Sponsored by

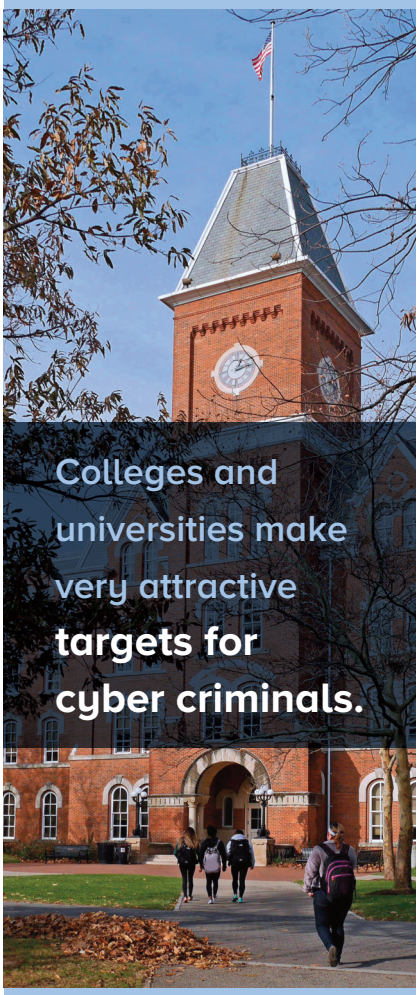
Spectrum ENTERPRISE

WHITE PAPER

7 CYBERSECURITY FACTS

EVERY CAMPUS LEADER SHOULD KNOW

eCampus News



7 cybersecurity facts every campus leader should know

Colleges and universities make very attractive targets for cyber criminals. As education has become more digital in nature, the use of mobile devices and smart classroom tools has increased the attack surface available to hackers. College networks also have large amounts of sensitive information that institutions might be willing to pay to get back.

What's more, higher-education networks are particularly vulnerable to attacks because of the highly collaborative nature of research and scholarship. And because campus budgets tend to be tight, especially for public colleges and universities, cybersecurity is often an underfunded area.

Cyberattacks might not be completely avoidable, but there are steps that campus leaders can take to reduce the odds of a successful attack and protect their sensitive data. The first step is to understand the nature of the threats they face and where they are most vulnerable.

To enhance this understanding, here are seven cybersecurity facts that every campus leader should know — along with recommendations to help institutions keep their networks and data secure.

1 Cyberattacks pose an existential threat to colleges and universities.

In December 2021, Lincoln College in Illinois was hit by a cyberattack that paralyzed key operations such as admissions activities and the systems required for recruitment, retention and fundraising efforts.

Lincoln College was already struggling financially because of low enrollment during the pandemic. The cyberattack was a further blow from which it couldn't recover. In spring 2022, after 157 years of operation, the college announced that it was shutting down.[1]

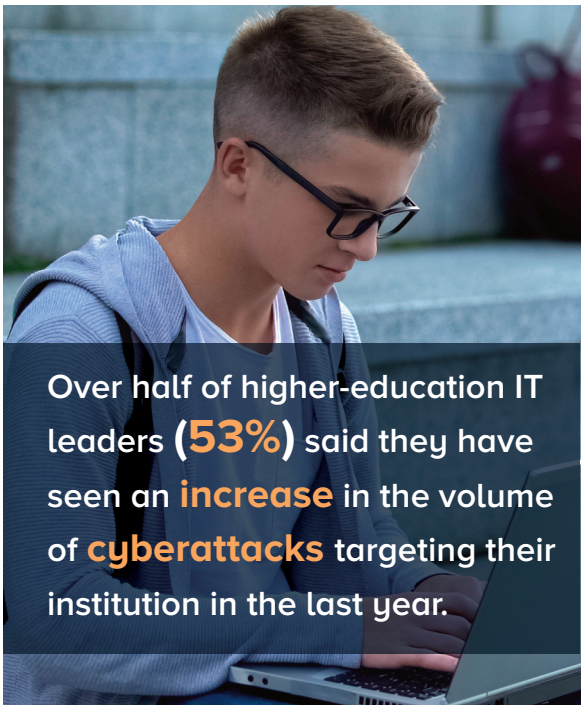
Lincoln College's fate highlights the extreme toll that successful cyberattacks can take on colleges and universities.

