



Knights in Cyber Armor

Business schools rely on technical wizardry to keep their systems safe from virtual dragons.



The world of cyberspace is both magical and dangerous, and those who would cross its borders require skill and strong defenders to keep themselves safe. As electronic data transmission and wireless Internet access become coins of the university realm, business schools need to determine how to protect themselves, and their students, from cyber warriors. Schools have always taken cursory protective measures; but these days, school administrators are donning full armor as they step onto the virtual battlefield of the Internet.

This attitude is relatively recent. “Until a couple of years ago, educational institutions viewed security as a philosophical issue as opposed to a technology issue,” says John Arsneault, director of network operations for Harvard Business School’s IT Group in Boston, Massachusetts. “In the past, when we talked about implementing systems security or creating policies for restricting access, discussion would be about how this infringed on freedom and put up barriers to collaboration. That attitude has dramatically changed. Today, the schools that have the funds to do it are implementing systems in a very similar fashion to corporations.”

Openness on a university campus is a thing of the past, agrees Arthur Downing, assistant vice president for information technology, professor and chief librarian at Baruch College in New York City. “We’re moving in a direction where faculty and students are more concerned about anonymity and confidentiality. They don’t want me looking over their shoulders when they’re on their network. But I have to be able to make sure that anybody who’s on our network using our resources at any given time is someone who should be there, and I have to know who they are.”

Security experts are fairly certain that administrators at most schools are covering the basics—installing firewalls, recommending anti-virus software, communicating with users, and creating backups. Even so, many could stand to put up a few more shields and deploy a few more swords in an increasingly volatile cyber environment.

The Outer Defenses: Firewalls

Firewalls prevent unauthorized personnel—even personnel from the rest of the university—from gaining access to the business school network. These software applications keep out users who are not authenticated and note unusual activity that signals some kind of attack. “We have people who monitor the reports of our servers and devices that watch for spikes in activity at certain points in our network,” says Downing. “It can become quite expensive to invest in all this technology.”

by Sharon Shinn

illustration by Neil Brennan

Before setting up a firewall, HBS administrators implemented a product called PacketShaper, which restricts bandwidth available for services such as file sharing. Not only does this instantly cut down on illegal activities such as swapping movies and music, says Arsneault, it allows the system administrator to see which ports are being used for which applications. "When it came time to put in the firewall and close services, we were able to close more than 99 percent of the ports without stopping a single service that was being used on the campus," says Arsneault.

About a year after installing the first firewall, he says, administrators went back in and shut down all incoming traffic outside the data center. "That means people can't go in and host their own Web sites, and can't host peer-to-peer information to their own PCs. It has literally made problems like denial of service attacks and compromised PCs almost disappear."

Inside the Castle: Virus Protection

Anti-virus software can do a superb job of preventing infected information from corrupting the network—but it only works if every user has installed it and is keeping it up-to-date. And "every user" means every professor, staff member, and student who logs on to the network. "You can literally take out the network with one rogue PC," says Arsneault.

It's easiest to control faculty and staff computers. At Harvard, faculty and staff must be authenticated as they log onto a school directory. Service patches and anti-virus updates are automatically pushed through the staff/faculty system by the central IT office. Recently Arsneault changed the virus update refresh date from once a week to once an hour. "When you ask the server if there are any definition updates available, 99 percent of the time the answer is no," he says. "But if a virus definition is released, within 60 minutes the system is updated."

Harvard has also installed LANDesk management software on the faculty and staff systems, which gives the central IT department the capability to do hardware and software inventories while allowing individual users to install software on their own computers. "They still have ownership over their PCs, but we have the ability to know what's on the network now and what software is running," says Arsneault.

Harvard's IT department also has installed two layers of virus control. The one at the e-mail gateway, which guards the system from outside attackers, purges 25,000 infected e-mails a day, says Arsneault. The second one, a McAfee product, monitors internal e-mail—which doesn't have to go through the gateway—to make sure school personnel don't pass on viruses picked up inadvertently.

