Toward A Virus-Free Campus

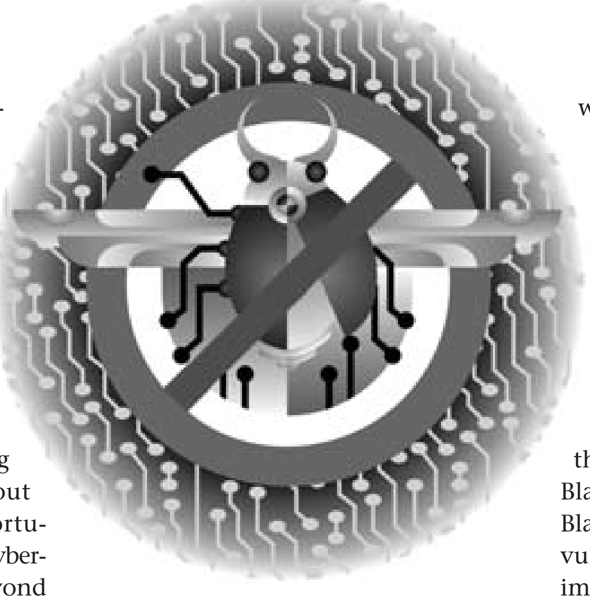
Temple University's IT staff created a campus-wide culture of awareness to mitigate security threats

By **Ariel Silverstone**

The latest proliferation of Internet threats has been felt around the world, by both public- and private-sector organizations. Academic institutions are no exception. Many who have been infected with viruses have had little choice but to shut down mail servers and start painstaking, costly clean-up procedures.

In academic settings, battling Internet threats and coming out unscathed is uncommon. Unfortunately, on many college campuses cybersecurity concerns rarely extend beyond the IT staff and are addressed in a disparate, ad-hoc fashion. Recent virus outbreaks have shown that users continue to open attachments from unknown senders, forget to update security software, or fail to apply vendor-supplied patches to operating systems and applications.

Yet, while many universities and large corporations were hit hard by the recent NetSky and Sasser worms, fewer than 60 of the 14,000 computers on Temple University's comprehensive network were affected. Not only is the network protected, but Temple's security infrastructure also saves the university significant money and resources. This success results from the university's ongoing efforts to combine people, processes, and technology to form a comprehensive, targeted strategy that protects students and university assets without compromising academic freedom.



Security at Temple

Temple University is a public university in Philadelphia with 5,000 employees, 33,000 students, and a hybrid wired/wireless network. Just four information-security employees are tasked with keeping the university virus-free while protecting its information and resources.

Until recently, Temple did not have a comprehensive, holistic security plan in place. Before September 2002, computer security at Temple consisted of several extremely competent professionals in the network group, knowledgeable consultants at the desktop support group, and a cadre of computer security personnel whose main focus was securing the mainframes and providing disaster recovery.

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 recruited me to serve as Temple's first chief information security officer, or CISO. My first job was to create a comprehensive security program.

Our History

During the summer of 2003, before the security plan was fully in place, Blaster attacked the Temple network. Blaster is a worm that targets a known vulnerability in Microsoft Windows' implementation of remote procedure calls. The worm then launches a denial-of-service attack against Web sites and can cripple the network it uses to facilitate its attacks. Within four hours, 600 unprotected computers were identified as infected, and the Temple network slowed to a crawl. The worm inserted data into the Windows registry of targeted systems, installed an application, scheduled a denial-of-service attack against Microsoft's Windows update site, then attempted to infect other machines.

We responded by dispatching all available technical support representatives as well as nearly 100 other employees to assist in fighting the worm. At the same time, the university disconnected infected computers from the network. Our team's fast response helped us nip in the bud what could have been a debilitating attack. Nevertheless, this response cost us $500,000.

With fall semester move-in day fast

approaching, we faced the prospect of some 6,000 students returning to residence halls, bringing with them thousands of computers quite possibly infected with the Blaster worm or various computer viruses. We realized that we needed to act quickly to provide an effective deterrent to this and future attacks on our network.

The Plan

Under my direction, a task force was formed, comprising key members of the computer and information security group, the telecommunications group, and both the academic and administrative computer support groups. With input from a security roundtable consisting of a broad cross-section of university constituencies, we first focused on the development and implementation of a comprehensive computer and network security policy. This policy established appropriate security requirements and restrictions on the access and use of university computers, networks, and information.

The importance of an information security policy in a university setting cannot be overestimated. The security policy formalizes the university's philosophy and regulatory requirements for securing information assets. It specifies how the requirements apply to faculty, staff, and students and defines the security controls that must be employed and managed. It's not a substitute for risk management; rather, a sound information security policy is founded on good risk-management practices.

Without a formal information security policy, an organization is left to react to security events, putting out fires where possible but rarely preventing new flare-ups. Reactive security is costly in terms of both time and money, as scarce security personnel scramble in response to an attack only to spend days cleaning and rebuilding machines. Meanwhile, students, faculty, and staff must wait until the crisis passes and clean-up is complete.

A key aspect of Temple's policy is to hold its computer and network users explicitly accountable for understanding and complying with the policy and for demonstrating due diligence in protecting the integrity and privacy of university data. Users are responsible for the local security of any computer they connect to the university network and for reporting security lapses to the CISO or system administrator. This approach serves to notify each user of his or her role as an active participant in the overall plan to safeguard Temple's network, computers, and information resources.