As Henry Stoever, president and CEO of the Association of Governing Boards of Universities and Colleges, told Forbes, a cyberattack "can pose existential threats to any organization — large or small, public or private. If you cannot operate your business, if you can't operate your college, then you may not be able to exist."[2]

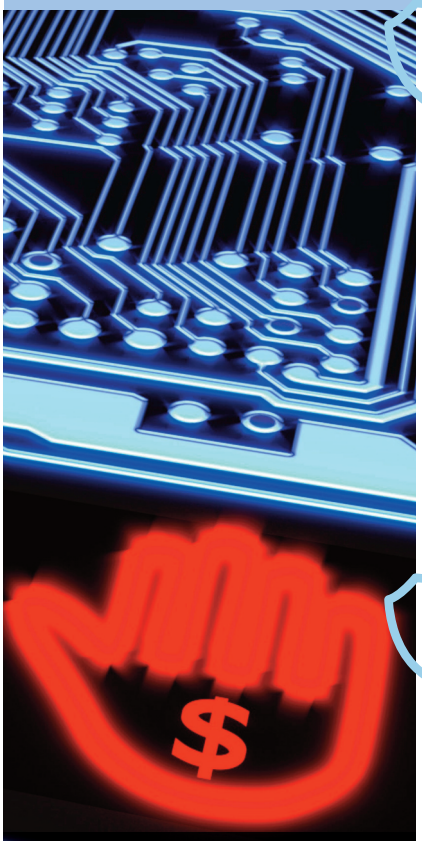
2 Ransomware attacks have exploded within higher education over the last few years.

The kind of cyberattack that hit Lincoln College, in which criminals seize control of campus networks and demand a ransom in exchange for the return of mission-critical systems and data, has become increasingly common within higher education.

In fact, according to a 2022 survey that included more than 400 IT professionals within higher education, nearly two-thirds of colleges and universities experienced a ransomware attack in the last year, up from 44 percent of education respondents in 2021.[3] This increase in ransomware attacks is part of a global trend across all sectors.



Overall, just over half of higher-education IT leaders (53 percent) said they have seen an increase in the volume of cyberattacks targeting their institution in the last year, according to the survey. Fifty percent reported an increase in the complexity and impact of cyberattacks on their institution.[4]



3 Most ransomware attacks against colleges and universities are successful...

Education is the sector that is least likely to stop data from being encrypted in a ransomware attack, the survey found. Nearly three-quarters (74 percent) of the ransomware attacks reported against colleges and universities resulted in data being encrypted by the attackers. In comparison, the global average encryption rate across all sectors is 65 percent.[5]

These findings suggest that colleges and universities may be less prepared to defend against a ransomware attack than other types of organizations, perhaps because they lack the layered defenses needed to secure their networks.

4 ...and they come at a significant financial cost.

The average cost to remediate a ransomware attack in higher education is $1.42 million.[6] This includes not just the cost of paying the ransom, but the expense of restoring software and data systems to their original state.

Aside from the huge financial expense, it can take months to fully recover from a cyberattack. The disruption this causes to campus operations can be significant, as Lincoln College's example demonstrates.

Higher education has the slowest recovery rate of any sector. It takes 40 percent of colleges and universities at least a month to recover from a ransomware attack, compared to the global average of 20 percent across all sectors. Nearly one in 10 higher-education institutions (9 percent) take at least three months to recover.[7]

Richard Forno, assistant director of the University of Maryland Baltimore County Center for Cybersecurity, told Inside Higher Ed that the network environments of colleges and universities are highly distributed. These institutions serve a fairly transient population, with students frequently coming and going, as well as students, faculty and researchers from around the world. This can make it challenging for IT leaders to know exactly who's on their network at any time.