The Chink in the Armor

You can install every piece of hardware ever invented; you can require absolute synchronization of software. But if you don't get a buy-in from the users, the system will eventually break down. As is so often the case, in the realm of cybersecurity, human beings are the weakest link.

The organization Educause offers schools basic information about technical security solutions on its Web site at www.educause.edu/security/guide, says security task force coordinator Rodney Petersen. But for any school security program to work, the human administrators must first develop a policy that explicitly spells out who is responsible for what and what should happen when something goes wrong. "The three steps are prevention, detection, and response," he says.

In terms of *prevention*, the first important component is risk assessment, which includes identifying and classifying all the data an institution collects. "For instance, a public Web server is public by definition, whereas student records and grades are private," he says. The second component is to identify who the "data steward" is—such as the registrar for student information and the comptroller for financial information. The third component of prevention is setting policies about access: who has it and what kind of controls are in place.

The fourth component is training those with access about how to use and protect the data under their stewardship. "I once worked at a university where a student employee in the registrar's office gave the media information about a student athlete that he had obtained from student records," says Petersen.

In the area of *detection*, Petersen says, administrators can't just secure the mainframes and think they're done; they have to secure the multiple devices that download and manipulate data from that mainframe. For instance, a trusted employee can go to a protected mainframe and download employee information to his laptop. If the laptop is stolen or compromised, all that data is at risk.

"We tend to focus on electronic data and forget that it can exist in a physical form," says Petersen. "One day an administrator showed me a printout of all the employee information, which he'd found in a trash can. What we're talking about is the three stages of data flow: in storage, in transit, and in use. And we forget about data in transit and in use."



A fairly obvious part of detection involves monitoring the systems to determine if someone is trying to break in. A less obvious part is having an administrator do preemptive investigating to find out how much information is publicly available when it shouldn't be. For instance, says Petersen, it's a given that students' Social Security numbers shouldn't be readily accessible. He suggests using a Web search engine to type in "Social Security numbers" and your school's .edu address, and seeing if any faculty Web sites turn up with student grades posted by SSN. They shouldn't—but they might.

Finally, Petersen believes it's critical to have a rapid response team in place so that if a security breach does occur, this group can instantly swing into action. Team members should include tech professionals, legal counsel, public relations representatives, and risk managers. "Have a procedure in place, have the team in place, and test them both periodically," Petersen advises.

Anyone on campus who has any responsibility for data should have a baseline level of knowledge about security, Petersen believes. Over and above that, he should understand his specific duties. "The institution has the role of setting policy, and the user also has responsibility," says Petersen. "The leadership should come from that data trustee and not from the IT department."

In complete agreement is Richard Baskerville, professor and chairman of the computer information systems department of the Robinson College of Business at Georgia State University in Atlanta. Having researched information systems security for about 25 years, he has seen that most organizations focus on technical solutions and overlook management solutions. "People think that with the right encryption, the right access control technology, and the right firewall, you can solve the problems," he says. "We don't have much good work on socially oriented solutions to these problems, like relating employee behavior to security."

What Baskerville really expects to shape the future of information security is not technology, but a new attitude about risk management. "Risk management has always been based

on probability theory," he says. "If there is a low probability of a particular kind of attack, it has never justified a high investment of resources to protect it. However, that theory doesn't really apply to critical infrastructure, because you really have to protect against any possibility of attack, even

if it's a very low probability." When possibility theory is applied to the risk management of critical infrastructure, he says, "it actually changes the kind of control framework and safeguards that you put in place."

Recently, Baskerville has been exploring how information warfare drawn from military models can be used in business applications. Specifically, the military follows a "decision cycle" of observation, orientation, decision, and action; during each stage, it seeks to achieve information superiority over an opponent. "You can apply those same concepts to information security in a business organization so you can protect the decision cycle against all threats, whether they're viruses, intrusions, or attacks by miscreants," he says. "This then forces you to manage information security using that model rather than the technological model in which you merely make sure you have all the right technology in place. Information security officers following that cycle would be looking at a much higher level in terms of management concepts."

