Students' communications devices and the ubiquity of wireless networks have all ratcheted up the difficulty of securing campus networks and data. What has resulted? Identity theft. Data breaches. Compliance violations. Increased costs. Legal liabilities. What else? A battle fought with valor by MIS directors and the technology vendors who support them.

By Tom Robinson

Pick one: Cybersecurity.

Convenience.

Cybersecurity.

Who is the enemy?

A decade ago, you might have envisioned a geek at MIT entertaining himself trying to crack a Pentagon firewall just for the fun of it. "The days of mischief are gone," says Chris King, director of product marketing at Palo Alto Networks. He estimates 70 to 80 percent of today's bad guys are sophisticated criminals—including syndicates operating from Russia—and supported by a growing industry that trades in stolen data.

What do they want?

Colleges and universities are a treasure trove of data. On any given campus there are thousands, perhaps millions, of records for applicants, students, faculty and staff. Don't overlook former staffers, alumni, donors and even patients. And, oh yes, small, medium, large and even enormous research databases.

An unethical researcher at a pharmaceutical company may be scouring data from clinical trials being conducted at a university medical center. A competitive academic may want to publish findings before a colleague. Foreign governments may want a peek at plans for communications systems being developed at an engineering school with a Department of Defense grant.

There are system attacks that take over computers and create a botnet of zombie machines. These can harness enormous amounts of computing power for a variety of nefarious purposes, including the distribution of viruses that destroy data.

Very often the cybercriminal wants a social security or credit card number. Better yet, a name, an address, an employment history, and any other information that can build a complete persona by which a crook can fraudulently obtain credit or access deposit accounts.

The Open Security Foundation, a volunteer nonprofit that tracks data breaches, reports that more than 11 million records stored at colleges and universities have been compromised. Last April, administrators at the University of California, Berkeley, discovered that hackers had accessed records affecting nearly 160,000 individuals—including social security numbers.

How do they do it?

Some do it the easy way: *steal a laptop* with confidential files. Better still, leave the laptop in place. Enormous amounts of data can fit on a thumb drive. Beyond the obvious there are more devious ways:

Others *intercept data transmissions* from unsecured wireless networks. During transmission to or from a laptop or smart phone, unsecured data is vulnerable to a snoop listening in.

Put the pieces together. If a cyber criminal acquires the password you use to log onto Facebook, then maybe that password works with your bank account, too.

Phishing, as defined by *Wikipedia*, is masquerading as a trustworthy entity to fraudulently acquire sensitive information such as usernames, passwords and credit card details. Phishing often uses e-mail or instant messaging from bogus sources purporting to be legitimate. The *phisherman* directs recipients to enter details at a fake website whose look and feel are almost identical to an authentic one.

Convenience.

Human error. Inexperienced network administrators or others who have administrative privileges can, often without even realizing it, leave databases open. In such cases a bad guy need not hack his way in; just search with impunity. A researcher—not a hacker—at Dartmouth found schematics for Marine 1 (the President's helicopter) and the First Lady's safe houses in Washington simply by searching.