In contrast, he said, IT professionals in other sectors are able to "monitor and control pretty much everything" on their networks more easily.[8]

5 Not all ransomware victims recover all their data.

Even if colleges and universities pay the ransom their attackers are demanding, there is no guarantee they'll get all their data back. While paying the ransom almost always results in the return of some data, the percentage of data restored after paying has declined.

On average, higher-education institutions got back 61 percent of their encrypted data after paying a ransom in 2021. This is identical to the global average of 61 percent across all sectors. However, it represents a drop from the 68 percent of data restored to education organizations in 2020. What's more, only 4 percent of organizations — and just 2 percent of colleges and universities — got *all* their data back, down from 8 percent in 2020.[9]

The key lesson here is that paying the ransom will only restore some of the data encrypted in an attack. Colleges and universities can't rely on the ransom payment to bail them out; they must take proactive steps to enhance their cyber defenses.

On average, higher-education institutions got back 61 percent of their encrypted data after paying a ransom in 2021. This is identical to the global average of 61 percent across all sectors. However, it represents a drop from the 68 percent of data restored to education organizations in 2020.

6 Education has a lower rate of cyber insurance coverage than other sectors.

Cyber insurance has become a critical tool in helping institutions prepare for and recover from a ransomware attack. However, nearly one-fourth (22 percent) of colleges and universities have yet to obtain a cyber insurance policy. In comparison, only 17 percent of organizations across all sectors lack insurance against a cyberattack.[10]

Obtaining cyber insurance is becoming harder. Nearly half of colleges and universities (49 percent) say the level of cybersecurity they need to qualify for insurance is even greater now than last year. Forty-four percent report there are fewer providers offering cyber insurance, 40 percent say the process is more complex and 31 percent say policies are more expensive.[11]

These changes are a product of the increase in ransomware attacks worldwide, which has driven up payout costs. In fact, some cyber insurance providers have left the market because it has become unprofitable for them. The providers who are left are looking to reduce their risk and are raising their rates as a result. Having strong cybersecurity in place will make it easier for colleges and universities to obtain cyber insurance.

7 A "zero trust" approach can protect campus networks more effectively.

A cybersecurity strategy that is becoming increasingly popular across all sectors is the concept of "zero trust." In this approach, all network users — whether they're located on or off campus — are required to be authenticated, authorized and continuously validated before they are given access to an institution's data and applications.

A "zero trust" approach acknowledges there is no longer a traditional network perimeter to be defended, because applications now reside in the cloud and users are accessing network resources from any location. In essence, the network edge extends to each user, and security is achieved by authenticating users' identities as they log on the network.

By 2025, 60 percent of organizations worldwide will embrace zero trust as a starting point for their cybersecurity strategy, Gartner predicts.[12]

A "zero trust" approach acknowledges there is no longer a traditional network perimeter to be defended, because applications now reside in the cloud and users are accessing network resources from any location.

Recommendations for campus leaders

Consider managed network services.

When colleges and universities purchase and install their own network infrastructure, they're also accountable for implementing patches and upgrades to keep these systems secure. With a managed network services approach, institutions can extend the capabilities of overburdened IT staff and keep up with rapidly evolving network needs — while also enhancing their security. With managed services, security patches and firmware changes are installed automatically, keeping network systems continually secure and up to date.

Invest in multiple cybersecurity defenses.

A multilayered approach to network security offers the best protection from cyber threats. In a multilayered approach, institutions employ multiple security systems and technologies to protect various operational layers from attacks, such as a firewall service to protect the internet gateway, antivirus and anti-malware software to shield network endpoints, DDoS protection to guard against a distributed denial of service attack and so on. These multiple defenses all work together to enhance security by protecting against numerous types of threats, as well as multipronged attacks that seek to gain network access through multiple channels.

Partner with a trusted provider for help.

