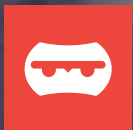




CYBERSECURITY AWARENESS

ON CAMPUS

STRATEGIES FOR ENGAGING PEOPLE IN CYBER DEFENSE



NINJIO

INSIGHTS REPORT

TABLE OF CONTENTS

Executive Summary	3
The Evolution of Cyber Threats to Higher Education	6
Higher Education's Unique Cyber Challenges	10
How to Protect Your Institution	14
Building a Culture of Cybersecurity	16

EXECUTIVE SUMMARY




Institutions of higher education play a central role in society, from shaping citizens and preparing the workforce to conducting groundbreaking research and providing medical care. We all rely on the leaders responsible for their cybersecurity.

While there's an emerging awareness of cyber threats to colleges and universities, many are still underprepared to identify, prevent, and recover from cyberattacks. Cybercriminals have powerful incentives to target these institutions, so it's no surprise that cyberattacks in higher education are on the rise. University CISOs and administrators are confronting a dangerous situation: playing catch-up as threats from highly motivated cybercriminals continuously evolve.



KEY FINDINGS

In this NINJIO Insights Report, we've found that:

-  Ransomware has become the dominant form of cyberattack targeting institutions of higher education with significant financial, reputational, and even health implications.
-  The size and complexity of university networks, paired with the amount of sensitive data housed within them, makes institutions of higher education both vulnerable and valuable targets for hackers and scammers.
-  The higher education sector's core competency - education - is a key component in preventing cyberattacks and one that technology leaders on campus can leverage to address vulnerabilities.

PROTECTING YOUR INSTITUTION

Campus technology leaders can protect their institutions by leveraging their institutional infrastructure to educate faculty, staff, and students to build cybersecurity awareness. Technical measures are absolutely necessary, but **82 percent of successful cyberattacks rely on fooling people into making poor choices.** Expanding awareness to build cybersecurity into your campus culture is the key to an effective cybersecurity strategy.

To that end, here are our top components for a successful cybersecurity awareness program in Higher Education:

- ✓ **Earn the attention of your learners.** Campus life is busy, so you'll need to communicate across multiple channels and styles, especially in a non-technical way, to effectively reach everyone.
- ✓ **Explain why cybersecurity is so crucial for everyone.** There are always be many competing priorities and cybersecurity is rarely at the top for most people with non-technical roles. Clearly explain the risks and highlight the benefits to everyone, regardless of their role.
- ✓ **Personalize your cybersecurity training.** It's important that you meet your learners where they are. That means customizing training content to different learning styles and subject matter familiarity.
- ✓ **Promote accountability.** It's a given that teaching but not testing for understanding will get you nowhere. Regularly evaluate your program with simulated phishing, assessments, engagement tracking, and reporting.

Effective campus cybersecurity is not built in a vacuum. Consider integrating your efforts into your institution's existing educational, communications, and cultural infrastructure to make cybersecurity part of your community's experience.



INTRODUCTION

Institutions of higher education face a growing set of cybersecurity challenges. From managing sprawling networks and IT infrastructure to securing confidential data for thousands of students, professors, and researchers, the task is enormous. For many cybercriminals, colleges and universities are high value targets because the data these institutions are responsible for protecting is extremely sensitive and potentially lucrative. This is why ransomware attacks are so common in the higher education sector – hackers know administrators will be under tremendous pressure to make a deal in the hope that information won't be published. That hope is often in vain.

The best way to counter cyber threats to institutions of higher education is, appropriately enough, through education.

One reason colleges and universities are uniquely susceptible to cyberattacks is the sheer size of their networks. Large student bodies, multiple departments, and the administrative staff operating on interconnected digital systems provide a wide range of attack vectors for cyber criminals to exploit. This is why your institution's defenses need to be distributed. You can accomplish that with a good cybersecurity awareness training program.

