The job of network defenders in higher education hasn’t gotten any easier as colleges, universities and institutes have reopened for on-campus teaching and learning. Taking the right cybersecurity posture will position your school for maximum flexibility. These do's and don'ts can make the difference.

Colleges and universities have entered a competitive landscape unlike any they’ve ever experienced. Continuing enrollment declines linked to rising tuition costs, more young people choosing "jobs over class" and lingering "pandemic paralysis" have sent institutions scrambling for quick and decisive moves to draw new students into their communities and ensure the students they’ve already enrolled will stay with them.

One bright spot that has emerged in the disruption of the last two years is the wide adoption of hybrid learning. Giving students flexibility in how and where they take classes is proving a differentiator. Those institutions that have chosen to continue investment in online course development will gain reputations as being “more student-centered,” as Harvard Business Review recently noted, while those pulling back from online options are seeing just the opposite.

The hybrid theme is playing out well for other aspects of campus operations too. As employers all across America are finding, the current workforce is less inclined to want to go into an office every day. Leading schools are finding ways to make flexible work policies sustainable for the long haul. Ohio University, as one example, projects a dramatic
uptick in employee retention and major savings tied to a reduction in campus building usage requirements from its Ohio FlexWork policy.

Delivering flexibility and enabling people to learn and work from anywhere at any time on any device requires a rock-solid approach to cybersecurity. You need to ensure that the right users are getting access to the right assets, the right data and the right applications. Otherwise, any new services offered to students, faculty and staff could turn out to be new vectors for attack.

The Big Target on Higher Ed’s Back

It’s no secret that higher education has become a ripe target for cybercrime. In 2021 the FBI identified one pernicious flavor of ransomware, PYSA, as specifically targeting education. Shortly after that warning was published, Moody’s determined that cyberattacks were a “negative factor” weighing on the credit worthiness of the higher education sector.

So, it’s little wonder that the top-ranking item on Educause’s latest “IT Issues” list, once again, is cybersecurity. Even a single break-in, the report stated, “can cause loss of reputation and loss of educational opportunities for students, as well as financial and reputational issues for both the campus and the individuals impacted.”

Not only are systems and personal data at risk, but research content has become a particular favorite for cybercriminals and nation-state agents. As Cisco Cybersecurity Principal Peter Romness pointed out, “unique challenges” are making research institutions “attractive to hackers”:

- Universities tend to favor open environments
- These organizations have large volumes of sensitive data, which is frequently maintained in a dispersed way — in individual research labs or even on individual researchers’ computers
- Personal devices, which are likely to contain sensitive data, are often put at risk when users check into personal services — e-mail, banking — on public WiFi and then shift to institutional networks.

Romness works in Cisco’s U.S. Public Sector CTO Office, where he rolls up his sleeves to immerse himself in cybersecurity work at numerous institutions of higher ed and government agencies. These days, conversations with IT leaders and professionals tend to focus on guidance that can be distilled to a handful of do’s and don’ts.

DO prioritize zero trust.

Taking a zero-trust stance means two things: First, every time someone or something requests access, there’s a check to make sure that person or system should be getting access. Second, it provides defense-in-depth. If bad guys do get into one part of the network, they can’t get to the other parts.

Romness said he considers zero trust at the heart of hybrid flexibility. “The whole goal of a university is not to secure data; the goal is to teach students. But securing data is a way to get there,” he explained. “Zero trust is a great way of looking at your security posture and making risk-based decisions.”

The long-range goal is to gain granular access control to every asset in the environment. His plain advice: “Start doing things that that can help with that.”

DO pursue fast time-to-value projects.

These are efforts that make for a “huge improvement quickly and easily.” The right DNS protection, for example, can prevent users from surfing to websites that serve up malware or provide backdoors to criminals. Multi-factor authentication is another such example.

“MFA is widely acknowledged to eliminate probably 90% of phishing effectiveness,” said Romness. “Even if someone gets hold of a username and password, with MFA, it doesn’t do them any good because they don’t have that other factor — or they have to take huge steps to get around it.”