In the wake of the pandemic, many colleges and universities are grappling with significant labor shortages — and IT departments are among the areas that have been affected the most. The *Chronicle of Higher Education* reports that the high-pressure and highly public role that IT staff played in moving campus operations online during the pandemic has led to burnout among many IT employees.[13] With campus IT staff stretched thin, a reliable service provider with extensive experience in serving the higher-education market can help.

Spectrum Enterprise has helped hundreds of colleges and universities improve their cybersecurity with hands-off services that don't require the use of IT staff time to administer, such as their edge networking solutions and managed network services, including DDoS Protection.

The time to act is now

With ransomware attacks and other cyber threats on the rise, campus leaders can't afford to wait any longer to take comprehensive action to secure their networks and data from attacks. A multipronged approach to cybersecurity offers the best chance of defense.

Colleges and universities can balance the need for sophisticated protection and simplicity of operation by choosing security as a managed or co-managed service. With the right partner, institutions are supported from design through implementation and beyond.

Learn how Spectrum Enterprise is uniquely qualified to protect higher-education networks: enterprise.spectrum.com/HigherEd.

[1] Collier, Kevin. "Illinois college, hit by ransomware attack, to shut down." NBC News, May 9, 2022. https://www.govtech.com/education/k-12/k-12-students-on-average-used-143-ed-tech-tools-in-2021-22

[2] Whitford, Emma. "Cyberattacks Pose 'Existential Risk' to Colleges — and Sealed One Small College's Fate." *Forbes*, April 19, 2022. https://www.forbes.com/sites/emmawhitford/2022/04/19/cyberattacks-pose-existential-risk-to-colleges-and-sealed-one-small-colleges-fate/?sh=685efbdc53c2

[3] Sophos, "The State of Ransomware in Education 2022." https://news.sophos.com/en-us/2022/07/12/the-state-of-ransomware-in-education-2022/

[4] Ibid.

[5] Ibid.

[6] Ibid.

[7] Ibid.

[8] D'Agostino, Susan. "Ransomware Attacks Against Higher Education Increase." *Inside Higher Ed*, July 22, 2022. https://www.insidehighered.com/news/2022/07/22/ransomware-attacks-against-higher-ed-increase

[9] "The State of Ransomware in Education 2022."

[10] Ibid.

[11] Ibid.

[12] Kelly, Rhea. "Gartner's Top 8 Cybersecurity Predictions for the Coming Year." Campus Technology, June 23, 2022 https://campustechnology.com/articles/2022/06/23/gartners-top-8-cybersecurity-predictions-for-the-coming-year

[13] Zahneis, Meghan. "Higher Ed's Labor Shortage Is Easing. But These Parts of Its Work Force Are Struggling to Return to Normal." *The Chronicle of Higher Education*, April 5, 2022 https://www.chronicle.com/article/higher-eds-labor-shortage-is-easing-but-these-parts-of-its-work-force-are-struggling-to-return-to-normal

eCampus News

This white paper was produced by eCampus News, the leading online platform that delivers daily technology news and information to higher-education administrators, educators, and technology professionals, and dedicated to the advancement and wise use of technology to improve teaching and learning for all. eCampus News offers ed-tech decision makers a wide range of informative content—including newsletters, webinars, case studies, white papers, websites, and more—that provide in-depth coverage of the latest innovations, trends, and real-world solutions impacting the education community. **www.eCampusNews.com**

Spectrum ENTERPRISE™

About Spectrum Enterprise

Spectrum Enterprise, a part of Charter Communications, Inc., is a national provider of scalable, fiber technology solutions serving many of America's largest businesses and communications service providers. The broad Spectrum Enterprise portfolio includes networking and managed services solutions: Internet access, Ethernet access and networks, Voice and TV solutions. The Spectrum Enterprise team of experts works closely with clients to achieve greater business success by providing solutions designed to meet their evolving needs.

For more information, visit **enterprise.spectrum.com**.

SE-ED-WP023