When cybersecurity awareness permeates every level of an institution, it is much more difficult for cybercriminals to use social engineering and other human based attack vectors and break into secure networks and systems. In this report, we'll explore the most urgent vulnerabilities that are putting institutions of higher education at risk, as well as the most effective ways to address those vulnerabilities. Although the current state of cybersecurity in higher education is concerning, there are plenty of measures institutions can take to protect themselves – and it all begins with their people.



THE EVOLUTION OF CYBER THREATS

Over the past several years, cyberattacks in the higher education sector have been constant and increasing in severity. Many universities have been forced into no-win situations in which they either pay a ransom to prevent stolen data from being published by hackers or wait for it to end up on the dark web or the open Internet. The result is damage to their institutional reputations, embarrassment for their administrations, and stress for their students and staff. Not to mention significant distractions and financial loss.

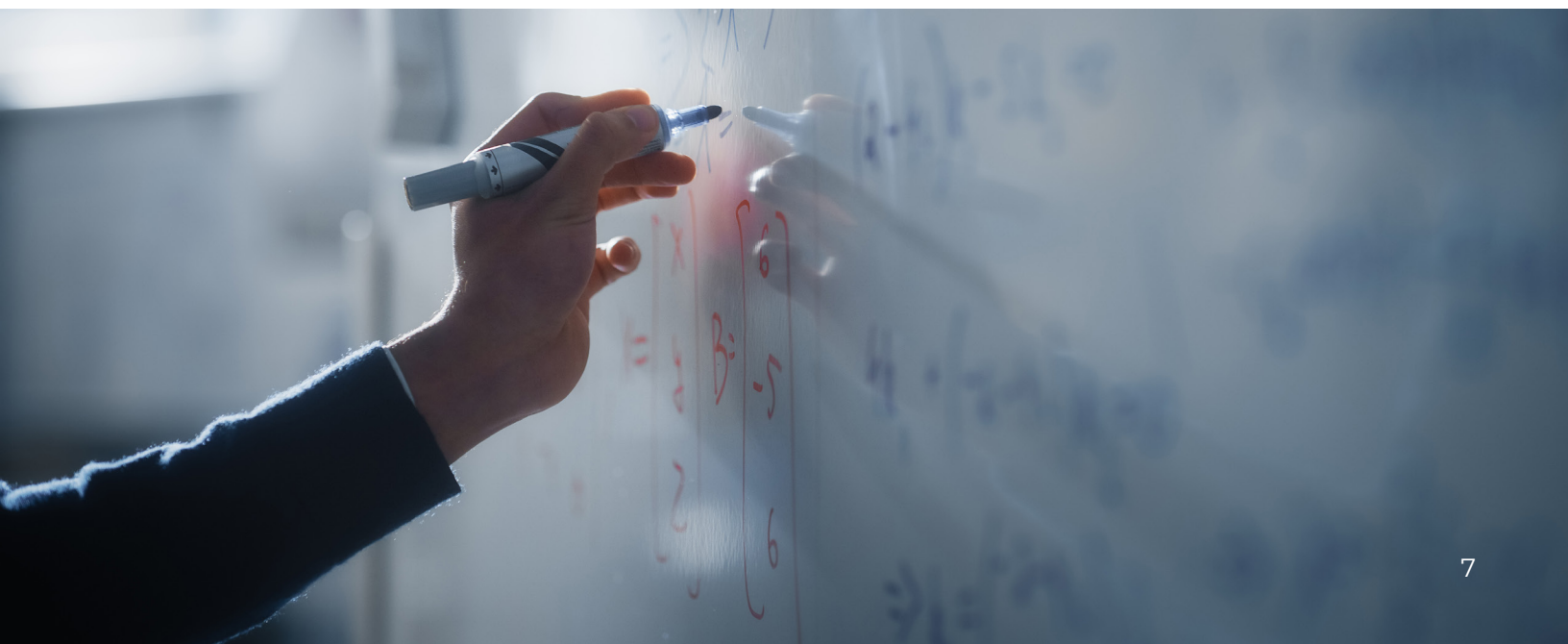
“64 percent of institutions of higher education were hit by ransomware attacks over the preceding year”



