Preventing IT Security Breaches

By Alan Dessoff

Spurred by several recent information technology security breaches, colleges and universities everywhere are scrambling to prevent more potentially devastating incidents, from thefts of personal identities and intellectual property to crashes of key systems.

As higher education institutions are discovering, cybercrime threatens all computer users these days, and schools of learning are as vulnerable to it—perhaps even more at risk—than government agencies and private corporations, which also have become victims.

A security task force established in 2000 by EDUCAUSE and Internet2 is spearheading an effort that has significantly raised awareness of IT security issues in the higher education community. The task force now is trying to develop practical steps institutions can take to protect their IT assets and also detect and respond to incidents when they occur.

"Information technology is pervasive on campuses, and security incidents that undermine campus networks or critical computers can create havoc for institutions or for broader systems like the Internet," says Jack Suess, a task force co-chair and chief information officer at the University of Maryland Baltimore County (UMBC).

But a continuing problem, he maintains, is that "the bar keeps getting raised higher and higher," which is why the task force "can't just declare victory and go out of business."

Most IT security threats initially came largely from amateur computer hackers—"novices, crazies, who just wanted to make a point or demonstrate how they could do it," says Mohammad H. Qayoumi, vice president for administration and finance and chief financial officer at California State University, Northridge. A long-time APPA member and contributor, he serves on one of several work groups the task force has established.

Now, Qayoumi and Suess say, even organized crime groups have joined hackers in threatening and often successfully attacking organizations from the U.S. Department of Defense to major credit card companies.

Security breaches have hit at least 16 U.S. colleges and universities so far this year, potentially exposing the information of more than a half-million people, according to *Computerworld*, a computer industry publication. As of last March, universities had accounted for 28 percent of the 50 security

Alan Dessoff is a freelance writer based in Bethesda, Maryland, who has written numerous articles for* Facilities Manager. *He can be reached at adedit@verizon.net.

Jack Suess

breaches recorded by the state of California since 2003, more than any other group. Financial institutions followed with 26 percent.

University of Southern California officials said over the summer that they planned to contact about 270,000 people who used the university's online application system in the past eight years, to alert them that a hacker had discovered a security flaw that could allow their files to be read.

"The hackers are more sophisticated than they used to be," Brad Noblet, director of technical services at Dartmouth College, told the *Dartmouth Alumni Magazine*. "We had cases where we patched a machine, thought we had fixed the problem, and then found later that the virus was deeper in the machine."

As the Dartmouth magazine reported, "A simple password that can be stolen by somebody guessing your dog's name is no longer sufficient to keep digital intruders at bay." The college has been forced to increase its security budget and deploy new technology, Noblet says.

Suess suggests that higher education's culture makes it a "a challenge for security." One reason, he explains, is that universities are largely decentralized, with individual offices commonly operating systems on personal computers that contain confidential information like students' names, birth dates, and social security numbers. *Computerworld* cites the widespread "webification" of university business processes, with more offline data coming online and becoming potential targets for attack.

Faculty, meanwhile, value free and open exchange of ideas and sharing of information for research, but risk loss through electronic attacks of the intellectual property they create. And students expect their institutions to provide the IT environments that allow them to use the latest advances in technology, like wireless laptops, BlackBerry devices, and camera phones.

"We have students with their own computers who do what they want to do, we have faculty doing research, and we have staff working on administrative systems and record-keeping. Trying to design a security system that supports all those mixed needs is a challenge," Suess asserts.

Qayoumi says campus IT security is "specifically critical" for facilities managers. "Up to this point, many people have concentrated on security issues for major data systems and considered IT security to be the job of the campus CIO or computing center," Qayoumi says. "But they have not concentrated on the next tier of systems that universities have."

He cites Internet-based telephone systems, HVAC systems, fire alarms and building security systems, and other areas of

Mohammad H. Qayoumi

campus infrastructure that usually are the responsibilities of facilities managers.

"We're seeing more security concerns being raised in those areas. If somebody broke into the campus key systems, it would cause havoc, and the costs to change or replace your systems are going to be in the millions of dollars," Qayoumi declares.

At the Georgia Institute of Technology, "We identified a number of common areas of vulnerability that apply to virtually every system on campus," reports Rob Clark, director of internal auditing. He co-chairs one of the EDUCAUSE security task force work groups.

