technological sophistication often outstrips a district's capabilities. New, incoming instructors often arrive with technical knowledge from their personal and collegiate experience beyond what a K-12 school can accommodate. And the students and their families often enjoy systems at home or the private workplace that raise their expectations for connectivity, availability and responsiveness.

In fact, technology over-all has raised people's expectations for service and convenience. And the sheer quantity of information now available to the general population is unprecedented in human history. This is both a blessing and a curse for schools, whose job it is to transmit information in a structured and productive process.

To both guide and constrain the school's tasks, regulatory regimes have evolved to cover every intersection of information technology, instruction, and school administration. Concern for children's online safety has produced the Children's Internet Protection Act (CIPA). The Family Educational Rights and Privacy Act (FERPA) extends these concerns to a student's entire family, preventing access or distribution of inappropriate content while protecting individuals' privacy. The measure of academic performance (which IT is supposed to help) is the No Child Left Behind Act (NCLB). While the measure of administrative efficiency and effectiveness (which IT is also supposed to help) can take any number of forms, from E-Rate eligibility to portions of the Elementary and Secondary Education Act (ESEA).

A Host of Opportunities

Against this backdrop, a clear vision of the way forward has emerged. Schools become a constantly connected, on-demand 24/7 learning environment, unifying school, home, and knowledge/information resources like libraries. School administrations can quickly recognize and propagate best practices for everything from instructional techniques and classroom materials to teacher/parent interaction. There will be no exclusion of physically or geographically challenged communities. And these technology- and information-based capabilities will give school administrators the flexibility to quickly and easily address regulatory compliance as requirements change.

The benefits of such a connected and accelerated learning environment include:

- Improved learning and comprehension
- Maximum utilization of valuable teaching resources
- Lower cost of curriculum development and distribution
- Lower cost of administrative duplication (through centralization of IT and electronic resources)
- More uniform services delivery across geographies

The technology components of the 21st Century Classroom include:

- High-speed network connections
- Datacenters
- Web 2.0 presence and functionality

  - Sophisticated school sites that supplement/replace paper-based information and outbound communications
  - Online forms that simplify administrative operations; cut costs and waste
- External/third-party services providers
  - Academic content, inc. websites, streamed live and on-demand video
  - Web-based on-demand administrative applications
  - Web-based student-teacher, parent-teacher, and parent-school shared information portals

Gray Clouds in the Blue Sky

Of course, integrating the information resources and communications systems of the school population with the wider community raises a number of security considerations. First and foremost, enabling a larger and more sophisticated user population will naturally produce more potential threats. These threats include:

- External access to critical systems can be exploited by student hackers and other malicious or mischievous "script kiddies" with sufficient computer coding skills to execute dangerous programs on school systems.
- Integrated systems are vulnerable to internal compromise by unsophisticated users or exploitation by unauthorized or disgruntled personnel. Valuable files can be stolen, corrupted, or destroyed.
- Streamed and rich media content impacts bandwidth, consuming valuable network capacity and taking priority over all other traffic, so systems seem less responsive.
- "Dirty" laptops and mobile devices from outside can get on the network, introducing all kinds of viruses and other malware.
- Objectionable content or usage—including illegal file-sharing—over school systems can violate laws and regulations, and expose districts to liability civil issues.

There are two general areas where information security issues converge:

- Datacenter protection
  - Traditionally, intrusion prevention has been the focus of attention here. But, as centralized data assets become more critical to distributed organizations and attacks become more sophisticated, administrators are forced to look beyond simply "blocking the exits."
  - Denial of Service (DoS) attacks have slowly but steadily become a constant threat to core network assets and operations. This is because knowledge and even the code to launch such attacks continues to be disseminated, and because the networks of remotely controlled "bot zombie" computers required for such attacks continue to grow.
- Endpoint and access control
  - Laptops moving in and out of LAN are the most dramatic disruptors to the concept of a "network perimeter." With initiatives to provide every student their own system, these can bring with them all the threats that administrators try so hard to block. And, naturally, they can be a particularly dangerous platform for deliberately malicious activities.
  - Remote access is a variant of the issues administrators have with laptops. While the remote access population is less fluid, their machines are just as susceptible to infections or misuse.
  - With email quickly becoming a dominant form of communication, malicious attachments and "social engineering" attacks (tricking people to open the attachments) represents a persistent threat.
  - Web-connected publicly accessible systems—like those in libraries—can be inlets for malicious code and files. These can also be used for policy violations, especially regarding objectionable or illegal content, which can expose schools to liability issues.
  - Wireless access is vulnerable to its own kind of hacking, being penetrated by systems not physically attached to the network. Outbound traffic and communications transiting the wireless network can also be re-directed to phishing sites. Or the communications can be wirelessly hijacked altogether and stolen like any other information asset. The installation of rogue access points by thoughtless or seemingly enterprising staff can open up the network to all these problems, compounded by a lack of management control.
  - G3 smart phones using IP are an emerging threat when students use the wireless infrastructure to interact with web content of all kinds. These represent handheld versions of many of the threats—both technical and legal—posed by common computer browsers.