According to a 2022 [report](#) published by Sophos, 64 percent of institutions of higher education were hit by ransomware attacks over the preceding year. Ninety-seven percent of the victims said ransomware incidents affected their ability to operate. Dr. Shaun McAlmont is the CEO of cybersecurity company [NINJIO](#), and his decades-long career in the education sector, including as a former college president, gives him unique insight into the cyber threats universities face. In reference to the proportion of institutions that have suffered ransomware attacks, Dr. McAlmont observes: “64 percent is high for any sector, especially one that has millions of young people. If you’re encrypting data for ransom, the data is highly private (Social Security numbers, background information, and test scores). If a bad actor gets to it, a school is likely going to pay a ransom.”

The publicly available number of ransomware attacks suffered by institutions of higher education is almost certainly a significant undercount because institutions don’t always disclose these attacks and try to handle them behind the scenes. The U.S. Federal Bureau of Investigation [discourages](#) the payment of ransoms because doing so “does not guarantee files will be recovered. It may also embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities.” But institutions are often tempted to pay ransoms, as they’re concerned about the publication of sensitive data and the reputational consequences of these disclosures. At the same time, the problem is getting worse. A [study](#) published by Emsisoft found that **almost two-thirds of ransomware attacks were successful in exfiltrating data in 2022** – up from half in the year prior.

“Almost two-thirds of ransomware attacks were successful in exfiltrating data in 2022”



Refusing to pay a ransom comes with its own risks. When the Los Angeles Unified School District was hit with a ransomware attack in the fall of 2022, Superintendent Alberto Carvalho declared that the district wouldn't give in to the hackers' demand for payment. The hackers promptly [published](#) 500 GB of the data they had stolen, which included Social Security numbers, bank account details, student psychological evaluations, and other forms of sensitive information. Dr. McAlmont emphasizes the long-term consequences of these attacks: "What an unfair way to start your life – your Social Security number is already compromised, a threat that can resurface many years later." University students face a comparable threat, and the dilemma confronted by LAUSD last year is a stark warning to institutions of higher education.

“The average cost of a data breach in the education sector is \$3.86 million.”

Beyond the financial vulnerability inflicted on students when they lose control over vital personal data, cyberattacks can also have serious consequences for their mental health. Dr. Sarah Adler, PsyD, is a clinical associate professor at Stanford University and the founder of [Wave](#), an evidence-based emotional healthcare platform. She observes that “a student being part of a system that does not provide safety can experience increases in anxiety and depression. Once you start seeing increases in mental health issues, this will create an ‘anti-virtuous cycle’ – if they can't trust the system, it increases demands for mental and physical health resources.” The cyber threat that higher education faces isn't just a question of reputational damage or financial ransom. It's also a matter of the health and wellbeing of the students.



Check Point's 2022 Security [Report](#) found that the education and research sector suffered 1,605 cyberattacks a week in 2021 – far more than any other sector, and a 75 percent increase over 2020. The report cites ransomware attacks on Howard University and Lewis and Clark Community College, both of which had to suspend classes while the attacks were investigated. However, these incidents were only a glimpse of the damage cyberattacks can inflict on institutions of higher education. Consider this [headline](#) from May 2022: “Ransomware attack shuts 157-year-old Lincoln College.” While Lincoln College was already under immense pressure amid the shift to remote learning and dropping enrollment numbers, this made the cyberattack all the more devastating: “All systems required for recruitment, retention, and fundraising efforts were inoperable,” the university [stated](#). Cyberattacks are capable of disrupting online learning platforms, critical digital infrastructure (such as email accounts and payroll services for university employees), and fundraising activities.

“The education and research sector suffered 1,605 cyberattacks a week in 2021”

The cyberattacks that have hit institutions of higher education over the past couple of years are a harbinger of what's to come for the sector, and change is long overdue. As Dr. McAlmont observes: “It's such a vulnerable time for the higher education sector. Institutions are finally looking in the mirror and saying, ‘There are too many ways into our systems.’ The question now is what to do about it.”



