



Planning for the Worst Day

IT security in the new normal requires a combination of human smarts, planning and preparation, peer guidance, and well-chosen technology. Anything less and you're putting your campus community at risk.

IT HAS BEEN A HARD YEAR FOR THOSE IN CHARGE of cybersecurity, especially so for people who handle information security in colleges and universities.

According to [one report](#), ransomware campaigns against higher education doubled in 2020 compared to 2019, with an average ransom demand of \$447,000. "This criminal targeting of the education sector, particularly at such a challenging time, is utterly reprehensible," [stated the director of a national cybersecurity center last fall](#).

The seemingly unstoppable assault on higher ed could almost be predicted. Traditionally, criminals tended to be opportunists; they'd strike at random and hope to get lucky. Now they've organized into highly sophisticated networks and

common infection vectors, allowing an attacker to gain access to a victim's network through weak passwords, polished phishing, lack of multi-factor authentication, insecure RDP configurations and unpatched software. Once inside the network, the attacker may destroy backups and auditing devices to thwart recovery, they may encrypt whole virtual servers, and they'll use pre-written scripts to deploy malware to automate the destruction of other resources.


Zero-Trust and Defense-in-Depth

Some institutions are better positioned to withstand cybersecurity attacks than others. A combination of zero-trust and defense-in-depth allows these schools to defend against malware and ransomware. A zero-trust approach means that nobody is trusted, whether they're inside or outside the network. When users try to log on to network resources, they have to verify who they are, where they are and why they should be allowed access. Defense-in-depth requires multiple, overlapping layers of security controls. Should one layer fail, another one is ready to protect.

Technology plays a critical role in cybersecurity oversight. Among the components to arm your operations with are:

- **VISIBILITY.** Campus IT needs a consistent view into how data flows through the network, cloud and endpoints. Otherwise, security systems will continue to be a hit-and-miss remedy.
- **AUTOMATION OF THE "EASY" STUFF** and use of artificial intelligence to keep up with the onslaught of attacks, recognize where anomalies have surfaced and do remediation without the constant need for human intervention.
- **FRONTLINE DNS DEFENSE** to stop bad traffic coming from a multitude of remote directions long before it hits the network infrastructure.
- **SMART USE OF THE PUBLIC CLOUD** for maintaining secure backups without the burden or expense of doing storage administration in-house.

Two other non-technical elements also play a role in the success of information management success. One is the



Two non-technical elements also play a role in the success of information management success. One is the use of community insight, such as that provided by Internet2's NET+ program, to make sure the school is choosing the right security solutions for campus use and getting the best pricing for it. The other is making sure IT staff isn't burdened with boring work.

cartels that will target any entity of substance they consider a viable target. Higher ed fits the profile. Schools have long collected plenty of personal data and developed valuable research while also trying to maintain an institutional personality that values openness over restriction. But the pandemic opened the floodgates, as people headed home to work and learn. [As one analysis put it](#), "A greater reliance on home networks, a need to prioritize continuity over security and a rapid increase in points of attack will always make an organization more vulnerable to cyber threats."

Remote access systems, including remote desktop protocols and virtual private networks, offer the most

Cybersecurity Response

Campus Technology • PULSE SURVEY

5 top cybersecurity roadmap challenges

- lack of budget
- fear of phishing e-mails
- concerns about ransomware attacks
- lack of cybersecurity training
- mobile device security

4 in 10

IT professionals continue seeking solutions to boost student device protection

Colleges and universities are using these 3 top solutions to protect student devices

36% Identity management

30% Anti-virus

26% Anti-phishing/e-mail spoofing

How the pandemic has reshaped higher education institutions' cybersecurity incident response

39%

seeking opportunities to improve capabilities

27%

still adapting to the shift to virtual

24%

putting finishing touches on their strategy

11%

strategy unchanged

Source: Campus Technology

use of community insight, such as that provided by Internet2's NET+ program, to make sure the school is choosing the right security solutions for campus use and getting the best pricing for it. The other is making sure IT staff isn't burdened with boring work. Employee turnover can slow cybersecurity momentum. By adopting tools meant to handle the mundane work, the more interesting jobs are left for staffers, increasing employee engagement and investment.

A Positive Outcome from the Pandemic

If the pandemic has posed innumerable security problems for schools, it has also uncovered one positive note: Numerous colleges and universities have used the time to get their houses in order. A Campus Technology "pulse survey" among IT leaders and professionals found that two-thirds of institutions (63%) have reshaped their cybersecurity incident response, either putting the finishing touches on their strategies or improving their capabilities.

The biggest challenge they've faced would probably be of little surprise to anybody in the IT space: lack of budget, cited by 27% of respondents.

But that wasn't the only hurdle mentioned:

- **13%** cited worries about keeping up with phishing e-mails;

- **12%** were concerned about ransomware attacks and lack of cybersecurity training; and
- **10%** mentioned mobile device security.

Other fears included a lack of qualified cybersecurity personnel, data breaches, password theft, identity management, theft of intellectual property, regulatory compliance and a denial-of-service attack hitting the website or network.

The protection of student devices was on the minds of most respondents. While four in 10 reported that they are continuing to seek solutions for boosting protection on student devices, the rest are using some combination of identity management (cited by 36%), anti-virus (30%) and anti-phishing software (26%).

Ultimately, the job of the cybersecurity professional in higher ed is to "plan for the worst day," as one cybersecurity expert recently noted during a **Campus Technology leadership summit**. "If ransomware were to happen to you, what's your plan? What will you do? Do you have security controls in place? Are you doing all you can to protect yourself? Where are your backups? Are they isolated so the bad guys can't get at them? When you're facing your worst day, making sure you've done all you can, knowing what to expect and how to respond, will be a huge benefit."