THE CHRONICLE
OF HIGHER EDUCATION®

FREE REPORT

How Colleges Can Defend Against Cyberattacks

By LEE GARDNER

Cyberattacks are nothing new for colleges. Hackers and the internet grew up together, and raids on university servers for fun and profit have been going on for decades. But cybercrime is now big business, and ransomware attacks that cost their targets thousands, even millions, of dollars and disrupt operations for days or weeks have become regular headlines. Colleges are not immune.

In fact, colleges can be especially susceptible to cyberattacks. Universities are built on principles of open inquiry and the free exchange of information that don't always coincide with information-security best practices. The end-users of higher-education technology can be especially heterogenous — students, office workers, librarians, professors, researchers, doctors — which makes securing a network more challenging.

Cyberattacks can be costly, in downtime and dollars. A hacked network can disrupt operations, cancel classes, and force information-technology staff to spend weeks or months cleaning up the mess. The literal costs can be steep as well. A cyberattack on the University of Vermont Medical Center in 2020 was estimated to cost the institution $1.5 million a day in lost revenue and response costs.

Colleges are up against a numberless, faceless opponent armed with an increasing level of sophistication. As nearly every chief information-security officer says in one way or another: We must be perfect every time. They just have to get lucky once.

Though many colleges operate on limited budgets that cramp their cybersecurity staffing and technology efforts, they can still take steps to protect their campuses — which are increasingly distributed and decentralized — and perhaps even get a step ahead.

This free report examines the current cybersecurity-threat landscape and how it has developed in recent years, including the rise of ransomware. The report looks at new avenues for cyberattacks and at the best ways that college leaders can bolster their defenses. And it anticipates what threats may lie on the horizon.

CURRENT THREATS

Sometime in the mid-2010s, people posing as researchers from other countries sent emails to professors at the University of Hawaii. The supposed candidates inquired about jobs and attached résumés or dossiers of their fabricated careers. The emails often landed in what seemed to be the wrong place — a researcher whose background appeared to be in chemistry, say, would write to an engineering faculty member — so the emails would be forwarded from professor to professor, department to department. Often the résumés were very similar. Sometimes only the name at the top was different.

The attachments themselves were harmless, but somewhere on each one sat a tiny web bug, "a one-by-one white pixel that you can't see," says Jodi Ito, chief information-security officer for the Hawaii system. It's a device commonly used by advertisers to track engagement; when faculty members opened the documents, Ito says, the pixel sent a signal back to a server somewhere. But what Ito now thinks may have happened is that by tracking the IP addresses of those who opened the documents, and who opened them next, hackers were able to start understanding the networking of the university's departments. Doing so may have allowed them to gain information to help them craft phishing at-

tacks targeted at specific individuals at the institution, to try to trick them into giving up sensitive information or downloading malware — software designed to exploit or sabotage systems.

In 2019, Ito learned that the University of Hawaii had been targeted by hackers looking for research on maritime technology. Two years later, a federal indictment was unsealed accusing four Chinese nationals of conspiracy to conduct cyberattacks on 21 entities, including the University of Hawaii and several other U.S. research universities, for an arm of China's Ministry of State Security. No arrests have been made.

The Hawaii attack was one of the highest-profile cybersecurity incidents at a college in recent years. It epitomized the growing ambition, sophistication, and patience of many hacker groups, a trend that shows no sign of flagging. And it highlighted what has been and still remains the biggest area of vulnerability for a college: email. In other respects, it's a relic of a different time. Cyberattacks are no longer aimed mostly at large institutions and valuable research. Any institution with internet access and an exploitable weakness is vulnerable — small private colleges and community colleges have also fallen victim. And the stakes for colleges of all sizes and types grow ever higher.

Lee Gardner writes about the management of colleges and universities. Follow him on Twitter @_lee_g, or email him at lee.gardner@chronicle.com.

The number of attempts at taking advantage of those vulnerabilities has exploded. "We have seen a marked increase in the numbers and sophistication of attacks in the last year and a half," says Ed Hudson, chief information-security officer for the California State University system. While Hudson doesn't have systemwide statistics available for the recent surge, he estimated that the number of attacks has doubled.

ISTOCK IMAGE

TAKEAWAYS

Cyberattacks and ransomware are nothing new, but the number of attacks has escalated, and the attackers are more sophisticated.