IT specialists will also find themselves in a more cooperative mode in the future, he thinks. Various organizations now monitor the networks 24 hours a day, such as the Computer Emergency Response Team (www.cert.org) run by the Carnegie Mellon Software Engineering Institute. That group works with users, software vendors, and the U.S. government to share information about viruses, worms, and other abuses. Another organization, InfraGard (www.infragard.net), is a coalition of private and governmental organizations, including the FBI, who have banded together to protect critical infrastructure in areas from agriculture to telecommunications.

Such cooperation is essential because, even as technology evolves, it opens the way for new vulnerabilities—and the villains have the edge. "The attackers only have to discover a single flaw in the new technology to abuse it, whereas the defender has to find all the flaws," says Baskerville. "That's actually impossible. Therefore, the defenders have to be able to deploy responses to threats very, very quickly. The vicious circle has moved to Internet speed."

It's harder to control student systems, since students are asked to comply voluntarily with regulations for patching systems and updating virus software. Arsneault recently implemented a user address registration system that kicks in when students get online in class; it allows him to track who is using the recommended software and who is not. "What we haven't decided is exactly how to deal with the folks who haven't installed the software," he says.

At Temple University's Fox School of Business and Management in Philadelphia, Pennsylvania, all students are required to install the school's approved anti-virus software. That software, Symantec's Norton AntiVirus Corporate Edition, is made available to students via CDs and downloads from the university's Web site. "We have been diligent," says Ariel Silverstone, Chief Information Security Officer at Temple. "They can't log on if they don't have it."

It's not quite as strict at Washington University's Olin School of Business in St. Louis, Missouri, which recommends Norton's anti-virus software but does not enforce its use. MBA students are required to bring laptops; if they order the preconfigured Dell option, it comes with the Norton software. "But we tell them that any anti-virus program is better than none," adds Scott Ladewig, manager of networking and operations. "For students who claim poverty, we direct them to a free adware program."

Students who live on the Wash U campus get the anti-virus software free as part of their housing fees. "We've looked at licensing it for other students who don't live in university housing, but we haven't gone down that road yet. It's expensive," says Ladewig. It's also management-intensive. "If I have 100 students using this software, how many of them live in the dorm, and how many taking classes here are really students at another school in the university? It's tricky unless the university decides to license the software for every student."

It can also be tricky to deal with executive education participants, who frequently bring laptops that have been configured by IT specialists back at the corporate headquarters. "We haven't really tackled this challenge," says Harvard's Arsneault. "But we do want to be able to identify the systems they're using and, if a machine is causing a problem, disable it. We'll probably do that with a MAC address registration application."

That MAC, or "media access control," address registration system directs users to the registration page of a virtual local area network (VLAN). They must supply details such as their names and domains before they're allowed full access to the VLAN. "The whole process takes 60 seconds, and then the user has full access to HBS network services," says Arsneault. "In addition, the IT group then knows who the person is and

when the person is on the network. The process only needs to happen once per PC."

Soldiers in Reserve: Redundant Measures

It's common practice for all institutions to back up data and store it someplace safe. But where is safe? And how much redundancy is enough? School administrators in New York are particularly haunted by these questions. Says Baruch's Downing, "We're probably more conscientious than most schools because the odds are greater that we'll be affected by terrorists. We've been at Orange Alert since 9/11."

When making backups, says Downing, the goal is to have them close enough for easy access—but not so close they're also destroyed by whatever catastrophe takes down the system. Because Baruch is part of CUNY, backup student and mainframe information can be stored on a systemwide mainframe.

Baruch doesn't stop at creating redundant data storage; the school also has more than one communications link for the campus network. "Before 9/11, many institutions only had one path for communications," says Downing. "If that link was destroyed or interrupted, they didn't have service. Since then, many places have invested in not only having another physical way in, but also in using another vendor."

Baruch is now part of a fiber-optic ring that includes a variety of educational institutions in Manhattan, says Downing. Fiber-optic networks, he explains, allow signals to go in reverse, as well as forward, so that they can still get to their destination even if there's a break in the loop. Because the signal travels at light speed, it arrives at its target in the same time frame, even if it has to travel farther to get there. "We're running that service in addition to the same connection that we had at the time of 9/11," he adds. "It would take quite an incident to create a disruption that would affect both of them."

