CREATING A CYBER-SECURE CAMPUS

valuable, so they need to lock down their data like any other entity. This requires a combination of technological defenses like firewalls and encryption, along with training for faculty, staff and students so they recognize phishing and social engineering attempts to hack into their systems.

"Believing that it can happen to us, and fearing that, is probably the first thing you have to have in order to be proactive," DesPlas says. "You've got to believe, 'We will be under attack at some point,' and you've got to believe, 'It can happen to us.' You've got to believe it is our responsibility to guard against the loss of data. It's all about the attitude from the top."

And at San Juan, President Toni Hopper Pendergrass helps set the tone. "As we all know, information and personal identities seem to be the new currency," Pendergrass says. "It is critical that we safeguard them as fervently as we do cash, equipment and other assets. In essence, they require Fort Knox levels of security and protection."

SETTING THE TONE

Indeed, the college president needs to set the tone, says Steven Hernandez, chief information security officer at the U.S. Department of Education. "If protecting information technology is in the college's strategic plan and part of the president's talking points, that puts everyone on notice that it's a priority," he says. "The president needs to have an ongoing dialogue with the [chief information officer], [chief technology officer] and certainly the [chief information security officer] as we're moving new technologies into the organization, and maybe move things onto the cloud. Every one of those is an opportunity to enhance security, in addition to improving the user experience."

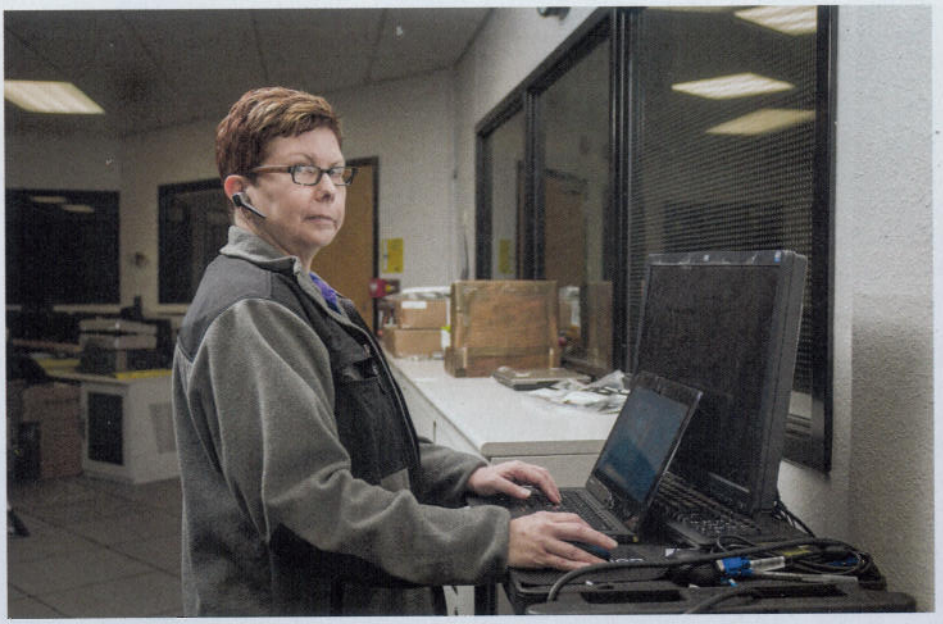
Community colleges need to take cybersecurity as seriously as they take physical security issues, says Lee Petry, Lee Petry, director of the Workspace One SET Team, government, education and healthcare, at cloud computing company VMWare. "If there is an active shooter on campus, there are policies, and you've trained your students and staff. What do you do for your data?" he says. "Have you updated your plan? What is your plan to secure your data? Do you have firewalls up? Do you have password protection? More often than not, there is no plan."

James Henningsen, president of the College of Central Florida in Ocala, says two-year colleges need a culture in place that understands the importance of data protection at the highest levels and throughout the management team. "The culture has got to be set by the president," he says.