Email is still the most common way hackers access a college's computer network.

Security-awareness training for employees and students is still the best tool for fighting cyberattacks.

One way for an institution to better protect its data is through stronger data governance.

New federal standards for data security could mean sweeping changes for colleges.

The biggest challenge for college leaders in maintaining their cybersecurity operations will lie in hiring and retaining high-quality information-security staff.

1,132

Incidents that compromised the integrity, confidentiality, or availability of information in the global education sector from November 1, 2019, through October 31, 2020.

334

Incidents during the same period that resulted in confirmed breaches.

Source: Verizon Data Breach Investigations Report

"I've been in the business for over 20 years," he says. "I've never seen anything like it is right now."

Not all colleges may be seeing the same volume of attacks or the same sort of increase as Cal State, but most institutions are enduring a steady stream of attempts to break into their networks. Anti-intrusion technology at the University of California at San Diego detects about 45,000 attacks every hour, says Michael A. Corn, chief information-security officer. "Most of those are doorknob rattling, and they bounce off of our infrastructure," he says. "But it gives you a sense."

For many years, there were two primary prizes to be seized on any college's network. The first was personally identifiable information, or PII — the names, birth dates, Social Security numbers, and other data that fuel identity theft and other financial crimes. Criminal hackers would plunder databases for caches of PII and peddle them on the dark web, the sub rosa section of the internet where criminal activity flourishes. The second was proprietary research, typically a rarified commodity targeted by hackers from a foreign government, or so-called state actors.

In recent years, both criminal gangs and state actors have professionalized. It was easy to spot early phishing emails, says Cheryl W. Washington, chief information-security officer at the University of California at Davis, because "the construction of the English sentences was so poor that you kind of knew what you were looking at." Today's phishes may not only feature perfect spelling and grammar, but thanks to the kind of reconnaissance carried out at the University of Hawaii, it also may appear to have been from a particular employee's boss, with signatures and seals scraped from other emails, and look legitimate. "There's some sophistication now enshrouding phishing that we haven't seen before," she adds.

The hackers themselves are becoming more sophisticated in their organization. Instead of gangs of hackers attempting to pull off heists on their own, they're finding areas in which to specialize. It used to be that one group "would do everything, from compromising the computers, then installing the malware, then leveraging those computers," says Ito, of the University of Hawaii. Now some groups are dividing the work according to their expertise. Elite coders might craft custom malware for hackers who specialize in cracking networks for a share of the profits. "Everybody's getting more siloed," Ito says.

And the barrier to entry for would-be hackers is at an all-time low, says Donald M. Benack III, deputy associate director of vulnerability management for the Cybersecurity and Infrastructure Security Agency, or CISA, the federal government's cybersecurity arm. Getting a ransomware exploit, he says, is "as easy as going to McDonald's and ordering a Big Mac."

One of the reasons today's hackers are more sophisticated and bolder, he says, is that many of them may be sponsored by countries like Russia, China, and North Korea, all of which the United States has accused of launching cyberattacks. But it

isn't always easy to tell who's up to what. Attacks often come from places the United States doesn't have jurisdiction over or extradition agreements with, says Benack: "Those tend to be the same areas where it makes it even more difficult for us to differentiate between, 'is this state-sponsored, is this state-endorsed, is this just criminal activity?'"

Perhaps the biggest shift has come from the rise of ransomware, which involves the introduction of malware into a computer or computer system to destroy it or block user access until a ransom is paid, effectively holding it hostage. It isn't a new problem for colleges, but it was for many years a small-stakes gambit, says Stefan Savage, a professor of computer science and engineering at the University of California at San Diego and a cybersecurity researcher. Now, it's big business. The costs of damage from ransomware attacks worldwide could reach $20 billion in 2021, according to a report from the research firm Cybersecurity Ventures, up from nearly $12 billion in 2019.

$447K

Average cost to colleges to resolve a ransomware attack.

Source: BlueVoyant

That number may not account for the full total, as private companies often don't report ransomware attacks or whether they've made any payouts. "There's a bit of a victim-shaming factor," Benack says. "People don't want to admit or go public if they don't have to." Colleges are often compelled to report cyberattacks — for example, any attack that exposes student PII at an institution that accepts federal financial aid must be reported to the U.S. Department of Education.

