Securing Higher-Ed Networks in a Complex IT Environment

March 2013

Sponsored By:

Symantec

CAMPUS TECHNOLOGY

Table of Contents

IT's Difficult Balancing Act 2

Develop and Enforce IT Policies 2

Simplify User Authentication 3

Safeguard Confidential Information 3

Manage the Infrastructure 4

Protect Computing Infrastructure and Data in the Cloud 4

About Us 6

IT's Difficult Balancing Act

It's an exciting time in higher education where technology is enhancing the learning process. Courseware is now available 24 hours a day, seven days a week in a variety of formats, including PowerPoint presentations, short video clips, and interactive exercises. Teachers are beginning to leverage technologies, such as online classes and digital textbooks. The result is information exchanges are richer, learning is deeper, and the results more noteworthy.

This deluge of data, however, is presenting new challenges for campus IT departments. Seventy-seven percent of organizations have seen the complexity of their IT infrastructure increase over the last two years, according to research compiled by Symantec.One factor is the growing flexibility that IT departments provide to users. User-owned devices account for a number of keyloggers, viruses, and other types of malicious software that have destroyed data and compromised system integrity on college and university campuses.Such problems are quite common: nearly 80 percent of schools have experienced two or more data breaches, according to Symantec.

Academic IT departments need security and management tools that work in the current infrastructure and protect confidential individual and college information. These products must be cost effective, easy to use, and support both traditional as well as online learning applications in a secure manner. To be effective, such tools must:

1. Develop and enforce IT policies
2. Simplify user authentication
3. Safeguard confidential information
4. Manage the infrastructure
5. Protect the computing infrastructure and data in the cloud

In this custom white paper, sponsored by Symantec, Campus Technology outlines a 5-point plan for creating a secure network, within your existing environment, that enables you to meet the academic needs of your students and faculty. See how Temple University is using this plan--with solutions from Symantec--to protect its network and data while providing students with the learning tools they need to be successful.

Develop and Enforce IT Policies

IT policy is the key to managing risk and maintaining compliance in today's higher-ed environment. Effective policy should support the objective of the institution and identify critical assets, potential vulnerabilities, and consequences in the event of a network or system breach.

Once policy is in place, institutions need tools that will enforce these guidelines and safeguard its data assets. Symantec Control Compliance Suite for Governance, Risk and Compliance can help. The software is designed to group IT assets and virtual

Securing the Network at Temple University

Like most higher education institutions,Temple University faces significant challenges in protecting its data and needs a wide range of tools to monitor and secure information. While a number of vendors offer small pieces of the puzzle, Temple has found working with a vendor with a complete set of solutions as a better option.

"We have been using Symantec solutions for a decade, starting out with anti-virus software and gradually branching out with endpoint protection, encryption, and data backup," said Shestack.

Another advantage, notes Shestack, is the products' ability to scale as the university's needs evolve. "We reevaluate our security selections every three years when it is time to renew our contracts," said Shestack. "While other vendors have developed strong products, we have found that Symantec offers solutions that have been able to grow with us as our needs have changed."

Founded in 1884, Temple University, located in Philadelphia, is a public research institution with more than 35,000 students. Attendees are enrolled in 125 undergraduate, 113 masters, and 52 doctoral programs on its urban campus. Temple University, which supports 17 schools and colleges on nine campuses, is the nation's 28th largest university with world-renowned programs in medicine, law, and public policy.

assets, so a school understands and can manage the risks associated with its computer systems. IT managers can better define risk thresholds and develop models for the most efficient ways to reduce them. They then can monitor their work in an ongoing fashion and protect their schools against any potential compliance breaches.

Simplify User Authentication

A growing number of institutions are moving beyond Virtual Private Network, network access IDs, and passwords to authenticate users. Two-factor authentication relies on something users know—such as a password—as well as something they are given, such as a software token. This second check makes it more difficult for hackers to break into a campus network. The VeriSign Identity Protection, or VIP solution, is a shared, cloud-based two-factor authentication solution that offers a variety of credential choices.

The BYOD movement has garnered a great deal of momentum because of the growing popularity of smartphones and tablets. Employees, faculty, and students are using their smartphones, laptops, and tablets to conduct research, take tests, and collaborate on assignments. Symantec Mobile Management provides strong policy management across the widest range of mobile platforms. Centralized control, user enrollment, configuration management, application distribution, and helpdesk management highlight the solution's features. In addition to Mobile Management, Symantec's mobility portfolio secures remote access using strong authentication and helps to protect sensitive information using encryption, data loss prevention solutions, and anti-malware products.

Furthermore, the Symantec Fraud Detection Service is a risk-based authentication, a software-based detection solution that enables organizations to determine and intervene in fraudulent transactions in real time. This solution can be effective in preventing mobile devices from conducting bogus transactions on academic networks.

Safeguard Confidential Information

Campus networks house a wide and ever changing array of information. Schools must protect this data or risk losing funding. They should also look to leverage data loss prevention capabilities to avoid the possibility of confidential student information leaving the network, or being copied to a USB or DVD. A smart security strategy includes policies and tools that restrict access to this data and guards it as it's transmitted from place to place.

Encryption is a key element in Temple's strategy. The university uses Symantec PGP for Encryption, which delivers encryption functions at different points: individual PC files, PC folders, and e-mail transactions. Data is encrypted as it travels from source to destination throughout the campus network. In addition, the university encrypts all of the data stored on laptop disk drives for employees known to work with confidential information, such as student data and Human Resource information.

Once a university deploys an encryption system, it needs software to manage the Public Key Infrastructure, which is responsible for issuing digital certificates, providing strong authentication, and encrypting data. Temple relies on Symantec solutions to perform this task.