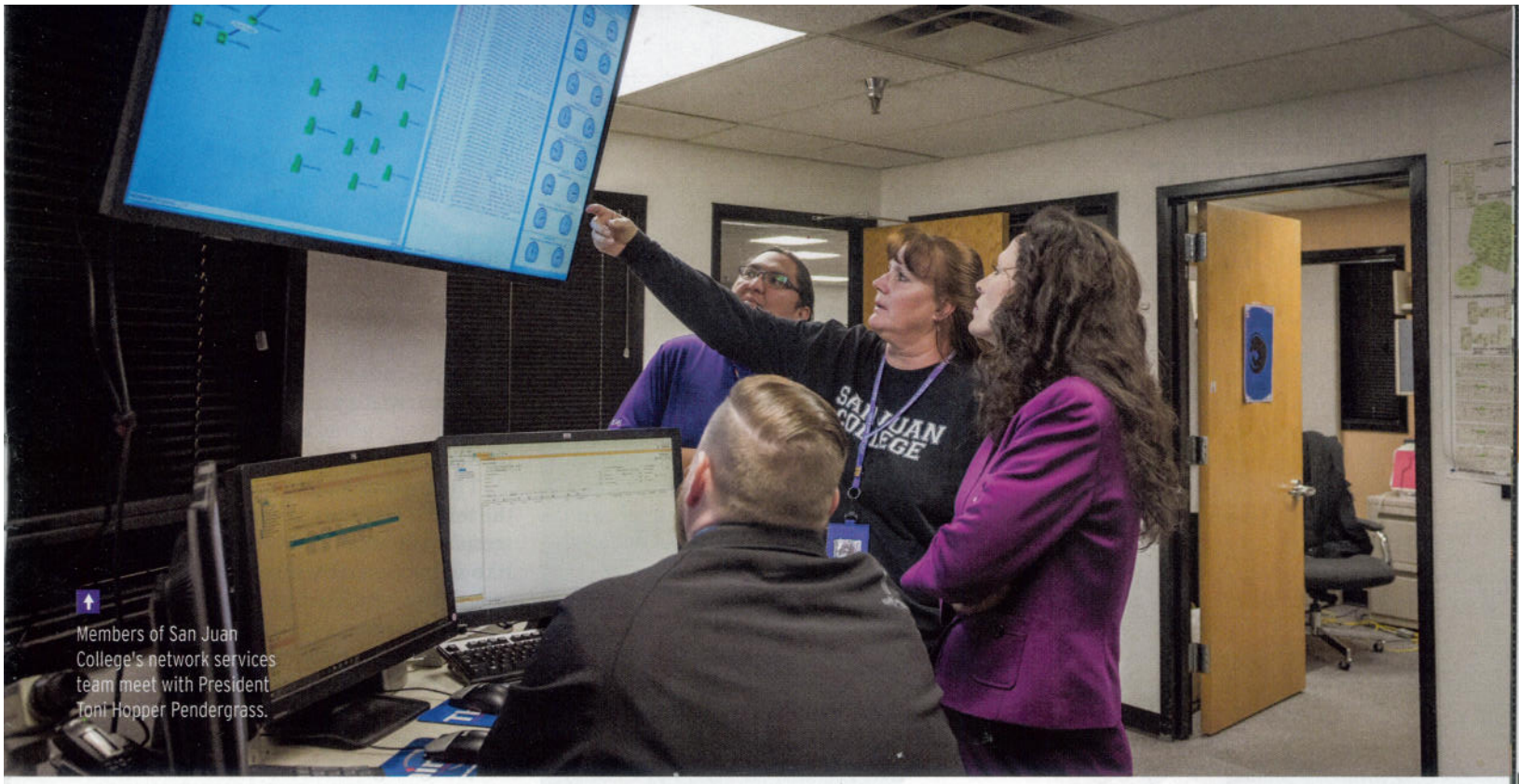
Executives need to ensure that the right policies and procedures as well as communication channels are in place to keep up with cybercriminals, Henningsen says. "Hackers are developing new strategies every day, and security people are developing countermeasures every day," he says. "We disseminate our message through governance groups. It's important to get the word out. You can send stuff in an e-mail, but not everybody is going to read it. You've got to do multiple communication channels, and you need real-world examples."

The president and CIO need a free, honest channel of communication about not only successes but also challenges and shortcomings, says Henry Glaspie, CIO at College of Central Florida. "Dr. Henningsen is very supportive in saying to me, 'We have this problem, we don't have the expertise, can I engage a third party so we can have those resources and skills on the ground?'"