In the 2000s, if a hacker wanted to accept a ransom without running the risk of getting caught, he or she would have to use an instrument like a prepaid debit card, which is difficult to trace because it isn't attached to a bank account. But it's difficult to demand a million-dollar ransom using such cards. "The thing that really enables this enterprise-level ransomware is liquidity in the cryptocurrency markets," Savage says. "Suddenly, it becomes feasible to move a couple million dollars." Thanks to ostensibly untraceable payment methods like Bitcoin, hackers have become emboldened to demand substantial ransoms for a suddenly encrypted server or locked-up network, making ransomware more lucrative and attractive.

The rise of ransomware has raised the stakes for colleges and information-security officers. A cybersecurity company called BlueVoyant surveyed data from more than 2,700 colleges and found that the number of ransomware attacks doubled between 2019 and 2020 and were the primary cybersecurity threat facing colleges. The average cost to resolve an attack was $447,000.

Any computerized function a college needs or any data set it wants to regain access to could make a target for hostile lockdown, encryption, or threat of erasure. If almost any aspect of an institution's operations could be a target, "it's no longer sufficient to harden your most sensitive data," says Corn, of UC-San Diego. "You need to start looking at the general cyber hygiene of your environment." If hackers can crack one computer anywhere, it may allow them access to a college's entire network, where they can spend weeks, even months, exploring. "They call it 'dwell time,'" says George Finney, chief security officer at Southern Methodist University. "The average bad guy is in your network for 200-plus days before you know."

The Colonial Pipeline incident in the spring of 2021 demonstrated the larger dangers of ransomware to the entire coun-

try, after an attack shut down a major East Coast petroleum supplier, hobbling fuel supplies and sparking a run on gas stations across multiple states. That's the kind of problem that worries information security officers, says Corn. Losing data locked up on one machine, or one server, is bad, he says, "but what really is existential to us is not the loss of data, it's the unavailability of services and systems." The Scripps Health system in San Diego was hit with a ransomware attack in May 2021 that wasn't resolved for a month and made it difficult to treat patients. "That's the kind of problem we need to start worrying more about," Corn says.

Regis University, a private institution in Denver, had to scramble in 2019 when much of its computer network was encrypted by hackers at the beginning of fall semester. Administrators had to make hard copies of students' class schedules and professors' class rosters at a local copy shop and everyone picked them up at tables, says Shari Plantz-Masters, academic dean for the Anderson College of Business and Computing, like "we did 40 years ago."

Even when data can be recovered and operations resumed relatively quickly, the impact can be long-lasting. Just a month before a March 2020 ransomware attack on Metropolitan Community College of Kansas City, the college had adopted a cloud-first approach to its campus network and moved its core business functions and its learning-management system to the cloud. Cloud storage and cloud-based applications have given colleges and other organizations an invaluable tool in fending off the worst effects of ransomware. The applications were briefly inaccessible due to the attack, says John M. Chawana, vice chancellor for institutional effectiveness, research, and technology at Metropolitan. But, he says, "within a week, we had all our core business processes up and running."

Regis, too, had some of its data and processes in the cloud — that's how it was able to print out student records so quickly — but much of its data was locked up on servers on its premises, Plantz-Masters says, and for some functions "it might have been a month or two that we were disrupted and coming back." (The unencrypted, uninfected data that Metropolitan was able to rescue from its rebooted servers was completely disorganized and had to be re-sorted by hand — Chawana compares it to shopping at a Walmart if all the contents had been piled in dumpsters. It took staff members most of a year.)

45K

Attacks per hour detected by the University of California at San Diego.

Source: U. of California at San Diego

Then there's the question of how to respond to ransom demands. The hackers who hit Metropolitan demanded what Chawana calls "a substantive amount" of money to unlock the campus's servers, but college leaders decided not to pay. Leaders at Regis did pay an undisclosed sum to end its attack. The FBI and CISA officially discourage paying ransoms. "That's money right back into the R&D coffers of the malicious actors to develop new exploits to target more people," Benack says. Regis paid because the attack hit the institution "at a precarious time," writes Jennifer Forker, director of communications, in an email. "We needed to ensure we had all the possible opportunities to restore or rebuild the systems" and get its semester underway.