Without a formal information security policy, an organization is left to react to security events, putting out fires where possible but rarely preventing new flare-ups.

Awareness and Training

Users are reportedly the weakest link in an information security defense. Whether at home, school, or work, computer users often inadvertently compromise the security of critical information and systems simply by neglecting to follow safe computing practices. All too often, the result is the spread of malicious code that takes down individual systems or entire networks, halts productivity, taxes already overburdened support resources, and puts confidential information at risk.

Our security team realized that we needed to enlist the help of students and faculty in protecting information resources by creating a culture of security that would, in essence, expand the security team to about 40,000 members. The computer and network security policy serves as a guide, directing each user to follow established best practices for information security. As a result, Temple avoids many potential problems.

Like most universities, we take pains not to monitor students' Web use or impose unreasonable restrictions on their access. We view the Internet as an extraordinary tool for enhancing education. At the same time, we are charged with ensuring that the university's resources are not involved in malicious attacks or other harmful online activities and that confidential school records remain protected.

Information is the key to building consensus for best practices among faculty and staff at Temple. More specifically, we believe

It is the right information
using the right forum
targeted at the right people
delivered at the right time.

We theorized that if students and faculty understood that failing to incorporate best practices into their daily computing activities would put their own data and systems in danger, compliance would be much more likely.

The awareness campaign model that we used is one that translates well to other universities. Even with the limited funding typical of most university programs, we were able to use a number of low-cost mechanisms to spread the message. Among them were specialty items such as candy dispensers, promotional elements such as posters and flyers, and informational messages through newsletters and Web sites—all reinforcing the same security-awareness slogan: "The Bug Stops Here!" We even broadcast information security infomercials on big-screen televisions situated in different lobbies and hot-spots around campus.

We also introduced non-credit classes covering IT issues, including security. Although interested students had to take the classes on their own time, and some courses extended for a full week, the classes filled up quickly. What's more, interest in the courses grew, requiring us to expand our offerings to meet increasing demands.

Our Security System

The computer services team at Temple, led by Vice President Tim O'Rourke, backed up the awareness campaign with technology, providing a standardized antivirus solution at no cost to students. After defining our needs in a requirements document, we conducted a through technical analysis of possible solutions (see the sidebar). As a result of this process, we chose Symantec AntiVirus Corporate Edition, which was made available to students via CDs and downloads from the university's Web site. We also set aside certain days when students could bring their laptops to university IT staff to 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, we announced that only users with updated, properly configured antivirus software would be allowed to connect to the school's network. Unprotected devices were automatically identified as they attempted to connect to the network and were prohibited from connecting. We sent consultants to the unprotected or misconfigured systems to make sure Symantec's antivirus software was correctly installed.

Evaluating Virus Protection Programs

In considering requirements for a virus protection program to be part of the security plan, Temple considered the following issues:

☑ Can the antivirus solution be managed from a central console?

☑ Can the program be distributed and updated from both a Web site and another type of server?

☑ Can it support Windows? What flavors? Mac OS? Linux?

☑ Can home users update on their own by connecting to the vendor's site and not by connecting to a Temple server?

☑ Can the central console automatically create a remedy ticket if a machine on campus becomes infected?

☑ What are the minimum hardware requirements?

☑ How many servers would be needed to roll out the solution throughout campus?

☑ What support options does the vendor offer?

☑ Does the program include an automatic removal tool for other antivirus software that might be on the machine? If not, is one available?

Temple's Security Test

Even as the university made significant progress toward securing the information and systems of students, faculty, and staff, our efforts were challenged during the summer of 2003. In July, a security bulletin was released describing a major vulnerability in the Windows operating system. One day later, our team assessed the threat as easy to exploit and widespread and decided that it was a critical issue that had to be addressed. We issued a campus-wide e-mail message to 55,000 recipients warning people to update their Windows-based computers immediately. Less than a month later the Blaster worm attacked our network.

Temple had a well-written security policy in place, a security-conscious user environment, and protection tools on many systems. Consequently, an attack that could have spelled disaster had we been less well prepared instead simply impelled us to upgrade our existing security activities. Although not yet fully implemented, our security plan yielded impressive results by protecting us from the worst of the Blaster attack.

On a typical day (not marked by a massive attack such as Blaster), some 1,300 viruses attempt to infect computers connected to Temple's network. Each successful attack eventually generates a call to Temple's help desk, costing about $100 per service call. Theoretically, the cost of repairing and reacting to each of these viruses would have cost us millions of dollars. Thanks to our comprehensive security plan, Temple's help desk now logs fewer than five virus-related calls per day.

By November 2003, almost 90 percent of Temple's network-connected computers were protected with the university's standardized antivirus software. Nearly all were performing scheduled scans and were routinely and automatically updated.

Today all but 0.1 percent of supported computers on Temple's network have the antivirus software installed and running. More importantly, the NetSky and Sasser worms, having grabbed international headlines with their impact, had come and gone at Temple without causing a stir. Updates of rules and virus signatures are sent to the client computers automatically and are fully propagated through the network in less than 30 minutes.

Today, the security team at Temple continues to enforce the university's information security policies while helping students, faculty, and staff participate in maintaining a security-aware culture. By helping students understand that every computer—and computer user—counts, we successfully fortified our security posture without threatening academic freedom.

Ariel Silverstone (ariel.silverstone@temple.edu) is the Chief Information Security Officer for Temple University in Philadelphia.