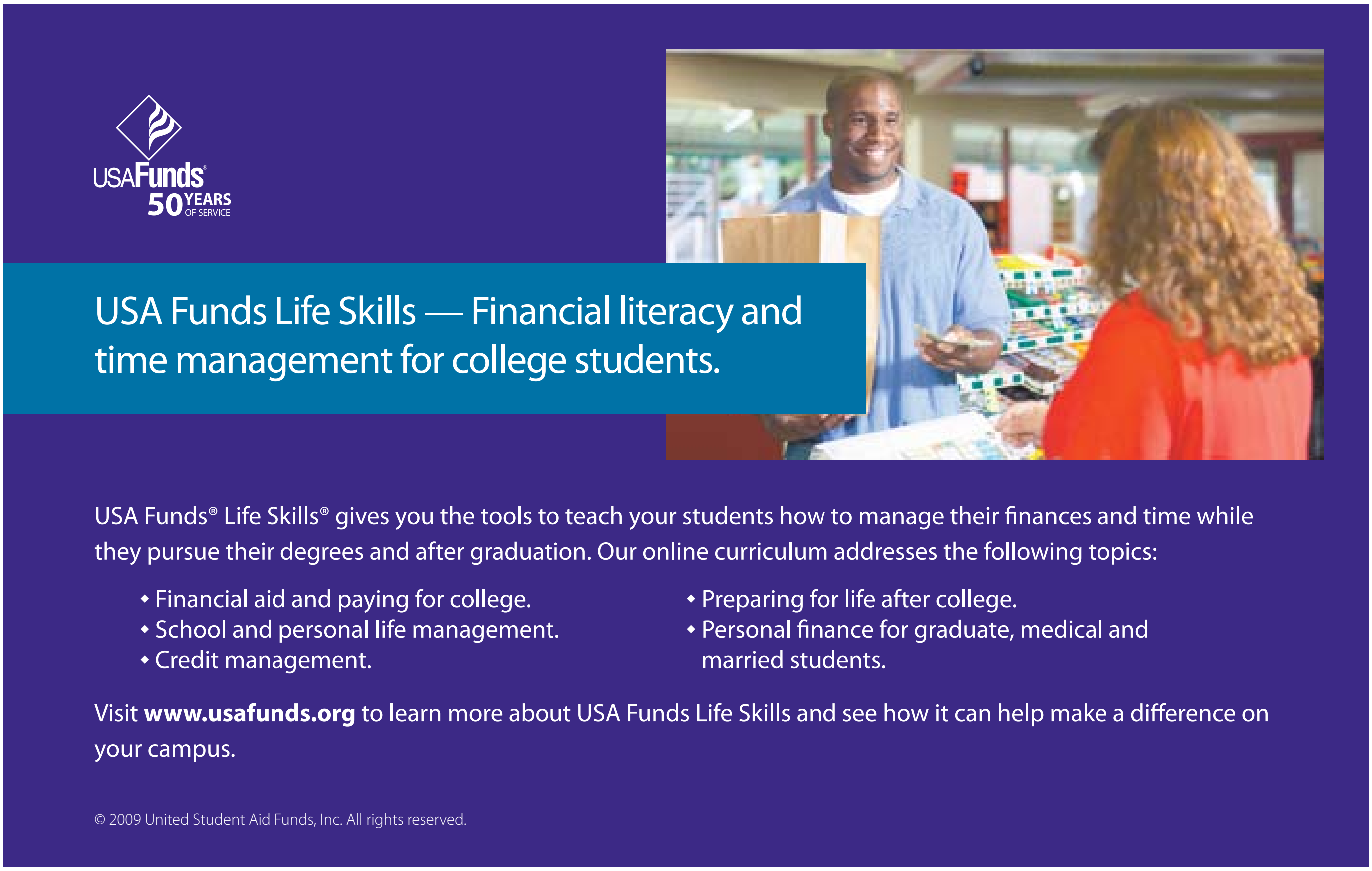
Are campuses particularly vulnerable?
Not necessarily. Virginia Rezmierski, director of policy development and education at the University of Michigan, was the lead researcher on the Computer Incident Factor Analysis and Categorization (CIFAC) project. CIFAC collected security incident data from colleges and universities to identify the nature of the incidents and the action taken. This data was later compared to security incidents in the business sector. Campuses were found to be no more or less vulnerable.

The increase in the number, and more importantly the types of devices, and the proliferation of applications used by students is nonetheless a challenge for security directors. Sheldon Malm, senior director of security strategy for Rapid 7, says rich internet applications move tasks from secure servers to "clients" and back with little user awareness. Vulnerabilities are created in the name of user convenience and customer satisfaction.

Students themselves pose problems. Despite being technologically adept, they are often naïve about the risks they take. For example, they open attachments or links on social network sites without really knowing the "friend" who sent them. Or they pick up a thumb drive lying around a student lounge and insert it into their laptop. The drive might have been that of a forgetful student. Or it might have been intentionally left by a bad guy, expecting someone to pick it up, and inadvertently trigger an auto-run executable to a malicious website. As soon as the student logs on to the university network, the malware infects it.

Business-enabling applications like social networking, collaborative applications, VoIP and messaging are not threats themselves, yet they pose risks to enterprise networks. Palo Alto Networks analyzed 255 Enterprise 2.0 applications. Of them, 70 percent are capable of transferring files; 64 percent have known vulnerabilities; 28 percent are known to propagate malware; and 16 percent can tunnel other applications. Examples of new threats introduced to enterprise networks by applications such as Facebook include Koobface, Fbaction and Boface, each of which can hijack accounts and personal data.