DesPlas says San Juan College engages in collaboration among departments from information technology to student services to administrative services to achieve the necessary combination of technological solutions—like next-generation firewalls and added protection against malware and ransomware—as well as "almost perpetual training, almost perpetual readiness drills" to ensure people have the right mindset. "We all have to know the first and last line of defense is the people we have working for us," he says.



Lisa McCord is the lead system administrator at San Juan College.



Members of San Juan College's network services team meet with President Toni Hopper Pendergrass.

Laramie County Community College (LCCC) in Wyoming works to ensure broad, high-level communication about any potential cyber-dangers to students or employees, CTO Chad Marley says. "We like to go to the president's cabinet and make sure they're informed," he says. "We want to make sure everybody is aware of the risks."

The college also has strengthened password policies, added encryption services to e-mail, implemented new training software, leveraged existing tools in the Microsoft campus environment and then some.

The president of Michigan's Lansing Community College provides top-level support for cybersecurity when it comes to resources and budget, as well as culture, says Paul Schwartz, director of information security. "Then he delegates the responsibility to the CIO, who delegates it down to me, eventually, to implement the various cybersecurity tools and principles," he says. "There is a bit of cybersecurity in everybody's job."

Leadership teams at the executive and directorship levels meet regularly to collaborate and discuss the issue, Schwartz says. And the president sits on the board of trustees, which helps communicate the urgency to them, as well.

College executives and their boards need to talk about cybersecurity risk in terms of the impact on the college's mission, Hernandez says. The pitch should be something like, "If you fund an information security program, we can get down to a low area of risk. Whereas if you're not going to support us at a certain level, you have done less due diligence, less due care," he says. "And the public and any regulatory agencies are going to ask the board, if there's a breach: 'You knew about this, you chose a path of higher risk. Talk to us about that decision-making.' That's going to help the board make a great decision."

"People understand that breaches happen. They're used to it. But folks are unforgiving when they feel lied to, when the timeliness is not there."

STEVEN HERNANDEZ, *chief information security officer, U.S. Department of Education*

LCCC senior staff have presented to the board about the potential risks and how they have been able to mitigate them, which has helped earn investments in cybersecurity, Marley says. "We just provided the cost-benefit, and what it will allow us to do if we have an attack or a ransomware situation," he says. "We try to manage our security footprint within our operating budget. So far, we've been able to do that."

Henningsen says he's had no issues convincing his board members. "This is a very serious situation. A lot of people are already aware," he says.

Anyone having difficulty convincing their board just needs to do a Google search on data breaches, DesPlas says. "You can produce pages upon pages of different educational institutions, healthcare facilities—heck, look at Facebook," he says. The real-world examples are out there, and they are stunning."

REACTING TO A BREACH

While being proactive hopefully will stop any breaches, there are no guarantees. Containment of the breach is always the first step, Hernandez says. That means knowing "that we have data flying out of the organization and having a plan in place where people who are authorized to do so can stop the leak," he says.

CREATING A CYBER-SECURE CAMPUS

Second, community colleges need to contain the communication about the breach. "Being able to control the message around this is what will make you or break you," Hernandez says. "People understand that breaches happen. They're used to it. But folks are unforgiving when they feel lied to, when the timeliness is not there. Being able to already have that [communications] scenario played out and available is priceless."

Third, Hernandez recommends calling in outside professionals to identify the problems, fix them and give the college a clean bill of health. They need to be able to say, "We did a root cause analysis, these are the steps we took to fix the problem, and here you are now with the problems taken care of," he says. "And the lessons learned need to be fed into information security going forward."

If a breach happens, Petry says a community college needs to understand the full scope. Some hackers break in all at once while others "slowly but surely take data over three years. The really good ones are quiet about it," he says. He also recommends shutting off connectivity and doing a complete password reset.

Schwartz's advice starts with not panicking, keeping in mind that detection will always be a more realistic goal than total prevention. "The bad guys always have the upper hand," he says. "They're constantly looking for ways to breach a network. We solve the ones we're aware of. There are so many more they're discovering, especially through social engineering and phishing."