HIGHER EDUCATION'S UNIQUE CYBER CHALLENGES

Institutions of higher education face unique cyber challenges for several reasons. They hold significant amounts of data, they're meant to be open and inquisitive environments, and they're linked to other key societal functions like healthcare and national security. Colleges and universities do everything from educating young adults to providing medical care for communities to conducting vital research and development for the nation and world. They play a central role in society, so their cybersecurity needs look different than those of typical businesses.



Some of these vulnerabilities play off of each other. Consider how the sheer amount of sensitive data colleges and universities are responsible for safeguarding interplays with the size and complexity of university networks. As Dr. McAlmont explains, this means “bad actors have more access points, a problem which is exacerbated by the number of digital touchpoints students are interacting with on a regular basis.” It’s no surprise that higher education has consistently proven to be more susceptible to cyberattacks than other sectors. To take one of the most salient examples: Sophos found that institutions of higher education [reported](#) slower post-ransomware attack recovery times than any other sector. And because ransomware attacks are particularly common in the higher education sector, that fact is even more disturbing.

Black Kite [rated](#) the cybersecurity postures of the top 100 universities in the United States on a scale of A to F. None of them received an A, and researchers found that the institutions are extremely vulnerable. This crisis isn't confined to national borders – [92 percent](#) of institutions of higher education in the UK recently reported that they had identified breaches or cyberattacks in the preceding year. This is further evidence that there are structural issues preventing universities from protecting themselves, as well as consistencies in attack patterns across institutions and geographies.

There are other reasons ransomware attacks are exceptionally prominent in the higher education sector beyond the availability of personally sensitive data. Universities produce huge quantities of research, which often relies on proprietary datasets and information that has been painstakingly gathered over the course of months or even years. The commercial applications of university research can be worth large sums of money, as universities often forge partnerships to simultaneously advance knowledge in a field and create marketable products. Research in AI, robotics, genetic engineering, bioweaponry, communicable diseases, and many other fields can also have sweeping implications for national security. Universities are targeted by cybercriminal syndicates that just want to steal money, but they also suffer attacks by foreign espionage operations seeking economic or political gain.





Some universities house major medical centers, responsible for storing an enormous amount of patient data: billing information, health records, and research on new medications and treatments, among others. According to real-time [data](#) from Microsoft Security Intelligence, educational institutions experience far more malware encounters than any other sector, but the “healthcare and pharmaceuticals” sector ranks third. Check Point [reports](#) that healthcare was among the most heavily attacked sectors in 2022, along with education. It’s no surprise that university health systems at the intersection of these sectors are under sustained assault.

“From anti-plagiarism software to online learning platforms like Canvas, think about all the systems that students’ information is going through on a regular basis.”

While institutions of higher education have to be capable of protecting student data, intellectual property, and other forms of sensitive information, they don’t have as much top-down control over this information as companies and other entities. This is largely due to the open and distributed nature of university networks, which have to accommodate a wide and diverse array of digital platforms, cloud-based communication and collaboration tools, and learning resources. As Dr. McAlmont notes, this profusion of attack vectors makes it much easier for cybercriminals to bypass security mechanisms and infiltrate university networks: “From anti-plagiarism software to online learning platforms like Canvas, think about all the systems that students’ information is going through on a regular basis.” Dr. McAlmont points out that monitoring and preventing cyber incidents on these systems is even more difficult when “institutions have tens of thousands of employees and students versus typical businesses with far fewer people.”



The challenge posed by managing large student bodies has become more severe in recent years thanks to the popularity of some social media apps with dubious privacy controls. “There are hundreds of millions of kids on TikTok,” Dr. McAlmont says, “and they aren’t thinking about the vulnerabilities. They are just clicking on things they like. TikTok is hyper-engaging, which makes it difficult to detect vulnerabilities.” Over [20 institutions](#) in the U.S. have banned the app or recommended that students remove it, but students will find a way to use the apps they enjoy.

