DATA SECURITY IN HIGHER ED: A MOVING TARGET

How do you make sure everybody with access to information on your campus knows what they have and how to keep it secure — in an ever-changing landscape of behaviors and risks?

BY MICHAEL HART

YOU WORK AT a college or a university. Your job title has some combination of the words "security," "data" and "information" in it. You've got a lot on your mind, and a lot on your plate.

So, are you worried about the teaching assistant in the basement of the chemistry building selling beakers to students to use in their labs? How about the system the popular pizza place across the street from campus is using to process credit card transactions? ▸

shutterstock.com

Probably not — but you should be. It's those activities, and more just like them, that fly way below the radar at most institutions of higher education. However, they can make your school just as vulnerable as any information gap you might find in the admissions office.

An Open Environment

For years, if not decades, universities have been notorious for their relaxed attitudes when it comes to information security. But there's a reason why their systems aren't as airtight as, say, the financial sector: Higher education is a unique environment with distinct needs.

For starters, there is the long tradition in higher education that bends toward openness and transparency. For generations, academics have believed in making sure information and data can be widely shared and validated by others. In many cases, that spirit has been transferred to parts of the campus that aren't necessarily involved with learning and research, leading those who work with mundane administrative and financial processes to adopt a more permissive attitude toward data security than their peers who work in other cultures.

"When we build networks, generally banks and hospitals start by locking everything down and opening up just what they need," said Dan deBeaubien, director at the SANS Institute. "Universities often start with leaving everything open and then locking down what they think they need to protect, so there's a little bit different philosophy because of academic freedom."

Universities have not been subject to the same kinds of mandates faced by industries like banking or healthcare, which, for instance, has been forced by the U.S. government to meet strict security standards or risk losing federal funding.

"I came out of healthcare IT," said Jessica States, who was recently named **Fort Hays State University**'s (KS) first information security officer. "There are things you have to do there to get your Medicare payment. Here we aren't a hospital where a security breach can force you to pay enough fines that you have to go out of business."

The growing concern for greater data security in higher education is being fueled by the equally fast-growing awareness in the general public of the threat of identity theft — accompanied by the realization on the part of criminal elements that the local college or university could be an easy target.

"Universities are simply huge repositories of monetizable data," said Sadik Al-Abdulla, director of security solutions for CDW. "There is a vast amount of personal and financial data available and, more than that, there are long-term financial relationships that take place."

Finally, there are the hoards of employees, faculty, students and administrators at higher education institutions who have an alarming amount of access to sensitive information — and may not even know it.

"People don't think a class roster is sensitive data, but it can be," States said. "They look at a list and think that nobody cares about all these names and addresses, but I look at it and think, 'Oh no!'"

"Universities are simply huge repositories of monetizable data. There is a vast amount of personal and financial data available and, more than that, there are long-term financial relationships that take place." — *Sadik Al-Abdulla, CDW*

Do's and Don'ts

So what are those entrusted with the security of data at their institutions to do? Before answering that question, it might be helpful to think about what *not* to do.

1) Do not consider it a mere technical challenge. "In the past, security was not seen as a university-wide problem," said Ashley Sudderth, **Michigan Technological University**'s chief information compliance officer. "It was something the technology people could take care of. The attitude was, 'IT's going to do it and we're fine.'"

Securing the technology side of things is vital, of course, but that is not the end of the story. Neither is it enough to make sure your university is complying with all the mandates

that come from government. While Sudderth's job title does have the word "compliance" in it, she does much more than that: "You have to change people's behavior," she said. And much of the time, it is behavior they don't even know might be causing problems.

"Users will do things, sometimes accidentally," deBeaubien agreed. "They can expose data they don't mean to, even when they're using the best technology."

2) Don't rely on a one-size-fits-all awareness and training program. Beginning in 2010, deBeaubien and Sudderth set out to implement an ongoing program at Michigan Tech to deal with data security awareness. (At the time, deBeaubien was the university's chief technology officer.) They quickly learned what they shouldn't do.

"The broad brush approach, giving everybody the same training, does not work very well," deBeaubien said. "It's very expensive and not very effective. The idea is to use the exact right training for exactly the right role."

3) Do not view security as a single problem that needs to be solved. "View this as a journey, not a destination," Al-Abdulla said. "It's more a case of managing risks."

He compared it to the never-ending national campaign to reduce the number of highway traffic deaths: "Hopefully, with a combination of technology in the vehicle, education of the driver and regulation of the roadways, you can keep the death toll down," Al-Abdulla said, "but you can never eliminate it altogether."

"Security is a lot like that," he added. "It is not a solvable problem. It is something organizations and individuals need to be cognizant of and be working toward improving all the time."

The means by which you make your data more secure typically involve changing the behavior of the people in your institution — both in their work and non-work lives, and in the most fundamental ways possible.