A community college affected by a breach needs to contain it, taking servers offline as necessary, then notify relevant parties ranging from legal counsel to cyber insurance carriers—who can bring forensics to bear about what caused it, Schwartz says. "It's key to identify what was lost or stolen, and then figure out, 'What are your compliance obligations?'" he says.

COSTS OF A BREACH

A cybersecurity breach carries both financial and reputational costs. Hernandez estimates the former ranges from the tens to hundreds of thousands for smaller breaches to millions for larger ones. But he figures the fines, credit monitoring and other money costs are less painful than the reputational kind, particularly for colleges with a cybersecurity degree program. "It's not directly involved, but that doesn't matter," he says. "Why would I get a cybersecurity degree from a school that's just had a breach?"

The insurance market for cybersecurity is developing and evolving, Hernandez says, with larger players starting to get into the space, but it only helps with financial costs, of course. "Cyber insurance doesn't protect your reputation or goodwill," he says. "There's a saying about being tried in court and being tried in public opinion. Public opinion can be more severe and irreversible."

And cyber insurance cannot be seen as a substitute for a solid risk management program—in fact, that's the first thing underwriters will want to know about, Hernandez says. "An active cybersecurity program is the best primary insurance an organization can have," he says. "If you don't have it, they're going to look at you and say, 'OK, we'll insure you, but probably at a premium that's higher than what it's going to cost you to stand up that program.' "

The costs of a breach can run into the tens of millions in a worst-case scenario in which student information like Social Security numbers end up "out in the wild" and a flood of lawsuits result, Petry says. "If every individual student who lost their Social Security number is exposed and gets their identity stolen, how liable is that school?" he says. "If you don't get ahead of it, what are you going to do?"

Joe Mazur, vice president of administration and finance at Central Florida, adds the reputation hit from newspaper headlines and the presence of auditors and oversight agencies, "exerting more strain on human and financial resources." When examining insurance policies, Mazur advises closely perusing the exclusions laid out, like a data breach due to a USB drive, or very short windows in which to notify the insurance company. "It's just like home or auto policies," he says.

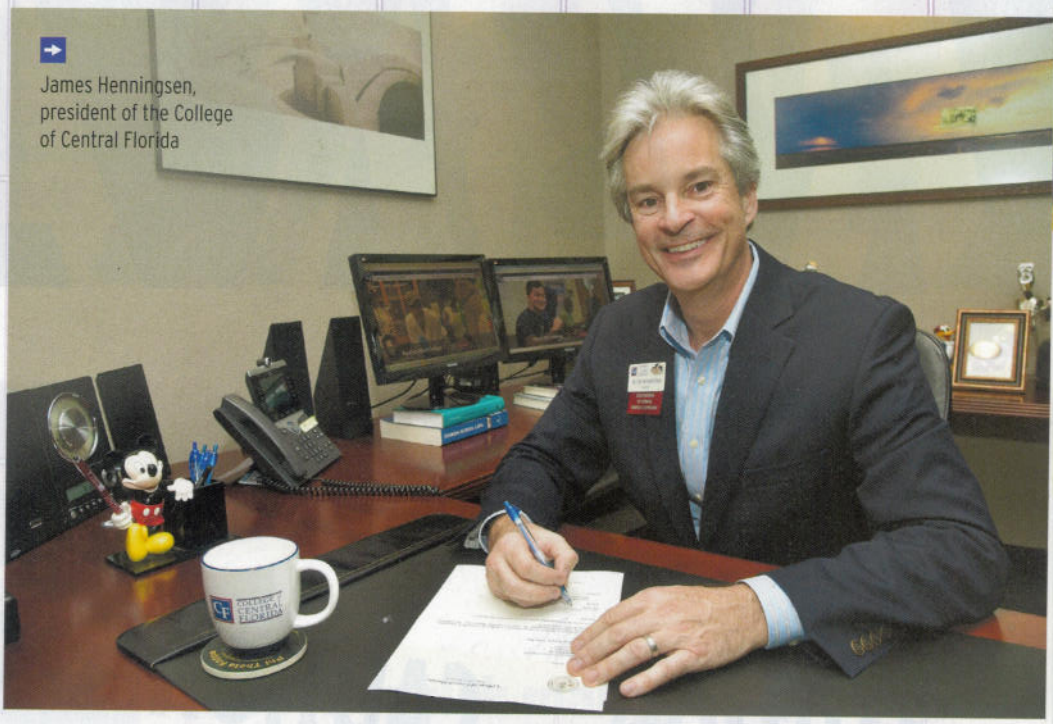
Schwartz of Lansing tallies up the direct costs of fixing the problem, notifying those affected and potentially monitoring their credit, and the hit to the college's reputation. A breach also is an opportunity to convince your board to fund what it might not have, he says. Cyber insurance policies will typically pay for external, specialized forensics experts who examine access logs, figure out when hackers invaded and what they took, he adds.

