Higher education solution brief

Securing information in higher education organizations

The explosive adoption of technology in higher education has changed the network as we know it. The perimeter has disappeared along with traditional ways of interacting with applications. This is the result of many trends and technologies including:

- Universal use of mobile computers, plus other network-attached devices like handhelds and mobile phones
- Remote user access to information resources
- Centralization of data centers to support more diverse access
- The deliberate move to cloud computing and cloud storage
- Use of Web 2.0 functionality that both accesses and generates stored data

All of this has led to a dramatic increase of security challenges however the strategies and tactics to address them are less apparent.

This is especially the case when an institution's IT budget is allocated between different schools, campuses, and even departments. While this budget distribution provides resources to tailor security solutions on the "front lines," it can adversely impact IT's ability to address the increasing amount of vulnerabilities.

Different populations. different needs. The same equipment.

The first level of simplification at most schools is to split the user population between students, faculty and administration.

First, staff is likelier to share geographical proximity. From an architecture standpoint, this is more traditional and therefore easier to provision. Adding SSL VPN access to such a topology is a conventional solution for enabling remote access to network resources.

Also, it is assumed that staff is closer to more valuable and proprietary assets. That is why they need to be addressed first. This fact also helps prioritize initiatives as well as budget allocation.

The use of networked electronic educational resources—many supplied by third-parties—introduces a new consideration in what represents "faculty" capabilities.

Key technologies now used extensively for teaching are podcasts, online social networks, smart boards and other Web 2.0 tools, all integrated with enterprise-level learning management systems to provide seamless access to online learning. Major applications and tools include:

- Learning management systems
- Anti-plagiarism tools
- Social bookmarking applications
- Assessments tools
- Online exam applications
- Content creation
- Student information and notification systems

Networked classroom technology includes smartboards, wireless projectors, and PCs as fully functional endpoints or as primary-purpose "terminals."

From a policy standpoint, it is easier to promulgate and enforce safe system practices among "invested" populations like staff and faculty. Students simply have less at stake. Students are also arriving with network usage habits engrained over years. So policy must be enforced automatically.

Forecast: cloudy

Another dynamic with major implications for information security is the move to cloud computing. This can include:

- Cloud-based applications
- Cloud storage; accessing and saving back to storage facilities in geographically distributed locations
- Distributed processing

This move to extending infrastructure beyond the enterprise perimeter means traffic handling becomes more critical. The integrity of data has an even slimmer margin for error. New bandwidth-hungry applications are being used on a consistent basis slowing down the performance of the network and access to mission-critical applications. Traffic throughputs and bandwidth must be maintained or even accelerated. This is then multiplied by the number of emerging rich applications and potential endpoints.

To secure such an environment requires high-speed systems that can perform inspections in real-time. Old port blocking and store-and-forward techniques are simply not up to the task.

Additionally, strategies then employ site blocking and bandwidth-shaping can discourage or completely thwart the recreational use of secure networks. But such a strategy must be employed with a proper sensitivity to the total user experience. Impinging too much on the student population's quality of life can adversely affect the productivity, efficiencies and have a negative affect on the profile of the institution. As a starting point, the surest guidance in this area is the bright line of what is legally acceptable. People might want to share movies. But if the law doesn't permit it, there can be no argument about the appropriateness of blocking the activity.

Identifying "hot spots"

Certain assets and operations are universally recognized as essential and demand the most robust security possible:

- Finance, including financial aid
- Medical records
- Proprietary data sets (research, student records, etc.)

These are usually accounted for in the basic network architecture. As the security infrastructure evolves, it is wise to account for these assets first. To the extent they are increasingly critical in distributed operations (like Web 2.0 self-service functionality), meeting the dual objectives of absolute security and ease of access requires special attention and a high degree of planning. Data Leakage Prevention capabilities are now integrated with firewalls and email security solutions so ensure that this is considered when evaluating technology.

Regulatory compliance, naturally

With the promulgation of private and public information security regulations, it's easy to imagine these as an obvious starting point for an information security strategy. They may include:

- CIPA (Children's Internet Protection Act), which nonetheless applies to higher education facilities
- HIPAA (Health Insurance Portability and Accountability Act) applies to student medical records
- FIPS, FISMA, Common Criteria and other relevant regimes for those institutions providing services to the Federal Government under contract

However, most regulations are designed to represent the "invisible party" in electronic interactions: say, the customer in a company's network or the patient in a healthcare system. In Higher Ed, all users are stakeholders in the institution, whether faculty, staff, or student. So regulations are practically "in the DNA" of IT managers at educational institutions.

Adapting to changes in the regulations may sometimes inspire IT managers to re-examine their solutions. But rarely will it affect strategy or purchase criteria.

Teaming up

Because of the unique considerations in network usage at Higher Ed institutions, IT managers are increasingly subscribing to knowledge- and strategy-sharing organizations.

The EDUCAUSE Cybersecurity Initiative website, developed by the EDUCAUSE/Internet2 Higher Education Information Security Council (formerly the Security Task Force), is intended to be a focal point of information and resources on cybersecurity for the higher education community.

EDUCAUSE programs help navigate the challenges involved in advancing higher education with IT through applied research, data benchmarking, and programs addressing advanced networking, policy, security, and teaching and learning. Three of these initiatives—the EDUCAUSE Center for Applied Research, the EDUCAUSE Learning Initiative, and Net@EDU—are fee-based programs offering member or subscriber-only products and services, although many of their resources are publicly available.