Paying ransom may not be the end of a college's troubles. There's a growing trend for hackers to pivot from ransom to extortion. First, they ask for money to give you your data back, Benack says, then they ask for more money not to make it public, or de-

stroy it. Paying ransom is also no guarantee that they won't be back. A report by Cybereason, a cybersecurity firm, estimated that 80 percent of organizations that paid a ransom were hit again, half of them by the same hackers.

Ransomware is a problem that's unlikely to go away anytime soon. "Modern cybercrime is like the purest form of capitalism that exists," Savage says, "where there are almost no barriers to entry, and you need very little capital to innovate." Hackers are rarely arrested, much less punished, and "the attackers know that there's a high likelihood that insurance will pay the ransom," says Brian Kelly, director of the cybersecurity program at Educause, the higher-education information-technology association. "It's sort of open season."

The growing frequency, and success, of ransomware attacks is making cyberattack insurance more of a challenge for colleges as well. "Frankly, there've been drastic rate increases over the last many months," says Paul Pousson, managing director for higher education at Gallagher, an insurance company that works with colleges. Insurance companies are also mandating that colleges beef up their network defenses, and if they don't, they risk having to take limited or even more expensive coverage, adding further cost at a time when many institutions subsist on tight budgets.

Colleges also need to keep their security plans up to date, says Chawana, of Metropolitan. After an attack, the college's security policy is the first thing regulators and insurers want to see. "In other words, Have you done your due diligence to be able to mitigate risk of such an attack?" he says. "If you have not, then the organization is liable."

PLAYING DEFENSE

Every year, colleges' cyberinformation-security officers learn more, get better tools, and improve at their jobs. But so do the hackers. What can colleges do to continue to defend against the rising tempo and sophistication of threats?

The most obvious tool is raising awareness of how to combat security breaches. The Cal State system, with its 23 campuses, was one of the first to announce it would conduct the 2020-21 academic year entirely online, committing its universities to a year of video classes and remote work, "so we did a lot of communication and awareness efforts with our staff," Hudson says. "Make sure your home systems are patched" — or updated — "make sure you're not using default passwords." It's the kind of messaging faculty and staff often already receive, often about practices they're already supposed to follow, say some cybersecurity experts. The messaging just needs to be reinforced.

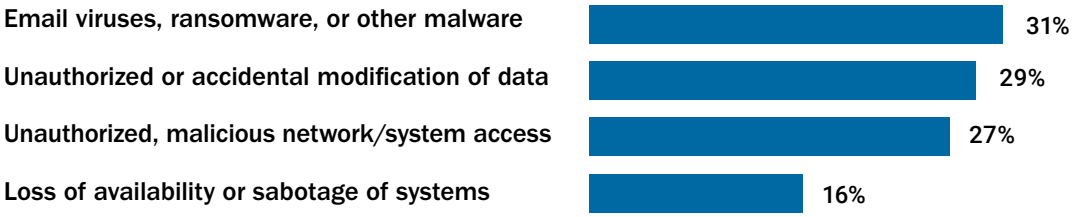
Awareness will only become more important in years to come. "I was asked one time if I had $100 to spend on information security, what would I spend it on, and I said awareness," Hudson says. "Our users are the front line." Cybersecurity success relies on good habits, says Ito. "We just need to reinforce all of those." In the wake of the successful ransomware attack against it in 2020, Metropolitan Community College mandated an hour of cybersecurity training for all employees.

How to do security-awareness training well remains an open question. Corn, for one, thinks most such training is "terrible" and too generic. "What we're doing here is really rejiggering our training to focus on bite-size specific things we want people to do," he says. So, instead of a quick lecture or a placard urging you to use strong passwords, Corn's team is working on a one-minute video that shows you how to use a password manager that sets strong passwords for you. "If security-awareness training consisted of the 15 most common things that people need to learn — how to use a strong password, how to recognize an email as a phish," he says, "that will help us an awful lot."

Awareness training can also be carried too far. Southern Methodist, like many colleges, has run simulated phishing exercises, which are essentially fake phishes sent out

Colleges' Biggest Concerns

Institutions rated the following as their most common information-security threats.