Unlike the old paradigm of “school hours,” the new school / instructor / student / parent interaction matrix virtually never sleeps or takes weekends off. This places 24 / 7 / 365 security demands on a district’s IT infrastructure. This need can be best addressed by consolidating and centralizing the security infrastructure, making it easier to maintain, monitor and manage.

The benefits of network security consolidation include:

- Simplified management, with attendant lower costs in equipment and administrator time
- Gap prevention: Consolidation means fewer potential points of failure and reducing or eliminating conflicts between various hardware and software combinations.
- Regulatory compliance: A centralized security operation with a management console means policies can be promulgated and enforced quickly and uniformly. These systems also simplify the auditing and reporting operations required by many regulatory regimes.

Addressing Security

The core task of any security deployment is protecting the organization’s information assets and the systems that transfer and store them. These threats fall into two main categories: Directed and Automated.

Directed threats are individualized activities targeting specific organizations or assets. They include:

- Hacking and other forms of manual intrusion. Students records are a common example of the target of such attacks, with the intent of changing or corrupting the records or stealing private personal information.
- Directed Denial of Service (DDoS) attacks flood web servers—including email servers—with millions of robotically generated requests in an attempt to “bring the site down.” These are pure acts of vandalism perpetrated in anger.
- Access to assets in violation of policies: Whether accidental or deliberate, these are “inside jobs” where people exceed their permissions to access information.

A solid firewall solution will address the first two threats, which are well-recognized security issues. Because both hacking and DDoS activities have conspicuous and distinctive profiles, they can be recognized and countered.

A more sophisticated solution is needed to counter the “inside” activity since it can otherwise appear normal to security equipment. A Unified Threat Management appliance serves as a firewall against external attacks. And it can run content filtering and policy enforcement software that will recognize network activity that violate policies or permissions, shut the activity down, and report the incident.

Automated threats, as the name suggests, are run automatically and indiscriminately, usually in large waves.

- Viruses and worms are the oldest and most familiar of these threats. They are programmed to disrupt and disable system for no other purpose than vandalism.
- Trojan Horses and bots (including spyware and keyloggers) are designed for automated theft—of personal information, or of a computer’s functionality for use in spamming operations or other automated crime.
- Spam is another familiar threat. It is an obvious nuisance or even a violation on content laws on its own. And it can be a transmitter for other, more sinister software like viruses and bots. It can also be one component of a multi-pronged attack that includes a phishing back-end website that tricks users into divulging passwords, account numbers and other valuable information, or “drive-by download” sites that “inject” any visitor with malicious software.
- Wireless scanning is automated only to the extent that an individual indiscriminately looks in a specific geography for open wireless networks to penetrate or pirate.

All software-based automated threats have identifying signatures that can be countered by security software.

Spam poses a slightly different challenge: It may have certain characteristics that identify it as “likely” spam. But it usually requires more sophisticated analysis to increase the success of catching true spam and decrease the “false positives” that block legitimate messages. This can be accomplished by an email-specific security solution. However, because spam is so frequently just one element of a more complex attack, spam filters need to be integrated with anti-virus, anti-spyware and anti-phishing operations to provide complete protection. Again, a Unified Threat Management platform—running all the necessary software components—can address the total threat as well as minimizing any delays or disruption of overall network traffic.