The challenges of cybersecurity in higher education won’t be addressed overnight. They’re inherent to the administration of institutions in which the production and management of data is an overriding priority. These institutions are also home to millions of students, professors, and staff who use many devices and pieces of software on sprawling, highly interconnected networks. While there’s no technological panacea for maintaining the security of these networks, there are steps universities can take to drastically reduce their risk: training the vast numbers of users as defenders.



HOW TO PROTECT YOUR INSTITUTION

Like many of the industries tracked in IBM’s Cost of a Data Breach [study](#), the average cost of a data breach in the education sector increased over the last year: rising from \$3.79 million in 2021 to \$3.86 million in 2022. The study classifies education as one of several industries that operate in “high data protection regulatory environments,” which “tended to see costs accrue in later years following the breach.” Comparitech [estimates](#) that almost a million students were affected by ransomware attacks in 2021, which cost \$3.56 billion in “downtime alone.”

“Co-thinking and co-design are both determining factors in facilitating engagement with this generation. They want to know their educators are teaching them things that are relevant and that they feel seen and validated.”

Institutions of higher education can’t afford to accept this as the status quo. They need to be capable of addressing many attack vectors at once and building cybersecurity into their operations at every level. This is why institutions have to create what Dr. McAlmont describes as a culture of cybersecurity – students, professors, and administrators need consistent and engaging cybersecurity awareness training to limit vulnerabilities across the institution.

Dr. Adler is quick to point out: “One of the key things that keeps students and learners engaged is structural, setting agendas and providing clear expectations. In other words, it’s about providing transparency as to the ‘what’, then setting clear expectations about what they should be able to achieve. The next step is teaching relevant, up to date content, then clearly showing how it’s applicable to their everyday lives.”

She encourages IT teams at these institutions to take a collaborative approach. “Co-thinking and co-design are both determining factors in facilitating engagement with this generation. They want to know their educators are teaching them things that are relevant and that they feel seen and validated.”

Engaging and personalized cybersecurity education is all the more important because, according to the 2022 Verizon Data Breach Investigations [Report](#) (DBIR), 82 percent of breaches involve a human element. In the education sector, errors are disproportionately likely to cause breaches. While these facts demonstrate that students and university employees create significant liabilities, they also illuminate a clear path forward: cybersecurity awareness training (CSAT). Everyone at a university is responsible for protecting the institution from cyberattacks, but they need to be equipped to do so. Effective CSAT programs work by providing actionable information about the latest cyber threats and strategies for resisting them in an engaging and digestible format.

Verizon found that the use of stolen credentials is the top action variety in education breaches. Although universities can provide password managers to prevent some of these breaches, there are many ways for cybercriminals to access the accounts of their victims. Meanwhile, over a third of the errors which have caused breaches in the education sector are due to emails sent to the wrong people or with the wrong attachments. Another top action variety is, of course, ransomware – the DBIR reports a “dramatic increase” in these attacks in the education sector, which represent over 30 percent of breaches. Phishing accounts for a significant proportion of breaches as well.

With widely distributed networks, universities need distributed defenses – and humans are an integral part of the equation.



BUILDING A CULTURE OF CYBERSECURITY

Cybersecurity awareness training can help universities address all these attack vectors even as specific tactics evolve. This is why the FBI [urges](#) educational institutions to “focus on awareness and training. Provide users with training on information security principles and techniques as well as overall emerging cybersecurity risks and vulnerabilities.” Similarly, the top “protective control” listed for the education sector in the DBIR is “security awareness and skills training.” These are the reasons why institutions have to build a culture of cybersecurity, which begins with engaging cybersecurity awareness training. Here’s how universities can make the most of this training:



ENGAGING YOUR CAMPUS COMMUNITY IN CYBERSECURITY AWARENESS

EARN YOUR LEARNERS' ATTENTION

The first step toward building a successful CSAT program is earning the attention of your learners. As Dr. McAlmont explains, these programs require “drama, engagement, and reward.” There’s no reason cybersecurity education has to fall into the familiar patterns and pitfalls of formal training programs: stale and monotonous content paired with zero interactivity. By providing high-quality, narrative-driven CSAT content, universities will help students, faculty, and administrators learn and retain critical cybersecurity concepts.