Along this ring is a commercial telecommunications and networking facility where the university leases space. "We have servers in there that can be brought into action should something happen to our main computing system," Downing says.

All Flags Flying: Constant Communication

Since security is only as effective as the people practicing it, these administrators work to keep their constituencies informed. Most schools provide information about viruses or other vulnerabilities via e-mail, printed notices, and alerts posted on school Web sites. Ladewig says that the Olin School covers the issue of cybersecurity during orientation for incoming students, which reinforces communications sent out electronically before students even arrive on campus.



Others go on an all-out campaign. For instance, Temple instituted an awareness crusade that makes it clear to students and faculty how important it is for them to join in the effort to safeguard data. Writing in the *Educause Quarterly*, Silverstone describes the school's efforts. "The awareness campaign is disseminated through candy dispensers, posters and fliers, and newsletters and Web sites—all carrying the 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," he says. "We also introduced noncredit 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."

Even so, sometimes students continue to be cavalier about taking simple safety precautions. That's when IT departments must take precautions for them. For instance, Baruch encourages students to change the default passwords they are issued when they enroll. Last summer, a check revealed that 89 percent of the students had not done so. Since the default passwords are generally crafted of readily available student information—such as the last digits from their ID cards—they're easy to steal.

"Not only can someone else get into a student's account and get access to all his personal information, but he can act on that student's behalf," says Downing. Among other things, one student can de-register another from a full class to make room to register himself. Therefore, over the summer, Baruch changed all the student passwords. "The school newspaper contacted us to say it was disruptive. But we viewed it as an opportunity to educate students on the importance of protecting their information," Downing says.

Girding Up for the Battle Ahead

It seems that universities' attitude toward cybersecurity can only go in one direction—toward more controls and tighter access. Many school administrators are closely watching the development of new products that will require authentication before students are allowed to log onto the network or that will quarantine computers that don't have the right updates.

Arsneault expects corporations to adopt such measures before schools do and notes that it will be harder for schools to implement systems that will abruptly deny students access. "Especially if you don't have tech support 24/7, you don't want to be knocking people off the network," he says. "If a student has an assignment due at 6 p.m. and he can't get on the network and there's no one to help him till the next morning, that's not good."

What the future really holds might be a higher degree of caution from human users, says Rodney J. Petersen, policy analyst and security task force coordinator for Educause, a nonprofit association geared toward advancing higher education through information technology. For instance, Petersen expects to see more data encryption, which will keep information safe even if someone hacks into a file or steals a laptop. Encryption techniques exist already, of course, but average computer users don't bother to learn them. "The technology needs to be transparent and easy to use," Petersen says.

He also predicts that there will be fewer multiple repositories of data, with files of personal information being kept at the library, the registrar, the HR department, the recreation center, and so on. Instead, he expects there will be one central repository of data that is checked by other entities that need to authenticate a person's identity.

Downing believes human, not technological, improvements will be necessary to make schools more secure. He says that administrators need to do a thorough self-assessment before trouble actually hits to determine what their policies should be and what they can afford to implement.

"How much are they willing to invest for peace of mind? That's an institutional decision that goes beyond the IT department," says Downing. "When there is a situation like a power blackout, do they want us to evacuate the computing center, or should we stay to make sure all the data is secure? Those decisions need to be made in advance and implemented campuswide."

Finally, everyone involved in cybersecurity needs to realize that their jobs are never over. "This is an endless game, unfortunately," says Arsneault. "We've made monumental progress in the last couple of years, but there's always something more coming."

In another decade, the preventative measures put in place right now might appear to be curiously medieval, while the weapons used against them might seem equally quaint. But for today, the attacks launched against a university's cyber fortress must be viewed as state-of-the-art, designed to bring down the ivory tower. The war is real, the enemy is armed, and the academic defenders simply can't afford to lose. **Z**