A less obvious threat to district assets is ***bandwidth piracy***. Because Internet access is so integral to school operations, its value as a school asset can almost be taken for granted, like water or electricity. Yet non-essential applications that consume more than their fair share of network bandwidth are the equivalent of having someone siphon off the district's water supply or tap the electricity. Such applications include:

- *Streaming media*—like video and audio—that not only use large amounts of available bandwidth, but get priority over traffic like email. When users stream entertainment content or transfer large files—like images—they are using a school resource for personal purposes, either deliberately or inadvertently. But the cost to the school district can add up quickly.
- *File-sharing* represents a double threat to school districts. Not only does it consume a great deal of bandwidth. But such activity frequently violates intellectual property laws and the Terms of Service of ISPs. In both those cases, there can be legal liability to the schools.

Bandwidth piracy can be addressed by a combination of ***content filtering*** and *application-layer filtering*. Content filtering supplies high-level protection against access to certain file types and websites. Application-layer protection goes much deeper to analyze the specific application type being used. This can distinguish between the "good" video that a school might use for instruction and the "bad" video that students might access strictly for entertainment. What's more application-layer filtering avoids shutting down whole sections of the network when a violation is detected. That's because content filters alone tend only to block the offending network traffic and, in the process, shut down an entire section of the network. Application-layer filtering enables blocking only the offending application so the rest of the traffic can move uninterrupted.

Since the ultimate goal of these technologies is to assure maximum available network bandwidth for school business, the faster and less disruptive the filtering technology, the better. By consolidating the filters in a Unified Threat Management appliance, and using the fastest scanning systems available, schools can reclaim large amounts of valuable network capacity. In fact, a fast UTM device can eliminate the need for single-purpose bandwidth accelerators that just mask the problem and don't solve it.

Security Consolidation

Just as there is a move to consolidate information assets, so there is a move to consolidate their protection. The advantages of this approach include:

- Reducing the amount of costly hardware required for effective security
- Simplifying systems management, to reduce demands on IT staff and time
- Gaining comprehensive view of network endpoints and activity for improved security and oversight
- Enabling uniform policy enforcement across the entire district, not just school by school or device by device

At the core of security consolidation is a view of security appliances as services platforms. Instead of buying and managing a different piece of hardware for each type of threat, a Unified Threat Management appliance is a multi-purpose device that can run applications that address those threats. By processing traffic once, overall network is accelerated, further eliminating the need for acceleration equipment.

Security consolidation also provides benefits to school administrators. By reducing the amount of equipment and addressing evolving threats through predictable routine software subscriptions, school administrators can:

- Lower overall costs and simplify budgeting
- Simplify the audits of network security performance, including event logs and forensics
- Simplify planning and rationalize purchasing
- Minimize provisioning time and expense

Information Security Solutions

How much security you need—and what kind—is driven by the complexity of the area you're trying to protect. *Classroom.* The simplest environment, security is addressed at the individual user level with each connection to the rest of the facility secured:

- *Client anti-virus/anti-malware*
  Managed and maintained from a central unified threat management (UTM) system; to simplify client protection maintenance, reduce demands on personnel time and expense.
- *Secure wireless*
  Enables connectivity for students as well as district-owned assets, while cutting wiring costs and allowing for maximum flexibility.
- *Unified Threat Management*
  Technically, a campus asset, but an essential component of a reduced expense and simplified management solution to Client system protection.

Campus. A logical extension of the necessary basic protections:

- *Unified Threat Management*
  Consolidating all network traffic protections on a single device cuts operating expenses while assuring no gaps in protection. These protections include: gateway anti-virus and anti-malware; client anti-virus and anti-malware maintenance; intrusion protection; and content filtering.
- *Secure wireless*
  Enables connectivity for students, and mobile staff, as well as district-owned assets, while cutting wiring costs and allowing for maximum flexibility. Ideally, these access points integrate with the UTM system for total network "awareness" inside and outside the perimeter.
- *Email filtering*
  One of the most vulnerable entry points for potential threats, email calls for distinct protection to assure comprehensive defense against malicious attachments as well as phishing scams.

District. A network of properly secured campuses can be safely connected with a few additional measures:

- *SSL-VPN*
  The lowest cost and most manageable way to connect a district. This can embrace all the campuses, enable access from home, as well as connect remote and mobile users.
- *A global management system*
  By gaining network visibility and control from a single physical location, districts can cut overall administrative costs, more quickly and precisely identify security gaps, and conduct forensics on any incidents. These systems also simplify audits in compliance with any regulatory reporting requirements.

By breaking security zones into these logical divisions, provisioning and implementation can be addressed according budgets and schedules set by overall management policy.

Implementation Scenario Diagrams

- Classroom
- Campus
- Multi-campus district