Source: Educause Information Security Almanac, 2019

by the institution to help teach employees and students how to spot the real ones. While the university has found the exercises valuable in teaching employees and students what to watch out for, Finney says, "we didn't want to create a situation where users are not responding to emails for days or weeks, and not interacting with our community the way that we want them to, because we were doing simulated phishing."

One of the challenges information-security officers face is keeping a system user-friendly while also keeping it secure. Tools like multifactor authentication, or MFA, which require a password and access to a certain device, such as a cellphone, to log in to an application or a network, can help keep interlopers out of a network. But it can also raise the frustration level of legitimate users. "If we make people go through six different logins to get to the personnel system just to update their phone number," says Ito, of Hawaii, "they're not going to do it, or you're going to make them go around your defenses." Across all colleges, the adoption curve for MFA is still at about 50 percent, says Kelly, of Educause.

Fortunately, there are some methods information-security officers can use in the background to monitor activity and improve security while the ordinary business of the institution continues. Many colleges have installed an endpoint-detection response system, which resembles "antivirus on steroids," Kelly says. Like the old desktop antivirus software, it scans for malware but it also looks for unusual activity. "If some other process or software activates or runs, and that's not something that is typical for behavior for your endpoint" — say, software that's installed on your computer that you never use boots up — "that could be a security indicator," Kelly says, and the system would alert information security, not the user. Other colleges also expanded the use of virtual private networks, or VPNs, encrypted connections to the network.

Some colleges, such as Southern Methodist, use deception to lure hackers by setting up "honey pots" or "honey nets" — essentially, decoy weaknesses designed to draw the attention of hackers — to "learn their MOs, their techniques that they're using to get in, so that we can use those live techniques to help improve our networks," Finney says.

Chief security officers have a handful of essential steps they say will be most likely to contribute to better cybersecurity for colleges in the years to come. The most commonly mentioned one is increasing information-security staff. "I would hire more people," Corn says. "And I'll tell you what's ironic about that, is when I talk to my counterparts, even at [institutions] with huge staffs, they'll say the exact same thing." Sophisticated software handles the scanning of all login attempts and network anomalies at any college, but decisions

about what constitutes a problem and how to act on it — and how to prevent it from happening again — require a human brain.

Corn says that UC-San Diego's information-security technology collects more than half a billion individual incidents of network activity every day and could probably collect double that. Machine learning handles a lot of the initial triage. "But I think you'll find very few security professionals believe they are maximizing the return on any specific technology they're using," he says. "It takes people dedicated time to sift through that data."

Some colleges are bolstering their technical systems and human resources in other ways. Leaders at Metropolitan and Regis, for example, who have learned about ransomware the hard way, have made changes aimed at minimizing the chances they'll have to deal with it again anytime soon. Chawana, of Metropolitan, believes even more strongly in the cloud now, and any new system the college considers would need to have cloud backup. The college has eliminated all "legacy tech" — older machines and software no longer supported by current technology that could lead to vulnerabilities. Regis has also moved toward cloud backup for its network and tightened the processes through which staff and faculty bring new equipment or software into the network, "because every time somebody introduces something new, they also introduce a risk that may not have been managed," says Plantz-Masters, the Regis dean. If someone wants to add a new hosting agreement or new system, they have to submit to a screening process that includes risk assessment.

One way to better protect institutional data will be to have better control of the data a college keeps on hand. "We're digitizing a lot of information at a really fast clip," says Washington, of UC-Davis. "I can't even begin to imagine how much data we have." But the university is beginning to try. About five years ago, it formed a data-governance council to begin evaluating the data it holds, whether it's all necessary, and whether it's adequately stored and protected.

Data-governance programs not only help colleges better administer the data they have in hand, such programs also help them establish better policies for the future. For example, members of the data-governance program at the University of Hawaii grew concerned that textbook publishers may have been collecting data from students downloading the ebook editions of their products. "We didn't know what information is being collected, or how it's being collected and how it's being used," Ito says. "We're letting the publishers know that they should not be collecting data beyond what they need."

For Ito, data governance isn't just a matter of making sure the university's flanks are covered by trying to minimize the data being collected. It's part of the educational mission, too. She says she wants people to "understand where their data is being collected, and how that makes them vulnerable." Ito cites the DriveSure data breach in January 2021, which resulted in more than 3 million people having their personal identifying information posted on the dark web. "My name is in that," Ito says, "and I don't even know what DriveSure was. How did my information get caught up in that breach? I still don't know."