Romness acknowledged that MFA has long been considered a “big pain for the user.” That’s no longer true. “MFA is not that hard anymore. You don’t have to type in a long series of digits that get e-mailed to you or carry around a fob. You just say, ‘Yes,’ on your phone.” That gets rid of user resistance quickly.

Plus, implementation has become “super-fast,” he added. “We have universities that implemented our MFA solution, Cisco Duo, in a week.”
CISCO SECURITY SOLUTIONS IN BRIEF

Cisco's Secure Remote Worker combines multiple products into one single integrated solution, making it easy to enable secure access and defend remote workers:

- **Cisco Duo** provides multi-factor authentication and single sign-on, to safeguard users, devices and applications.
- **Cisco AnyConnect** virtual private network ensures highly secure access to the institutional network.
- **Cisco Umbrella** delivers a fast, secure and reliable internet experience to users, blocking the internet's infrastructure from malicious and unwanted domains, IP addresses and cloud applications.
- **Cisco Secure Endpoint** offers a cloud-delivered next-generation antivirus endpoint protection platform and advanced endpoint detection and response. Using the worldwide threat intelligence of Cisco Talos, it will block attacks before they can target individual institutions or users.
- **Cisco SecureX**, available to security customers at no extra cost, unifies visibility and enables automation. Should a new threat arise, IT can click on the warning message in the console, to pull all indications of compromise and check them against every one of the secured devices in the environment. No more manual hunting.

These programs work together to make the overall security stance more effective, without human intervention. Should malware infect a staffer or student’s personal device, for example, Secure Endpoint will quarantine the malicious file and automatically inform Duo to block critical system access until the infection is eradicated. SecureX will keep IT informed all along the process.

**DO simplify the work with cloud.**

Like MFA, cloud security can help get operations up and running faster and make them easier to manage, said Romness. However, his preference is always to push a “cloud-smart” approach over a “cloud-first” mentality.

“Cloud security and cloud apps can help you get things up and running faster and make them easier to manage, but they can get expensive and may not be the right fit for every situation,” he explained. “If it’s something that you have an interest in, if it’s something that you’re going to use a lot of, if it’s something that is going to be in place for a long term, you may find that you have more control and end up saving money by bringing it on site. But you also really have to keep things up-to-date. You have to have the staffing to verify that the latest threats and modes of attack are taken into account. In those environments it may be smarter to pay a company with a bunch of smart people.”

Romness’ advice is to weigh options and consider how the outcome fits into your long-term security architecture plan.

**DO turn security modernization into learning and development opportunities.**

The integration and automation available in leading security tools provides a level of visibility and response that has never existed before. The result is that you can catch anomalies before they become major issues.

“Having that ability to see what’s going on in the whole environment is a huge thing,” said Romness. “You can see that someone is sending a bunch of data from a secure server out over the internet. And there may be a very logical reason for it, but you definitely have to check it and see why.”

Modern tools also enable IT to act quickly — quarantine a personal device, shut down a server — "without a huge investigation, without a huge investment of time.”

Those capabilities do something else too, Romness
emphasized: They make the job of the security defender “less sucky.” As he noted, “Instead of the monotony of going through reams and reams of data, checking logs or changing access control lists, your people can see something and respond quickly. That makes their jobs better; they’re able to up their capabilities; and you’re able to keep them happier on the job and retain them.”

At the same time, programs exist to outfit your campus with free curriculum, security products and other instructor resources to help educate students for careers in cybersecurity.

The Cisco Networking Academy provides programs licensed at no cost to public colleges and universities, supplying instructor training, Cisco products, lessons, assessments, labs, simulations and games, to help students earn full Cisco credentials, including the Cisco Certified Network Associate in Security.

Cisco’s new “Cyber Defense Clinic” can help your campus educate students, by providing them with hands-on interaction with the latest security tools, to hone their expertise in hacking defense.

DO seek help from the experts.

There’s no reason to go it alone with your cybersecurity work. A number of federal agencies and other organizations have developed voluntary resources to help schools grapple with the complexity of the challenge.