San Juan College has $3 million worth of insurance, which DesPlas

"There is a necessity to make sure all of your folks have that basic understanding that their actions can lead to permanent, in some cases irreversible, harm."

STEVEN HERNANDEZ, *chief information security officer, U.S. Department of Education*

Image Credit: College of Central Florida



James Henningsen, president of the College of Central Florida

acknowledges amounts to "a rather minor breach, in terms of the scale of what it could cost."

He adds, "It's not the cheapest or easiest insurance to get," requiring answers to a battery of questions from underwriters' technical teams ranging from what type of firewalls you have in place to whether you allow employees to send e-mails with people's Social Security numbers. "It's a pretty intrusive process," DesPlas says, but "it does put another team of eyes on your policies and procedures."

PREVENTION IS THE BEST CURE

Virtually all breaches have at least some element of human error, Hernandez says. No matter how high your firewalls might be, "Humans are the weakest link in the security chain," he says. "People instinctively want to help others. These virtues will be exploited by the charlatans." And humans are prone to getting tired, distracted or bored, he adds. "There is a necessity to make sure all of your folks have that basic understanding that their actions can lead to permanent, in some cases irreversible, harm."

A robust training program is key to minimizing the chances of human error, Hernandez says. "Phishing is by far the most popular and effective threat vector," he says. "Part of your training program should be simulated phishing exercises. Send e-mails to folks and see if we can get them to click. That helps draw a risk profile."

Annual training is not nearly enough, Hernandez says. "We need to make sure we have posters up, that we have spots in the campus newspaper, that we hook into their daily lives," he says. "The holiday season is a great time to remind people; in your personal life, you're out using a credit card, exercise great behavior there, as well. When you start to hook in the personal side with the business side, it resonates. It's not just, 'The college is telling us to do something again.'"

While firewalls and other technological security has advanced greatly, humans are virtually the same, although the employee culture has shifted toward being more supportive of cybersecurity in the past quarter-century, College of Central Florida's Henningsen says. "Rather than saying, 'I've got to change my password six times,' they understand the implications," he says.

The college has been testing employees by sending out realistic-looking phishing e-mails of its own, including some with Henningsen's signature, or with the college's logo. "We're continuously training our employees," he says. "We've put systems in place to help employees identify good e-mails vs. bad e-mails—every e-mail says either internal or external. We're providing more help for employees to realize, 'That doesn't smell right.'"

LCCC has implemented security mentor training thanks to a partnership between IT and human resources, which rolls out a new cybersecurity module every month. To date, modules have covered overall security awareness, e-mail security and phishing, and there are three more to come. The college has instituted multi-factor authentication and soon will go live with a service that enables employees to determine whether an e-mail originated off-campus.

"We're trying to be proactive," Marley says.

Schwartz figures human error leads to "the vast majority" of successful breaches, and he says Lansing requires all employees to do annual computer-based training on what to anticipate and how to recognize red flags in e-mails. Employees receive fake phishing e-mails, and "if they were foolish enough not to notice the red flags, we link them to a training page," he says. "We follow that up with traditional training. We try to track habitual violators. If they still don't get it, we get HR and their supervisor involved."

Lansing also rewards those who correctly identify phishing e-mails, handing out donuts with Swedish fish inside them the last time they tested employees.

Petry agrees that training staff, faculty and students with realistic looking phishing e-mails and providing remedial help for those who click is the way to go. "This has to be part of their plans, quarterly, annually," he says. "Do they know how many people have hacked their system? Chances are, China is doing it right now. Chances are, Russia is doing it right now. It's a game for those folks. It's an open system. Let's see what I can get today." ■

Ed Finkel is an education writer based in Illinois.