Perhaps the ultimate defense against hackers' devastating attacks is using tiered architecture in computer networks. The typical network architecture favored by an organization like a college assumes that anyone with access to one part of the system should be able to use most of the other parts. Such a structure "makes it easy for a threat actor to traverse the network," Hudson says. Hackers gaining access to a desktop computer might make their way to the network's active directory — something like a combination of the system's security guard and air-traffic controller — and from there, he says, "you kind of have the keys to the kingdom." Reorganizing the network into tiers isolates sensitive areas like the active directory to a separate, more isolated

tier, with servers on another tier, and user endpoints on a third tier. "That way, if a bad guy gets in," Hudson says, "they can't move willy-nilly around your network."

Rearranging a working network is a complex task, and the bigger the network, the more complex it is. UC-San Diego, for example, might have up to 250,000 computers on its network during normal operations. But some network segmentation can be achieved on a smaller scale, and with fewer resources, says Kelly, of Educause. Rather than thinking about making changes at the level of switches and routers and other network hardware, information-security officers can now do more to limit what "users have access to on your network based on who they are or where they are," he adds. "A lot of that doesn't require as many technical, architectural changes on the campus network."

Colleges can benefit from moving toward a "zero trust" approach to cybersecurity, Kelly says. In the past, most organizations assumed that if you were inside its computer network, you belonged there. A zero-trust environment presumes that any user could be a bad actor, and puts extra precautions and layers of scrutiny in place. End users such as professors, administrators, and students would need multifactor authentication to get access to the network, and then might be able to see only the most limited parts of it, based on their needs. Creating such an environment is more affordable than rearranging network hardware.

Network segmentation is one of many factors, along with using multifactor authentication and backing up data, that cyber insurance underwriters increasingly look for when determining the parameters and costs of a college's policy. Even though cybersecurity expenditures like network segmentation might be a low-budget priority for college leaders, they need to understand that "there's a reason why the underwriters are asking for it, and to keep that on your horizon of improvements that need to be made," says Stacie Kroll, executive director for higher education at Gallagher, the insurance company. "This is the trend. The claims are not going away. The cyberattacks won't go away."

Regis University has increased its spending on cybersecurity infrastructure "because we have to," says Plantz-Masters. While Regis was lucky and no student or employee data were exposed during the ransomware incident, "the urgency to improve the investment to protect all of that became very real to us," she says. "When you're not threatened, or you haven't experienced that kind of an attack, the urgency may not be where it needs to be. I wish that we had recognized that urgency before the attack."

Benack, of CISA, believes there needs to be a shift in thinking about budgeting for cybersecurity — from thinking about it as a cost center to thinking about it as an investment. "It's not just about spending money to keep something negative from happening, which it definitely is," he says. "It's about spending money to enable something very positive to safely happen. It can enable you to deliver services more effectively to increase revenue, to increase reliability."

FUTURE THREATS

The rapid development of technology will provide new tools for fighting off cyberattacks, but it will also provide new tools for hackers and introduce unpredictable twists. It's hard to predict the future — other than that more challenges are a safe bet.

Future challenges have appeared, however — some distant, and some just starting to loom.

Perhaps the most immediate wild card facing information-security officers is the uncertainty surrounding a new set of federal standards regarding cybersecurity for research. In the fall of 2020, the federal government rolled out the Cybersecurity Maturity Model Certification framework, which mandates tougher cybersecurity standards for university labs that do research funded by the U.S. Department of Defense. The new standards resemble

Advocating for Resources

The most obvious thing college leaders need from their chief information-security officers is a computer network that functions free of hacker incursions and other threats. Cybersecurity officers need things from leadership to do their jobs well, too — primarily backing from the top and sufficient resources. How can presidents and CISOs communicate effectively with one another to make sure cybersecurity receives due attention among all the critical institutional priorities a leader must juggle?

Veteran information-security officers recognize there's room for improvement. "We in cybersecurity have done a pretty terrible job as a field of explaining our role to campus executives," says Michael A. Corn, chief information-security officer at the University of California at San Diego. "We need to raise our game and how we communicate with the leadership."