What's the fallout?
A lot of law suits, right? Wrong. According to Frank Vinik of United Educators, the institution-owned insurance company, just one suit has been brought over a data breach—and that suit was unsuccessful. However, he cautions that no suit does not equate to no loss. There is the hard-to-determine, but nonetheless costly, loss of trust. Negative publicity and the resulting damage to an institution's reputation can



scare off donors, alienate alumni and make applicants hesitant.

Networks and servers taken offline following an incident interrupt business operations. Hundreds of employees can be idled waiting for computer access. Sometimes students who need access to learning management systems or library resources, especially during an exam period, are at risk for failing grades.

The hard costs of repairing relationships can be expensive. After a data breach, paying for 50,000 credit reports for alumni, even at the group rate of $20 each, would cost $1 million. The IT staff time diverted from productive work to tracking, analyzing and repairing damage costs money. Hundreds of hours quickly adds up to thousands of dollars. Avoiding a public relations gaffe is expensive when you add together the cost of system administrators, attorneys and outside PR counsel.

Sometimes data is not stolen, it is destroyed or corrupted. On purpose or by accident. Institutions may be liable for the cost of replicating research or for opportunity losses incurred by a grantor or contractor expecting to go to market with a new product.

Corporations have paid millions of dollars in fines for failing to comply with an alphabet soup of regulations, including PCI, HIPAA, FISMA, SOX and NERC. So far campuses have been spared. That may not always be so. The Senate Judiciary Committee approved legislation authored by chairman Patrick Leahy (D-Vt.) that would require entities to report personal data theft to those individuals and to law enforcement, and make concealment a crime.

What to do.

Data security is everyone's business. Campuses pride themselves on open access and academic freedom. Regardless, openness cannot come at any cost. Students and academicians, alike, must understand that for their own protection—as well as that of the institution—there must be policies and procedures in place to regulate access to and use of confidential data.

Many institutions are ramping up enterprise risk management (ERM) plans. Palo Alto's King believes that policy for such plans must originate at the highest level of an organization. "It should not be placed on the shoulders of the IT department," he warns. "They are not equipped to make risk management decisions." Margaret Tungseth, president of the University Risk Management and Insurance Association (URMIA) and risk management director at Concordia College, urges campuses to make sure a risk manager is at the table when preparing for or reacting to a cyber (or any other type of) threat to see beyond the nitty gritty of a particular incident and get a perspective from the 40,000 foot level.

Sheldon Mahl cautions risk managers and IT administrators to be wary of software vendors and consultants who purport to protect everything. "If you don't question, the industry will let you believe."

Virginia Rezmierski sees a potential IT career path problem. "It is not uncommon for administrative assistants who are 'good with computers' to end up as system administrators" managing more than their skills, training or experience justify.

Frank Vinik reminds risk managers to know what their insurance covers. Personal information and intellectual property theft is not like other property and casualty perils. Tungseth says Concordia carries insurance on things like internet media liability and cyber extortion as part of a bundle of security coverages; but it is difficult to establish what loss levels to insure against.

All the experts point out that user bad habits are a significant factor. Education is essential to increase awareness and to change risky behavior. Don't use one password for everything. Don't open unkown links and attachments. Encrypt and password-protect sensitive data. Use caution when on unsecured wireless networks. Don't give out personal information readily. TC

A security planning primer

Before you can protect your information assets, you must know what information needs protecting.

- What data you have
- Where it resides
- Who is accessing your data
- When users are accessing it
- How users are accessing it

Develop policies and procedures to manage data security. Many progressive institutions are adapting an approach called Public Key Infrastructure or PKI. It duplicates for electronic transactions what old-fashioned face-to-face interaction used to do, with five necessary components:

- Identification
- Authorization
- Data security
- Confidentiality
- Non-repudiation

Adopt PCI as a minimal standard. The PCI Security Standards Council is an open global forum founded by American Express, Discover, JCB International, MasterCard and Visa. While initially designed for financial service companies, its security standards are applicable to all account data protection.

Take advantage of the latest technology to:

- Encrypt data on the network
- Encrypt data at the "end point"—laptops, key drives, CDs, etc.
- Proactively scan for vulnerabilities
- Patch and repair
- Rescan
- Document for compliance

Continue with something colleges should be good at: educate, educate, educate.

People cited in this article

Chris King, director of product marketing, Palo Alto Networks

Virginia Rezmierski, director of policy development and education, University of Michigan

Sheldon Malm, senior director of security strategy, Rapid7

Frank Vinik, United Educators

Margaret Tungseth, president, United Risk Management and Insurance Association and risk manager, Concordia College