As a starting point, Romness steers the people he works with to the National Institute of Standards and Technology (NIST) Cybersecurity Framework, which provides standards, guidelines and best practices for managing cybersecurity risk. IT teams can use the framework to do an assessment of current state, compare that to desired end state and create a plan for moving forward.

“Once you self-assess where you are and where you want to be, either you can hire somebody to help you with that or you can do it yourself,” he advised.

The framework also creates a common language that allows the IT organization to share needs with approving bodies, such as the chancellor of the university or the board of trustees. “It gives you that credibility when you say, ‘We are lacking in these things that NIST says are important,’” Romness said. Should a security event occur, he added, “It gives you something to stand on to
be able to say, 'I made the right risk-based decisions.'"

MS-ISAC, the Multi-State Information Sharing & Analysis Center, a division of the Center for Internet Security, is another resource universities and colleges have found invaluable, Romness said. Free to public institutions, MS-ISAC helps schools with benchmarking their cybersecurity stance, develops controls for simplifying cybersecurity compliance and can come to the rescue when a security event occurs that the institutional IT team considers beyond its abilities.

DON’T put all your trust in patching.
Not that long ago, patching was the answer to sturdy cybersecurity. As the thinking went, major breaches occurred when software with vulnerabilities was cracked. Patching those cracks would stop the damage.

But patching will only get you so far, asserted Romness, especially in a higher ed setting. Most IT managers are “overworked and super-busy,” he observed, which makes it tough to manage thousands of computers that need periodic updates. In the university environment they may not even know all the systems that exist. "Managing updates on so many different pieces of software, on so many systems, can be overwhelming, and effective updates may slip through the cracks," Romness said.

Also, the school may use older, custom-written applications that can’t be updated because the software they’re based on is no longer supported. “But the outdated software continues to be used for the simple reason it gets the job done,” he pointed out.

Romness offered other barriers to effective patching:

The problem that patches need to be tested — a time-consuming process of testing, approval and implementation that “can strain limited resources.”

If computers are part of mission-critical systems that keep the organization running, they’re difficult to update because they can’t be taken offline. Some of them may still run Windows XP, an operating system that reached end of support in 2014.

It takes time to create and distribute patches for new vulnerabilities, which means “new or undiscovered malware can slip through the latest patch.”

Then there’s the user problem. “User behavior can often be the source of malware and data loss. Even with security training, members of your organization...”
may be tricked into giving away information, have their password stolen, or mistakenly share information. And, unfortunately, some may have bad intentions,” said Romness. "In these cases, patching will not protect you.”

"While it’s essential to patch, you can’t always be perfect,” he said. "So, you need these other security capabilities — zero trust, multi-factor authentication and so on — as the backup.”

"The pandemic really highlighted the need for schools to make their students happy and keep them coming, because it really has hurt the bottom line of many universities,” Romness said. “Having good wireless on campus has become something that students use when they’re trying to decide what college they’re going to go to. It allows colleges to deliver psychological counseling, scheduling and other services via the laptop. That gets back to flexibility — what you can provide for all of your students. It becomes a differentiator for schools.”

“You want to wow your students and teachers in a good way,” Romness observed. “You want them to say, ‘Wow, I didn’t know I could do this. This is really great.’”

DON’T minimize communication.

Outreach entails keeping cybersecurity in front of users consistently. Romness has worked with institutions that make time for the chief information security officer to speak during student and new faculty orientation. The main message: Don’t hesitate, even when you think you’ve done something wrong. Reach out to IT when you have problems with your computer.

He’s also seen schools put up cybersecurity-related signage in unexpected places, such as restroom stalls, to inform people about why they need to be alert and how to counteract attacks.

While IT may want to block access to websites from university users, it’s almost always a bad idea, Romness suggested. "Just as they decide to block what they consider a horrible website that nobody should go to, some professor will say he or she is doing research on it, and legitimately. They have to be able to provide those exceptions for those people.”