EXPLAIN WHY COLLABORATION IN CYBERSECURITY IS CRUCIAL

Every member of the university community needs to understand that they each play a critical role in cybersecurity. Dr. Adler observes that any effective educational platform should provide “relevant, up-to-date content and explain how it’s applicable to learners’ everyday lives and career goals.” When it comes to CSAT, this means providing information about the latest cyber threats, how they affect individuals, how much damage they can cause, and how everyone can work together to prevent them. Given the importance of cybersecurity awareness in today’s workforce, universities should emphasize the ways CSAT can help students and employees build marketable skills after they leave the institution.

PERSONALIZE YOUR EDUCATIONAL CONTENT

The most effective CSAT platforms are personalized, which means they account for individual skill levels, personalities, and learning styles. In other words, the “learning style for CSAT has to match the student,” as Dr. McAlmont puts it. This will improve engagement by building content around the specific needs of each learner, which will improve learning outcomes and make students feel valued. Beyond the psychological value of personalization, universities will also be in a stronger position to determine how well learners are absorbing the material if they have more in-depth, individualized data. And because the majority of users refresh every four years, a university’s CSAT program needs to be prepared to handle learners at any level, at any time.

FOSTER A CULTURE OF ACCOUNTABILITY

Universities should build accountability into their CSAT programs. There are many ways university CISOs and administrators can determine whether their CSAT programs are actually working: phishing tests and other assessments, tracking cyber incidents, and analyzing the individual needs and performance of learners. When institutions hold themselves accountable, they will ensure that their CSAT programs are creating long-term behavioral change.

CONCLUSION

There's a common misperception that cyberattacks are too complex and advanced for people without technical backgrounds to identify and thwart. This couldn't be further from the truth. By empowering students, faculty, and administrators with robust cybersecurity awareness, CSAT programs protect institutions from digital intrusion across the full range of attack vectors. The best way for universities to rapidly improve their cybersecurity posture is to make cybersecurity awareness a core focus at every level of the institution. Trained students, faculty, and staff will then become an integral part of the culture of cybersecurity: capable of keeping the entire university community secure.



OUR EXPERTS



Dr. Shaun McAlmont

Dr. Shaun McAlmont is the CEO of NINJIO Cybersecurity Awareness Training, and is one of the nation's leading education and training executives. Prior to NINJIO he served as President of Career and Workforce Training at Stride, Inc., had a decade-long tenure at Lincoln Educational Services, where he was President and CEO, and also served as CEO of Neumont College of Computer Science. His workforce and ed tech experience is supported by early student development roles at Stanford and Brigham Young Universities. He is a former NCAA and international athlete and serves on the BorgWarner and Lee Enterprises boards of directors. He earned his doctoral degree in higher education, with distinction, from the University of Pennsylvania, a master's degree from the University of San Francisco, and his bachelor's degree from BYU.



Dr. Sarah Adler

Dr. Sarah Adler is the founder/CEO of Wave, a clinical psychologist, and behavioral health executive with a background in finance and health care delivery design. She is passionate about increasing access to high quality mental health care using data, clinical innovation, & technology. As founding partner (owner/operator) of Peninsula Behavioral Health and the former CCO at Octave (led Clinical, Product & Engineering), Sarah has built practices providing high-value service through clinician culture, ML, product innovation, and deep relationships with commercial payers. She is also a Clinical Associate Professor of Psychiatry at Stanford University Medical School, where she has spent her career developing interventions that work.



NINJIO lowers human-based cybersecurity risk through engaging training, personalized testing, and insightful reporting. Our multi-pronged approach to training focuses on the latest attack vectors to build employee knowledge and the behavioral science behind human engineering to sharpen users' intuition. The proprietary NINJIO Risk Algorithm™ identifies users' social engineering vulnerabilities based on phishing simulation data and informs content delivery to provide a personalized experience that changes individual behavior.