In addition to encrypting sensitive information, schools must ensure that data is recoverable if a system problem arises. To guard against such problems, Temple uses Symantec System Recovery 2013, a backup and disaster recovery services solution for Windows servers. In the event of a system failure, IT administrators can rapidly restore whatever information they need, including entire physical and virtual machines to bare metal as well as files, folders, and granular application objects. The Symantec System Recovery 2013 solution also provides cross-platform physical-to-virtual (P2V), virtual-to-virtual (V2V) and virtual-to-physical (V2P) recoveries.

Manage the Infrastructure

With networks expanding, IT staff needs tools that automate manual tasks. The Symantec Altiris IT Management Suite provides comprehensive client, server, and asset management with full service desk and automation capabilities. The suite delivers visibility into IT assets, facilitates license compliance, and automates complex management tasks, such as operating system migrations. The system performs an inventory of existing licenses; matches installed software against contracts; reviews relationships among software assets and their owners; measures actual usage; determines license requirements; reassigns existing licenses or procures new ones, if necessary; and then delivers the requested software to users.

The above tools included with Symantec Altiris IT Management Suite allows the IT organization to create the virtual command center, should also be extensible to embrace mobility

Protect the Computing Infrastructure and Data in the Cloud

Safeguarding the network is a top priority for campus IT departments. Yet a growing move towards BYOD has made it difficult for IT organizations to secure their campus infrastructures, especially as assets become more dispersed. IT staff needs visibility into users' systems, ability to update outdated operating systems, or close a potential opening to malicious code. Without such visibility, malware can run amok.

Temple University experienced such problems in 2003. Adware and spyware from student computers attacked systems on the school's wireless network, knocking servers offline and shutting down segments of the network. While the virus attack was certainly an issue, the bigger challenge, said Seth Shestack, Temple's associate director of information security, was the fact that IT had little ability to control the real source of the problem: student-owned devices.

Where to Start?

Need a new security plan but aren't sure how to get started? Symantec can help.

The Symantec approach starts with a Pre-Assessment questionnaire, which helps give a complete picture of your institution's IT environment. The document outlines your school's central asset management strategy, environment (nodes, OS, topology), and service availability (SLA, RPO, RTO). The feedback from this survey will provide the foundation for building a new security infrastructure.

Next, Symantec conducts a one- to two-day onsite assessment of your school's IT infrastructure. This no-charge assessment analyzes current state review (applications, infrastructure, devices, users); business and technical requirements (future state requirements and initiatives), and conceptual architecture discussion (architecture adjustments, approach and prioritization). The goal is to determine not only the current state of your infrastructure, but also to anticipate future needs.

After completing the assessment process, Symantec compiles the results into an Assessment Analysis Document. This comprehensive, detailed report includes an executive summary,current and future state analysis; and recommended strategy and next steps.

Now armed with this information, you have a complete view of what is happening with your school's systems. You will know not only what is occurring, but also what the future will bring. With this information, you can then make smart purchasing decisionstoensure that your systems and information will bewell protected.

"As an academic institution, we have to support the culture of openness that is vital for higher education," noted Temple University's Shestack. "As a result, we have little control over student-owned computers, but yet we have to grant them full access to the university network."

Temple set out to find a new security system that would better guard its network and stop illegal behavior. The university opted for Symantec Endpoint Protection suite, an end-to-end solution that provides virus and spyware protection, a desktop firewall, intrusion prevention, and device control technologies, all through a single agent. Now, when any machine logs onto the school's network, the solution runs the latest antivirus definitions, examines programs as they run, identifies potential problems, and stops malicious behavior of both known and even unknown threats. The system ensures that all machines are fully compliant with the school's security policies.

The school is also using the Symantec suite to combat illegal downloads and peer-to-peer file sharing violations, another common security problem for colleges and universities. Violations of copyright law can affect an institution's reputation and put it at risk for legal action. Temple also relies on the Symantec Mail Security for Exchange not only to stop virus attacks targeted at the campus e-mail system, but also to reduce any peer-to-peer file sharing violations.

Protecting the network has become a simpler, more manageable task for Temple's IT managers and staff. IT administrators manage the environment with a single sign-on and a web console, which provides them with robust configuration management and reporting capability. A consolidated dashboard delivers quick and easy-to-follow views into what is happening with any network or system resource.

Moving information to the cloud adds another layer of complexity to a university's network. The threats from malicious software remain—and even grow—as information moves off site. As a result, schools need to develop new business processes, so they can take advantage of the on-demand services that cloud providers deliver. Universities still must protect information, make appropriate use of their resources, and ensure system compliance.

Symantec O3 is a cloud information protection platform that provides three layers of protection for the cloud: identity and access control; information security; and information management. The product delivers a context-aware, policy-driven layer of protection to cloud users, applications, and information.

Symantec Virtual Workspace supports virtual e-learning labs. The solution offers single sign-on, application auto launch, roaming with state persistence, location awareness and proximity printing, so users gain a consistent experience whether working locally or remotely.

About Us

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

For more information, visit our website: www.symantec.com

About Campus Technology

The only monthly publication focusing exclusively on the use of technology across all areas of higher education, Campus Technology provides in-depth coverage of specific technologies and their implementations, including wireless networks and mobile devices; enterprise resource planning; eLearning and course management systems; "smart classroom" technologies; telecom, web, and security solutions—all the important issues and trends for campus IT decision makers. Targeting administrators, IT professionals and tech-savvy faculty, Campus Technology provides direction, analysis and detailed coverage of emerging technologies to assist technology leaders in their specific roles on campus.

To learn more, visit www.campustechnology.com.

350 Ellis Street
Mountain View, CA 94043
650-527-8000
www.symantec.com

CAMPUS TECHNOLOGY

9201 Oakdale Ave.
Suite 101
Chatsworth, CA 91311

(818) 814-5277