The overall goal with communication is twofold: to keep people informed about specific risks that are cropping up and how IT is countering those risks; and to be “very open about what you’re not allowing people to do and why.”

DON’T underestimate the power of cybersecurity to make your institution more competitive.

While nobody chooses to attend an institution because of its security stance, security is certainly an enabler. Without top-notch cybersecurity, a college or university is unlikely to be able to provide safe access.

DON’T assume cybersecurity is one and done.

Putting security measures in place isn’t the kind of work that’s ever completed. Romness likened it to a journey toward continual improvement.

With each step, he said, “you have to start making decisions that improve your security posture.”

That’s why he has encouraged the colleges and universities he works with to consider adopting a cybersecurity framework such as the one from NIST or the Cybersecurity Maturity Model Certification (CMMC). While CMMC is intended for contractors that work with the Department of Defense, there’s applicability to higher education too, especially those doing federal government-sponsored research.

In November 2021, the DoD announced a new strategic direction for CMMC, which broke the framework into three tiers of security protection, depending on the nature of what needs to be protected. CMMC 2.0, as it’s called, maintains the program’s original goal of safeguarding sensitive information, while also simplifying the standard. The most basic level of maturity involves 17 security practices and self-assessment, Romness explained. As the levels advance, there are more security practices to be put in place and heightened levels of assessment to be done.

The point, he said, is to begin wherever you are and build on that. “Nobody has the capability to spend money upfront and just put everything in. The technology is oftentimes the easiest part. All the other things that make it hard are the people, processes and policies that go along with it.” Growth that’s incremental is growth all the same.
DON’T ignore the security opportunities available with relief funding.

While colleges and universities aren’t exactly awash with higher ed relief funding, the $40 billion available from HEERF III (half for student financial aid and half for institutional needs) can help pave the way for positioning them to be prepared for whatever comes next. Cybersecurity as a foundational element of the IT infrastructure should be part of those considerations.

As Romness works with institutions, he advises them to “come up with a long-term plan and then an implementation plan that includes a short list of needs.”

"Begin with the end in mind," he suggested. "Create a list based upon long term needs and go for relief grants to cover the expense."

If IT lacks the skill set to handle the applications necessary for pursuing funding, Cisco employs professional grant writers "who can help customers write their grant proposals."

Establishing the Better Approach

Delivering a reliable, efficient, high-performance hybrid learning environment and addressing the many needs of a hybrid workforce requires a re-energized IT approach. To speed up the work, choose a partner that can address the entire breadth of the IT infrastructure. In those matters, Cisco is always the one to beat.

In the last five years, said Romness, Cisco has acquired a number of security companies and invested heavily in integrating those technologies into a “one-of-a-kind platform” to make the job of defending the institution easier and more effective.

“You no longer have to look at multiple screens in different products or learn how to set up parameters in different software programs,” he pointed out. “We’ve applied machine learning, to make it easier to set up and defend networks and develop a more holistic security posture.”

As a result, university customers have increased visibility into their networks, said Romness. “That allows them to catch anomalies before they become issues, and they gain a simple, open and automated security approach to better protect their organizations against growing threats.”

GAINING DEEPER USER VISIBILITY FOR HYBRID LEARNING WITH CISCO

California Baptist University, with more than 11,500 students, had already begun the pivot to a hybrid education before COVID-19 closed the campus. The reasons, according to Tran Hong, associate vice president of technology and CIO, were many; but the primary one was the freedom hybrid learning provides students, especially when faced with family emergencies, childcare issues or the inability to reach campus due to pandemics, weather or other unexpected events. As part of the transition CBU deployed Cisco solutions, including Cisco Identity Services Engine, Umbrella and Cloudlock, to provide deeper visibility into the network, endpoints and the cloud, while protecting users, their data and apps. That implementation encompasses the adoption of automation for security to free up the university’s small IT staff and resources for other projects. Automation, according to Hong, can provide deeper visibility into the network and greater insights into user behaviors; helps identify potential threats before they’re activated; and speeds remediation if a break-in does occur. Learn more.