Clark cites the facilities department's work order system as an example. "Historically, it has made sense for that department to put up a computer as a server that will allow workers

"We have students with their own computers who do what they want to do, we have faculty doing research, and we have staff working on administrative systems and record-keeping. Trying to design a security system that supports all those mixed needs is a challenge," Suess asserts.

to log in and get their work orders and do status updates and all of that. The challenge comes when you put that machine up on the Georgia Tech network," Clark says.

The network, he says, is the target of up to 200,000 hacking attempts per day. "If the facilities department puts their server up and it is not properly configured and secured and updated with the latest security patches and is otherwise open and vulnerable, that system will be compromised. There is an absolute guarantee of that. It's just a matter of how soon; it could be minutes or hours or days, but it will be compromised because there are continual attacks against large networks like that," Clark asserts.

Suess says that in its first five years the EDUCAUSE security task force has "made a lot of progress" in raising awareness of the types of IT security issues higher ed institutions face. In 2000, when the task force was formed, fewer than 10 percent of universities represented at the initial conference had dedicated security officers on their campuses. Now, the number is probably close to 80 percent, Suess says.

EDUCAUSE and Internet2 established the task force following a number of attacks launched against major e-commerce websites like eBay and Amazon.com. When it was

Rob Clark

found that some of the attacks came from higher ed campuses themselves, "it became clear that higher education had not been taking computer security as seriously as it needed to," Suess says. To preempt possible crackdowns by the federal government, the higher ed community formed the task force to act on its own.

After the terrorist attacks of September 11, 2001 increased national focus on physical security, cybersecurity also "began to become a critical component" and forced the task force "to get even more serious about this problem," Suess says.

But the effort is complicated by operational needs of different college and university networks, which often directly conflict with security practices such as perimeter firewalls, port authentication, centralized configuration management, and strong authentication. Although firewalls are becoming widely used to protect critical systems on university networks, according to EDUCAUSE, it is difficult to reconcile their restrictiveness with the need for an open networking environment that supports research, learning, and high-speed networking.

"We're trying to establish the mindset, the framework, that everybody on campus shares in the responsibility to maintain secure systems..."

Also, although centralized management is feasible for certain hosts on a university network, it is not suitable for most student computers and many faculty, research, and clinical systems. Higher education networks must be designed to accommodate visitors, new students arriving with computers, researchers sharing large quantities of data with members of other academic institutions, remote access to a variety of network services for individuals who are traveling or telecommuting, and mobile users moving between classrooms, libraries, and indoor and outdoor study spots on campus.

Meanwhile, as technology advances, new challenges develop. Suess cites wireless computers as a current example. "Wireless computing has taken off and become mainstream. New buildings have wireless and many campuses are retrofitting their old buildings for it." The challenge, Suess says, is "how to provide wireless access without opening your campus network to anybody who walks through the gates with a laptop."

While his institution—UMBC— is funding deployment of wireless access to campus departments, it also is requiring that users enter their campus user names and passwords before they can surf the Web. "At least that way, we can restrict this to people who are part of the campus," Suess says. His office also is working with residential life officers to develop a security strategy for uses of wireless by students in dormitories.

Clark suggests that a key to effective IT security on a campus is the recognition of senior management that security "is not just an IT issue, it is a management issue." At Georgia Tech, says Clark, "We're trying to establish the mindset, the framework, that everybody on campus shares in the responsibility to maintain secure systems. That includes individual users, systems administrators who establish appropriate restrictions on systems and regularly update them, and management, which has an appropriate oversight role."

"Everybody doesn't have to be a geek-speak guru," Clark says, "but everybody does need to have at least a minimum understanding of effective practices to secure their systems.

Identifying those effective practices is what the EDUCAUSE security task force is working on now, and Suess expects the body to "remain viable certainly through the remainder of this decade."

5 Steps To IT Security

The EDUCAUSE security task force contributed to a national strategy to secure cyberspace, developed on the order of President George W. Bush and issued in February 2003. It encourages colleges and universities to secure their cyber systems by establishing some or all of the following, as appropriate:

- One or more information sharing and analysis centers to deal with cyber attacks and vulnerabilities.
- An on-call point-of-contact to Internet service providers and law enforcement officials in the event that a school's IT systems are discovered to be launching cyber attacks.
- Model guidelines empowering chief information officers (CIOs) to address cybersecurity.
- One or more sets of best practices for IT security.
- Model user awareness programs and materials.

For more information, visit EDUCAUSE at www.educause.edu/security.