4) Forget about broad, sweeping policy statements. While a clear policy is necessary, Al-Abdulla said, "it doesn't build skills for individuals to make good decisions on an ongoing basis to protect data for their institutions and in their personal lives."

Making Better Choices

For Al-Abdulla, who has been involved with data security most of his career, it begins with something as simple as helping people to be smart about choosing their personal passwords.

"If you simply communicate policy, people have the habit of doing only what you tell them, like using eight letters and one capital letter," he said. And that often results in compliant — but weak — passwords.

Al-Abdulla recently worked with a Chicago-based institution (not an educational entity) on its data security program. To demonstrate a point to its employees, he used the term "GoBears!" (a reference to the city's NFL team) as a password and checked it against every one of more than 1,000 accounts in the organization. "You would be shocked to know how many accounts I was able to get access to," he said.

Weak passwords should be a source of concern for higher education institutions, Al-Abdulla insisted, because hackers all over the world are relentless in their efforts to access sensitive research data. "There are many examples of both nation-states and criminals creating accounts so they can get access to passwords," he said — and it isn't just the data-rich laboratories you have to worry about either.

"Instead of attacking a research lab, they'll attack the most popular restaurant near the research lab and, if you're using the same credentials in both places, they now have access to your lab," Al-Abdulla pointed out.

For stronger passwords, the U.S. Department of Homeland Security's Computer Emergency Readiness Team recommends a variety of tactics:

- Don't use passwords that are based on personal information that can be easily accessed or guessed;
- Don't use words that can be found in any dictionary of any language;
- Develop a mnemonic for remembering complex passwords;
- Use both lowercase and capital letters;
- Use a combination of letters, numbers and special characters; ▸

- Use passphrases when you can; and
- Use different passwords on different systems.

A Comprehensive Approach

The need to make users more cautious about their security methods is what drove deBeaubien and Sudderth to implement a campuswide security awareness initiative at Michigan Tech in 2010. They focused their efforts around a single acronym: the TARR system (train, audit, review, remediate).

They began with a simple survey that, with the help of senior-level managers, they were able to make mandatory for every staff member in the university who dealt with information of any kind — credit card numbers, Social Security numbers, salary information, etc.

"We asked two simple questions," deBeaubien said. "Where do you get information and what do you do with it?" They wanted to know what kind of information each person had access to, what they did with it and what means they might use to deliver it to somebody else.

"Maybe you didn't know somebody's walking around with a bunch of credit card numbers encrypted on a cell phone," deBeaubien said. "You can start to make some pretty accurate statements about whether that's a practice that you want to change or one you can live with."

DeBeaubien and Sudderth used their surveys to come up with a numerical system that evaluated the risk level of every single person's behavior. That alone told them more than they imagined they'd learn.

"Before this, when we looked across the entire university, we had tended to focus on things we were worried about," deBeaubien said. That is why, in their pre-TARR days, they might implement a public relations campaign to protect credit card information they thought staff members might have access to. "We'd hang up a bunch of posters and train a lot of people," he said.

After the TARR survey, however, they learned "the number of high-risk behaviors associated with credit cards weren't nearly as significant as other high-risk behaviors," said deBeaubien.

They also learned that data was being exchanged in rather cavalier fashion in corners of the university where they never would have imagined it would be taking place. (For example, teaching assistants taking credit card information from students buying beakers for their chemistry class experiments.)

They broke the survey information down, not necessarily by individuals who were exhibiting high-risk behavior, but by departments and divisions where they found clusters of behavior that drew their attention. "That helps you with the two big questions in the information security game," deBeaubien said. "What training do I want to apply and who do I want to apply it to?"

DeBeaubien, Sudderth and their staff were thus able to tailor specific training programs to very specific populations in the university. For instance, in one department the high-risk behavior might have something to do with the way student ID numbers were stored. In another, it might be the way Social Security numbers were transmitted from one university unit to another. For each group, the training was designed to be most relevant to the people involved.

The team has repeated the survey every two years to monitor changing risks and behaviors, and is using a number of measurement devices to assure that the data security efforts are indeed working. By one common measure called the Payment Card Industry Data Security Standard (PCI-DSS), high-risk behaviors dealing with data at Michigan Tech were reduced nearly 60 percent from 2010 to 2014.

DeBeaubien and Sudderth believe the number of risky behaviors they find in their 2016 surveys will be even lower, but transgressions still will exist — so they will continue to work through their train-audit-review-remediate cycle. By then, not only will there be at least some fresh faces on campus who have yet to be "TARRed," but there will also be new threats that would-be criminals have come up with and new risks that haven't even surfaced yet.

Data security, as Al-Abdulla pointed out, is not a single problem to be solved. It is a journey that never ends. **CT**

Michael Hart *is a Los Angeles-based freelance writer and the former executive editor of* THE Journal.

BACK TO TOC