DELL Technologies

How Higher Ed Is Answering the Cybersecurity Challenge

The dilemmas posed by hackers are real and evolving. Some institutions are finding new ways to tackle the threat.

In December 2021, Lincoln College, a 157-year-old institution in Illinois, announced that it was closing its doors. The causes were many, including pressures wrought by the pandemic—but key among them was a ransomware attack that robbed the historically Black college of access to data and compelled it to pay up to $100,000 to regain its accounts, all at a time when financial pressures already loomed.

Cybersecurity is increasingly central to the smooth-running of academic institutions. A survey conducted by Sophos, a British cybersecurity company, revealed that ransomware hit 64 percent of higher-education institutions globally in 2021, and that the average cost of cleaning up after an attack was $1.2 million. As the stakes rise, industry experts stress that cybersecurity awareness is vital for administrators responsible for protecting staff and student data, and intellectual property.

Historically, education has lagged behind other industries in its ability to tackle the cyberthreat, but experts say they now see positive trends, with higher-ed leaders more aware of the need to equip their institutions for the evolving cybersecurity landscape. In addition, specialist courses in cybersecurity are emerging, educating a new generation of students trained to tackle the cybersecurity challenge.

Several factors are coming together to help improve security in higher ed. Technology companies offer what some describe as a utility model for monitoring and responding to risk, aiming to support institutions that lack resources and expertise to protect themselves from hacking. Colleges can turn to external vendors to provide coverage where they lack expertise.

Dr. Hernan Londono, chief innovation strategist at Dell Technologies, who served recently as chief technology officer at Barry University, compares it to electricity: In theory, households could produce their own but it's much more efficient if a utility company serves multiple homes at scale. "It is less costly for the utility company to give you that utility than for you to do it yourself. There's consistency and reliability— you know that every time you want electricity, and you just flip the switch."

The utility model also allows administrators to address staffing gaps."In higher ed, we are accustomed to working Monday through Friday, maybe 8 [a.m.] to 6 [p.m.]," Londono says. "And sometimes there are not enough people. So, what would happen on weekdays after 6? Who will monitor, who will respond?"

Another strategy takes a layered approach, seeing cybersecurity as a fabric (or mesh) of interlocking tools that work together to protect different parts of a system. Administrators are thinking about this in an increasingly critical way, Londono says, and asking vital questions: "How many layers are too many? How many layers are too few? And how are the layers connected?"

External factors are also converging to compel colleges to implement better cyber policies. The stakes are high, but a suite of potential options for addressing the risks is emerging.

Historically, education has lagged behind other industries in its ability to tackle the cyberthreat, but experts say they now see positive trends, with higher-ed leaders more aware of the need to equip their institutions for the evolving cybersecurity landscape.

Guidance from government

In recent years, the U.S. government has nudged institutions to improve their posture in response to cyberthreats, strengthening its best practice

Given the current state of the cybersecurity threat landscape, there are additional challenges when implementing security solutions for the remote workforce of an organization.

guidance. New guidelines will soon be issued by the National Institute of Standards in Technology (NIST), and Londono says that early drafts available for review have been welcomed by industry stakeholders. “There are significant improvements in the framework,” he says.

The first NIST framework was published in 2014, and outlined five functions central to effective cybersecurity: identify, protect, detect, respond, and recover. The new guidelines introduce a sixth— govern, a principle that aims to clarify the policies, regulatory requirements and tolerance for risk that apply across an institution. Education can also learn from other sectors, like health-care, where governance is better defined, Londono explained. Governance is “normally something that is incredibly difficult to do for almost any organization. And so now the future version of the NIST security framework will provide guidance for people to really act upon governance.”

Another development is increasingly stringent requirements from cyber-insurers, which are also urging colleges to strengthen their policies. Those that do not have “best-in-class” controls in place could see their premiums rise by between 100 and 300 percent. While this places pressure on leaders, it does have an upside, Londono notes. “It can be seen as positive. Over time, the more we improve our posture, the better we’re going to be at mitigating risk.”

Blended environments: University of Miami Health System

Some institutions already navigate a careful balance between applying rigorous security protocols and facilitating open research and teaching. One of those is the University of Miami Health System, Florida’s only university-based medical system, connected with the University of Miami Leonard M. Miller School of Medicine, comprising a large number of health care providers, researchers, students and other areas that support the organization.

Managing the concerns of different stakeholders is a delicate task, says the system’s chief information security officer (CISO), Dr. Mauricio Angee. For a hospital, protecting patient data and ensuring patient safety is the top priority. Health-care providers must also implement mandatory compliance measures—the Health Insurance Portability and Accountability Act (HIPAA) obliges hospitals and clinics to implement security-management processes to protect patient information, and guard against cyber attacks. More critically, poor cybersecurity leaves hospital systems vulnerable and puts patient lives at risk. In 2021, there were a number of deaths in hospitals across Europe and the United States because ransomware attacks led to reduced capacity that prevented patients

from receiving urgently needed care. Thus, understanding the delicate balance between the risks and the security safeguards that need to be implemented is the key.

Given the current state of the cybersecurity threat landscape, there are additional challenges when implementing security solutions for the remote workforce of an organization like the University of Miami, whose activities include teaching, academic research and medical care. To improve UHealth system's resilience, its security teams have worked to implement systems and solutions that identify, detect, protect ransomware, zero-trust architecture and, with the help of Dell, deployed 38 firewalls. They also planned how the system would recover from a potential attack by improving its resilience, introducing Dell's datavault technology, which provides a space where backed-up data is stored offline in a sequestered environment that hackers cannot reach.