The EDUCAUSE Center for Applied Research (ECAR) provides timely research and analysis to help higher education leaders make better decisions about information technology. ECAR assembles leading scholars, practitioners, researchers, and analysts to focus on issues of critical importance to higher education, many of which carry increasingly complicated and consequential implications. ECAR provides educational leaders with high-quality, well-researched, timely information to support institutional decision-making.

The EDUCAUSE Learning Initiative (ELI), is a community of institutions, organizations, and corporations committed to advancing learning through IT innovation. ELI achieves this mission through a strategic focus on learners, learning principles and practices, and learning technologies.

Net@EDU members work together and with industry and the federal government to understand, forecast, and shape these developments to best support the evolving needs of higher education. Net@EDU also serves as a national center for research and advocacy in network policy issues and provides information and recommendations on how colleges and universities can impact current business models, political initiatives, and mergers. Current Net@EDU working group topics include campus cyberinfrastructure, converged communications, and state education networks.

In addition, the Core Data Service is a web-based interactive database, based on an annual survey, that compares institutional IT environments and practices to help benchmark, plan for, and make decisions about IT on campus.

Distributed security for distributed institutions

Given all the constituencies and different levels of security required, Higher Education demands an intelligent,

flexible security system that can be managed centrally. The old notion of a perimeter must be replaced with the inverted network approach, secured by gateways. This includes IP, WAN and LAN ports, plus secure wireless access. SSL VPN technology must be implemented to ensure staff productivity when offsite and IPSec solutions used for site to site networking. If the network includes remote users, SSL VPN is a must.

Security can be pushed further, out to the endpoints of systems managed by the institution. This requires intelligent gateways that can recognize the secured devices, perform automated maintenance and, again, be centrally managed.

Dell SonicWALL and higher ed

Dell™ SonicWALL™ capabilities align with Higher Education security and user experience requirements and include the following:

- Secure network traffic controls
- Secure remote access
- Secure wireless
- Email filtering and anti-spam
- Identifying and addressing network vulnerabilities

Secure network traffic controls

Dell SonicWALL's firewall gateway appliances provide institutions with high-performance full Deep Packet Inspection for a secure network free from viruses and other malware. Unauthorized access to a university network could jeopardize day-to-day operations. The firewall provides the first line of defense against Internet security attacks of all types. Additionally, institutions can utilize advanced application intelligence and control features to ensure that bandwidth is properly utilized by throttling down peer-to-peer and video traffic while prioritizing access to education related applications. This can all be done automatically at the application layer, removing the burden of hunting for ports and protocols, thus freeing up IT administrative resources.

The Dell SonicWALL E-Class Network Security Appliance (NSA) Series is engineered to drive down administrative complexity, while defending against the entire spectrum of network attacks, both externally and internally, with unprecedented speed. NSAs offer centralized management, network segmentation, multiple deployment options and advanced networking features for ultimate control and flexibility. Combining multi-core technology unrestricted deep packet inspection, and application intelligence and control, NSAs are the most scalable, reliable and highest performing multi-function full Deep Packet Inspection network security appliances in their class.

Secure remote access

With the profusion of internet accesses (xDSL, Wimax, cable, Satellite, new 4G, etc.) and the consumerization of IT devices (laptops, netbooks, smartphones, etc.) combined with heightened focus on remote access for disaster preparedness and business continuity, secure remote access is imperative to today's learning environment. But in order to increase productivity and reduce IT overhead, the successful solution must also be easy for both users and administrators. Dell SonicWALL E-Class Aventail™ Secure Remote Access appliances provide ease-of-deployment and usage plus unsurpassed levels of granular control and connection to a wide range of leading endpoint devices.

Secure wireless

Dell SonicWALL makes wireless networking secure, simple and affordable with the innovative Dell SonicWALL Clean Wireless Solution—the first total security solution that integrates 802.11n and 802.11a/b/g wireless management with best-in-class Next-Generation Firewall security and application control to provide application based policy control. The Dell SonicWALL Clean Wireless solution gives organizations, for the first time, the confidence that their wireless network is as secure and well managed as their wired network.

Email filtering

With increased sophistication and complexity of inbound email threats, organizations need a powerful, integrated, yet easy-to-use email security solution that can effectively prevent in-bound and out-bound email threats. Dell SonicWALL E-Class Email Security solutions deliver easy, powerful protection against spam, virus and phishing attacks, information leaks and violations of regulatory compliance laws.

Identifying and addressing network vulnerabilities

Geographically-distributed sites exacerbate the costs and challenges of enabling distributed learning with a minimal administrative learning curve. A Global Management System (GMS®) facilitates the management of Dell SonicWALL firewalls, backup and recovery, secure remote access, and email security appliances from a single location. GMS also allows the IT administrator to monitor his Dell SonicWALL infrastructure and create reports necessary to comply with information security regulations.

The Dell SonicWALL Global Management System provides centralized policy-based network security management, active monitoring and reporting, that can scale up to thousands of locations. Dell SonicWALL's management and reporting solutions provide a comprehensive architecture for centrally creating and managing security policies, providing real-time network monitoring and event logging, and delivering intuitive compliance and usage reports, all from a single management interface. Customers may use GMS either on a third party Windows-based server or on the Dell SonicWALL Universal Management Appliance.

DELL SonicWALL