Leaders often respond best when they're engaged on their terms. When discussing cybersecurity with leaders, "we have to be delicate and poised in how we will talk about these issues, and try to demystify them," says Cheryl W. Washington, chief information-security officer at UC's Davis campus. A good information-security officer "is going to find a way to have a conversation about cyber, but put it in the terms of the language that leadership will understand — the language of the academy, the language of business — as opposed to the language of technology," she adds. The same principle applies to data. Rather than simply reciting a statistic, such as how many suspicious user accounts the information-security office locked last week, for example, relate those actions to how they affected, or didn't affect, the college's ability to operate.

Money can be the determining factor in cybersecurity success, but it's in short supply at many colleges and always the source of competition among units. Some information-security officers will use fear as a motivator to get more money at budget time, says George Finney, chief security officer at Southern Methodist University, "and it's easy to do, especially when things like ransomware are covered so heavily in the media." At the same time, the threat is real, and "if you start skimping, then you end up in the news," says Michael H. Hites, chief information officer at Southern Methodist. It's important for leaders and information-security officers to have regular conversations about "what's the state of the art look like, and what's the state-of-the-art cost," Hites says, "and then how far up that ladder should we go?"

Data are also important to the conversation about money. "If I can use real data in my real environment to show we're seeing a million cyberattacks a month with this particular vector, then, oh my gosh, of course people are going to want to help," Finney says. "If instead I just beat them over the head and say, We're going to get hacked, and this is terrible, and the sky is falling, people are going to see me as the boy who cried wolf." Finney also suggests running information-security pilot programs that can generate data and support the business case for additional spending on cybersecurity.

Information-security officers must be judicious with the resources entrusted to them. "We need to be exceptional stewards," Corn says. "The institution is full of people that can make a terrific case for more resources."

preventive health care for data. In addition to eating properly and exercising, "you also have to go see a doctor, and the doctor conducts tests and makes recommendations," Corn says. "What you're going to find for your research environment is something very analogous to that."

The uncertainty lies in how far new federal standards will expand. Corn believes that the next five years or so will see "a proliferation of pretty draconian security requirements coming from all federal agencies that offer grants or provide data." Some college information-security officers and researchers are concerned that other grant-awarding federal agencies, such as the National Institutes of Health, may also adopt the more-rigorous standards.

Protecting research in general may be one of the bigger challenges information-security officers face in years to come. A large university with a medical center might have thousands of research labs, and few of them may be under the full and consistent protection of institutional cybersecurity.

There are good reasons for that. Research labs are akin to the Wild West, as far as cybersecurity goes. Almost by definition, research is heterogeneous and experimental, and one-size-fits-all equipment and software issued by the institutional IT department wouldn't be suitable. Most research IT and cybersecurity is grant-funded, custom assembled, as inexpensive as possible, and run by graduate students. It also tends to be "much less conservative" than what a college IT department thinks about, says Savage, the cybersecurity researcher, such as making more use of cloud storage. "There is such innovation in all of these services, and it's cost-effective."

Information-security officers can protect office computers or core network functions, but they often don't have a grasp of how research labs function. "Security people don't understand how research works," Corn says. The information technology that researchers use often doesn't rely on standard applications or equipment, and they may work with bigger data sets or different types of networks. "A lot of times when we go into a lab, even when they're doing something correctly, they're doing it in a way that we don't know they're doing it, because they're building their own tools," he adds. "And so we have no visibility."

The good news, relatively speaking, is that the temptation for hackers to break into any given lab may be low. The overwhelming number of attacks are driven by profit. Hackers can often count on a payoff for returning specific data related to defense or proprietary information, or in ransoming particularly valuable research. In 2020, a hacker group forced the University of California at San Francisco to pay a $1.14-million ransom to release data that the hackers had rendered inaccessible by encrypting it on servers belonging to the institution's School of Medicine. But locking down one lab's data might be unlikely to draw a fat ransom, so it may not prove too tempting a target.

Growing threats and rising security standards mean that colleges need to do a better job of supporting research cybersecurity, and that will require relationship-building. Information-security officers need to get better at reaching out to researchers, making themselves a resource without getting in the way, and they need to start now.

The continuing evolution of technology could bring both benefits and drawbacks. Artificial intelligence and machine learning continue to help information-security officers sort through data and assess threats more efficiently than ever. "At the same time, the hackers are going to use machine learning and AI to attack me more efficiently," Corn says. "In the next five to 10 years, it's going to be very interesting."

