



Temple University Offers a Lesson in Information Security

Benefits Offered by Symantec AntiVirus Corporate Edition

- Prevented a single system within Temple's comprehensive network from being infected by SoBig and MyDoom
- Protects against new and emerging threats
- Performs scheduled scans and automatic updates
- Helps ensure safe learning environment

Temple University is one of the largest public universities in the U.S., with only four information security employees, yet its network was not infected by the SoBig and MyDoom worms that brought countless corporations and academic institutions to their knees. Its extraordinary success is the result of the University's ongoing efforts and lessons learned in combining people, processes, and technology to protect students and University assets without compromising academic freedom.

The Challenge

Until September 2002, computer security at Temple University in Philadelphia was limited to securing mainframes and providing disaster recovery. However, as information security threats increasingly focused on the Internet and networked systems, and as federal laws were passed requiring greater network security for public and private organizations, the University—led by Temple's vice president for computer and information systems—made the unusual decision to designate a chief information security officer, or CISO. Ariel Silverstone, with over 15 years in the computer industry and experience consulting nationally and internationally for Fortune 1000 firms, was appointed to the role.

For Temple, having a CISO on board was a significant prerequisite for implementing a proactive security infrastructure that would enable the University to address complex information security threats that inevitably become more pervasive and destructive over time. This was even more important since Temple University has over 10,000 employees; 33,000 students; 14,000 networked PCs; and a hybrid wired/wireless network—and just four information security (IS) employees

The Solution

Under Silverstone's direction, and with input from a security roundtable consisting of various University constituencies, the information security team developed and implemented a comprehensive computer and network security policy. This policy established appropriate security requirements and restrictions on accessing and using University computers, computer systems, and networks and safeguarding University information.

Among other responsibilities, users of Temple computers, systems and networks are explicitly accountable for understanding and complying with the university's information-security policies and for demonstrating due diligence in protecting the integrity and privacy of data therein. They are also tasked with ensuring the local security of any system they use to connect to the University network and of reporting security lapses to the CISO or system administrator.



Creating a culture of security

The scarcity of professional IT support resources and the abundance of employees and students requiring support led the Temple IS team to make another important decision: to enlist the help of students and faculty in protecting information resources by creating a culture of security. With each individual user following best practices for information security, Temple can head off many potential problems.

The IS team implemented an awareness campaign with posters, customized candy dispensers, and other popular paraphernalia promoting safe computing. It installed plasma screens at popular gathering places and played information-security focused infomercials. It also launched a series of seminars covering IT and related issues, including security. The team started small, offering just two classes in order to gauge students' interest in attending non-credit classes on their own time. The classes were so successful that a variety of seminars are now offered at the beginning of every semester, with a growing number of these classes targeting security issues.

Supporting awareness with technology

The IS team backed up its awareness campaign with technology, providing students with a standardized antivirus solution at no cost. Symantec AntiVirus™ Corporate Edition was made available to students via CDs and downloads from the University's Web site. The IS department also set aside certain days during which students could bring their laptops in and the IT staff would install the antivirus software for them. In addition, for a nominal fee, students could purchase a copy of the software for home use. University IT personnel managed the configuration, verification, and updating of the antivirus software, thereby assuring that users were appropriately protected against new and emerging threats.

Furthermore, only users with updated, properly configured antivirus software were allowed to connect to the school's network. Unprotected devices were automatically identified as they attempt to connect to the network and prohibited from connecting. The IS team sent consultants to check the unprotected or misconfigured systems to make sure Symantec's antivirus software was installed correctly.



Temple University security put to the test

Even as the University made significant progress toward securing the information and systems of students, faculty and staff, the information-security team's efforts were challenged during the summer of 2003.

In July, a security bulletin was released describing a major vulnerability in the Windows operating system. Just one day later, Temple's IS team assessed the threat as easy to exploit and widespread, in turn deciding that it was a critical issue that had to be addressed. In response, Silverstone's team issued a campus-wide e-mail message to 55,000 recipients, warning people to update Windows immediately.

Less than a month later, the Blaster blended threat hit the Temple University network. Blaster is a worm that targets the aforementioned vulnerability in Windows' implementation of Remote Procedure Calls. The worm then launches a denial-of-service attack against Web sites such as windowsupdate.com and can deluge a network it uses to facilitate its attacks. Within four hours of being detected within the Temple network, 600 unprotected computers were identified as infected, and the network was slowed to a snail's pace.

The IS team responded by dispatching all technical support representatives while also asking nearly 100 other employees to assist in fighting the worm. The University disconnected infected computers from the network. With fall semester move-in day fast approaching for 6,000 computer-laden students, the team accelerated its antivirus installation process for all students, faculty, and staff.

Customer Benefits

Because they had implemented a well-written security policy, had cultivated a more security-conscious environment, and had protection tools installed on many systems, Silverstone's team was able to minimize the impact of a potentially debilitating attack. The event did, however, impel Silverstone to accelerate the team's plans to install an effective antivirus solution campus-wide.

By November 2003, almost 90 percent of Temple's network-connected computers were protected with the University's standardized Symantec software, and nearly all were performing scheduled scans and were routinely and automatically updated. Furthermore, by January 2004, all but 0.1 percent of computers on Temple's network had the antivirus software installed and running. More importantly, by then, the SoBig and MyDoom worms, having grabbed international headlines with their impact, had come and gone at Temple University without causing a stir.

Today, Temple University's security team continues to enforce its information security policies while helping students, faculty, and staff participate in maintaining a security-aware culture. By leveraging technology tools and information security best practices, the University is able to provide a safe environment for learning and discovery.

"The SoBig and MyDoom worms did not infect a single system on our University's comprehensive network. Temple's security infrastructure is also saving big money and significant resources. During the last six months, the University saved an estimated \$25 million by eliminating the cost of 1,300 service calls per day over the course of 200 days." – Ariel Silverstone, Temple University CISO



About Symantec

Symantec, the world leader in Internet security technology, provides a broad range of content and network security software and appliance solutions to individuals, enterprises and service providers. The company is a leading provider of virus protection, firewall and virtual private network, vulnerability assessment, intrusion prevention, Internet content and email filtering, and remote management technologies and security services to enterprises and service providers around the world. Headquartered in Cupertino, Calif., Symantec has worldwide operations in 38 countries.

For more information, please visit www.symantec.com

WORLD HEADQUARTERS

20330 Stevens Creek Blvd.
Cupertino, CA 95014 U.S.A.
408 517 8000
800 721 3934

www.symantec.com

For Product Information
In the U.S., call toll-free
800 745 6054.

Symantec has worldwide
operations in 38 countries.
For specific country offices
and contact numbers
please visit our Web site.