Privacy, compliance, and cybersecurity teams worked together, creating a dedicated task force that consulted with the audit, legal, and HR departments to gain an overview of how changes to the system would affect those employed within it. "If the controls are too stringent, human beings try to bypass the security controls to make it more efficient or to do their job," says Angee.

Solving the talent question: Mercyhurst University

One of the biggest challenges facing administrators is the difficulty in hiring and retaining talent in the area of cybersecurity. At the same time, when students graduate from college, it's still hard for them to obtain jobs in cybersecurity, because they don't yet have experience.

Educators at Mercyhurst University are tackling this conundrum. In 2018 they set up a dedicated cybersecurity major, which combines courses in coding, engineering, and mathematics with opportunities for hands-on experience. Students in this sector must be adaptable and willing to stay up to date with a shifting landscape over the course of their careers, says Chris Mansour, assistant professor of cybersecurity and the program's co-founder.

"Education in this field is critical because it provides students with the knowledge, the skills, and the hands-on applied experience that is necessary to understand the complexity and strategic challenges in securing systems and security networks and digital assets," he adds.

At Mercyhurst, students throughout the university learn some of the basics in security hygiene, like protecting their personally identifiable information when they access networks at home. The program also offers three routes through which they can obtain practical experience. There are internships that bring students into contact with

large companies; alternatively, students can work with companies as part of an elective course so that they don't incur extra fees.

This structure benefits students and companies alike, says Brian Fuller, the director of operations for the Ridge College of Intelligence Students and Applied Sciences at Mercyhurst. "Our students could be working for the same company [over the course of different internships] and gaining applied real-world experience and building their resumes," he explains. "And that employment-talent pipeline with the client—we're hoping that they have an employment offer prior to their senior year."

Students can also take part in active projects through Mercyhurst's Center for Intelligence Research, Analysis and Training (CIRAT). Working alongside a faculty lead, they are responsible for assignments for government agencies and companies in the private sector in areas ranging from cyber-resilience to geopolitics. One current project, Fuller explains, involves working with a company developing an AI capability to process information for federal institutions in a way that hasn't yet been done. "It'll be cutting edge," he said. "And it will be something that will really help the government."

Through this experience, students become effective communicators on technical and non-technical matters. For Mansour, "the cyber field is a team sport," and Mercyhurst tries to create an environment that cultivates a culture of inclusivity. Students, for example, learn about important issues like ethics. In addition, the university supports neurodiverse students through its dedicated autism initiative, and 14.5 percent of the undergraduate population in cybersecurity is neurodiverse.

Faculty at Mercyhurst are upbeat about the cybersecurity challenge. For one thing, the field is expected to grow rapidly—job opportunities will rise by 35 percent by 2031, at least seven times the national average for all occupations. "What Mercyhurst does is actually something that addresses this challenge," Fuller explains, "through hands-on projects and hands-on assignments that are up-to-date with whatever is going on in the field."

Joining forces

Companies working with Mercyhurst students are honing win-win arrangements. More broadly in cybersecurity, collaboration between higher education and the private sector is increasing. Some companies now offer training on cybersecurity literacy to leaders in higher ed.

Experts from Dell recently partnered with FBI and CISA to spend a day teaching college leaders about incident response.

The cybersecurity field is expected to grow rapidly—job opportunities will rise by 35 percent by 2031, at least seven times the national average for all occupations.

Mauricio Angee agrees that collaboration is vital. A decade ago in health-care, he says, institutions worked alone against cyberattacks. Now, security leads at the University of Miami Health System swap tips with their peers, sharing data on suspicious activity and IP addresses. They also partner with the FBI, as well as with their key vendors.

The rising velocity of attacks combined with their technological sophistication will continue to demand a nimble response. Today, criminals are using the same techniques as a decade or two ago—phishing, denial of service techniques, and ransomware. AI is "changing the game. The bad guys are using AI and we're using humans. So, I'm telling you, we are at a disadvantage."

DR. MAURICIO ANGEE
CHIEF INFORMATION SECURITY OFFICER (CISO), UNIVERSITY OF MIAMI HEALTH SYSTEM

Resilience, recovery, and getting back to business

Colleges and organizations are investing more in securing their systems and are becoming more proactive in addressing the challenge. When industry clients approach Mercyhurst looking for support, it's not from a perspective of doom-and-gloom, Fuller says. "It's more like, 'We have a baseline program. Now here's what we haven't figured out. Can you figure it out for us? We need it. We want it.'"

New operating models—like the utility model and the fabric approach—offer clearer paths toward cyber resilience. As the landscape shifts, vendors may play a great role—taking on intensive tasks like the continuous monitoring of risk and threats, just as utility companies provide water or heat.

The rising velocity of attacks combined with their technological sophistication will continue to demand a nimble response. Today, criminals are using the same techniques as a decade or two ago—phishing, denial of service techniques, and ransomware. AI is "changing the game," Angee adds. "The bad guys are using AI and we're using humans. So, I'm telling you, we are at a disadvantage."

AI, however, also offers new tools for those on the other side, increasingly "leveraged by experts in more protective systems, more detective systems," Mansour says. Another important shift, he says, lays greater emphasis on incident response—a focus on resilience.

"Instead of investing heavily to prevent a cyber-attack, now they're investing heavily to see if they can detect the cyber-attack and trigger the incident response and recovery immediately, almost instantaneously," he says. "Then they can recover quickly and get back to business and get going."

To learn more about Dell Technologies solutions for Higher Education, visit Dell.com/HiED