Quantum computing, a theoretical field that might enable engineers to build devices based on subatomic particles instead of transistors, could boost computing power astronomically. Again, this could provide enormous benefits for society, but such high-speed computing capacity could also make traditional encryption obsolete.

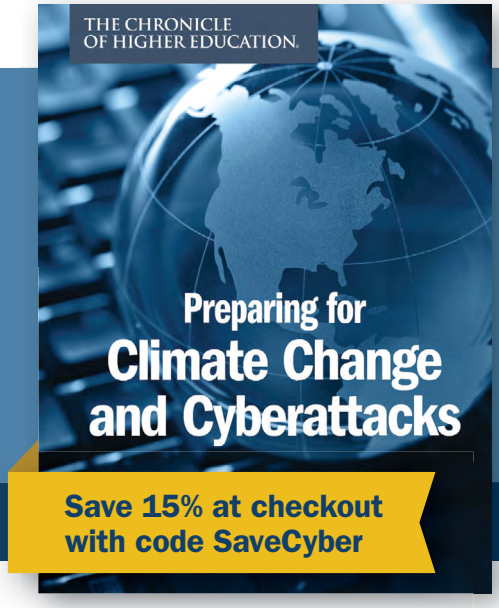
Perhaps the biggest challenge ahead, now and potentially in the future, lies with the information-security work force. Colleges must compete for a limited pool of cybersecurity talent with the private sector, which often has much deeper pockets, and many institutions already struggle to hire for open information-security positions. "That problem's going to grow considerably as more and more organizations inside and outside of higher education begin to realize that they need somebody to help lead their cybersecurity efforts," Washington says. "Imagine if you're in that position and can't find anyone to fill that role. What do you do?"

The good news is that colleges have part of the solution at hand — offering cybersecurity degrees and certificates. It's incumbent on leaders in higher education, says Hudson, to help build up the information-security work force, for the general good and for the good of their own institutions. It's also important for colleges to nurture the information-security personnel they already have. Most cybersecurity pros can make more in the private sector, so institutions have to provide "meaningful tasks for them to accomplish, and we also have to support them in continually educating them and helping them become the best they can be," says Bob Turner, chief information-security officer at the University of Wisconsin at Madison. "We do invest in our people, we invest in certifications, we invest in seminars and other things that they can go to and learn more." Professional development benefits both the employee and the university.

Ito's pitch for students of any age is pretty effective: "If you want a permanent career, cybersecurity is the place to be."

Preparing for Climate Change and Cyberattacks

How institutions can plan for existential threats



Uncovering weaknesses can be among the most valuable lessons learned from emergencies. It's also among the hardest.

PURCHASE THE FULL REPORT

The last several years have shown how quickly and drastically the unthinkable can upend colleges' expectations. Climate change and cyberattacks can seem so far off that they become low priorities on a day-to-day basis, but their impact on colleges' campuses, operations, and ability to achieve their missions can be existential.

To manage these challenges and many more, colleges will need to adopt a 21st-century conception of resilience — the ability to survive and thrive amid evolving and intensifying threats. This *Chronicle* report tackles how to plan and prepare for the unimaginable so that your institution can respond to the unpredictability of emergencies.

Order this report to:

- Understand the importance of revising and practicing emergency plans and risk assessments.
- Explore how climate change is affecting colleges in different regions of the country, including unexpected consequences for enrollments and budgets.
- Discover how other colleges have responded to data ransoms with strategies that help fortify cyber operations against attack.

THE CHRONICLE OF HIGHER EDUCATION

SCAN NOW TO PURCHASE

Purchase your copy:
chronicle.com/CLIMATECHANGEANDCYBERATTACKS

For information on group pricing, please contact us at 1-800-728-2803

From breaking news to key insights to real-world advice, *The Chronicle of Higher Education* is dedicated to serving academic leaders and professionals. Our newsletters, subscriptions, special reports, virtual events, and exclusive data projects provide a comprehensive view of the latest trends and critical issues affecting academe. For more than 50 years, higher-education professionals from around the world have trusted *The Chronicle*'s in-depth reporting and analysis to understand their world and make informed decisions.

THE CHRONICLE
OF HIGHER EDUCATION®