Executive **Summary**

A Make or Break Moment
for Campus Cyber Defense

Highly stressed, stretched-thin cybersecurity teams in higher education need more time and resources to keep up with the latest cyber threats. New and emerging defenses will only require greater attention and funding.

PRODUCED BY:

CAMPUS TECHNOLOGY

SPONSORED BY:

FORTINET®

11%

of cyberattacks in higher education are espionage-related

Few jobs are more stress-inducing than a cybersecurity professional in higher education today. Higher ed's free and open environments, stores of rich data, and rapidly growing numbers of endpoints or smart devices make the sector a prime target for malicious actors and cyber crimes. What's more, gaps in user training and communication on threats and proper cyber hygiene persist.

While investment in cybersecurity tools, training, and resources remains a top priority for institutions in 2023, many requests will go unfunded or underfunded. Combined with institutions' growing inability to recruit and retain highly qualified cyber professionals, cybersecurity in higher education appears to be at a tipping point.

One thing is clear: Humans pose the greatest risks to cybersecurity on and off campus. **Gartner predicts that by 2025**, lack of talent or human failure will be responsible for more than half of significant cyber incidents in all sectors.

A summer 2023 *Campus Technology* survey revealed details of the many competing challenges higher education IT and cybersecurity professionals face each day as they fight an ever-growing list of threats. At the same time, the survey also uncovered hope and confidence in specific technologies and attention from senior leadership, which offer greater protection and peace of mind when it comes to maintaining data security and protecting valuable institutional resources.

How We Got Here

For many years, higher education has stuck out as a leading and attractive target for cyber criminals. Networks that house advanced research data — including government-related and commercial research — are the main magnet for nation-state actors or black hats conducting industrial espionage. In 2019 alone, the Verizon Data Breach Investigations Report noted that 11% of cyberattacks in higher education were espionage-related.

Campus networks house massive stores of personal, financial, and medical information for students, alumni, faculty, and staff. Cybercriminals who look to wreak havoc or otherwise disrupt higher ed operations see opportunities at institutions where on-campus students enjoy access to most of life's necessities. Ever-expanding numbers of private devices on the networks complicate endpoint security and increase the shape and scale of the available attack surface.

As institutional networks grow more distributed, researchers in the field, branch campuses, and study-abroad facilities also add to cybersecurity complexity and successful provisioning of cybersecurity services or resources. Decentralized IT and services delivered

45.5%

name cybersecurity engineer as the most difficult role to fill

to departments or research teams on a chargeback basis complicate the landscape even more.

Getting a handle on it all will keep CISOs and their teams busy for years to come; however, evolving skillsets and technologies are also coming online to help teams meet these multi-faceted challenges.

5 Toughest Roles to Fill

Like its colleagues in industry, higher education struggles to recruit and retain cybersecurity talent. As specialties evolve and new skills are required, teams that find success in winning budget approval to expand then face additional hurdles to get that talent in the door. **The top five skills or specialties that remain unfilled on respondents' teams include:**

45.5% **Cybersecurity engineer**

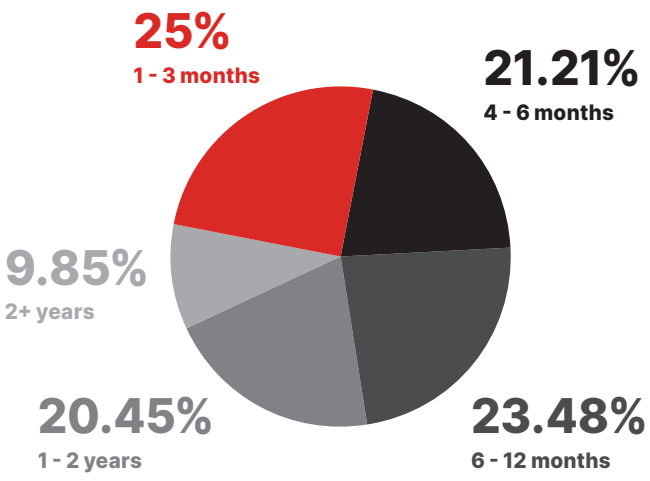
43.9% **Cloud security**

40.9% **Risk management**

33.3% **Network security**

25% **SecOps**

Some teams experience extended periods of time when those roles remain vacant:



Q: How many months have the most essential cybersecurity roles on your team gone unfilled? (n=132)

When respondents were asked what keeps them up at night, one noted that "not enough qualified staff may mean insufficient responses to security incidents or delayed handling of major cases."

Gaining Traction, Looking Ahead

Senior executives in higher education must empower security leaders to do the right things at the right time,

62%

report that only one person at their institution is designated as responsible for cybersecurity

and at the right cost. Clarified responsibilities and aligned relationships with other leaders throughout an institution also contribute to a more cohesive cybersecurity strategy that addresses distributed governance as well as identifies and comprehends campus applications, resources, and technical skills. Cross-campus cooperation can remove barriers that otherwise prevent asset visibility. **Respondents ranked the following "wish list" from most important to least important:**

Governance - Contributions and cooperation from campus leaders and technologists

Empowerment - Endorsements from leadership to do the right thing

Cooperation - Help from campus business units in creating visibility for connected systems, applications and cloud objects

Data consolidation - Including technical, procedural, and intelligence with staff who understand available data and data governance strategies

Most respondents (62%) reported that one person at their institution is designated as "responsible for cybersecurity," and that person regularly reports to senior leadership (president, chancellor, provost) and the institution's governing board (87%). That reporting relationship and stature become increasingly important as the critical needs around cybersecurity continue to compound and grow. Consistent and ongoing communication of the evolving threat landscape and effective mitigation require deeper understanding than that imparted exclusively in annual budget conversations.

Internal Threats

By far, people represent higher education's number one threat vector, as well as institutions' first level of defense. Persistent and comprehensive training and communication that help users understand the precise nature and appearance of threats or malicious actions — as well as proper cyber hygiene — are critical to successfully mitigating the variety of risks inherent to the wide-ranging and diverse uses for higher education networks and data. Campus visitors, administrators, students, faculty, researchers, and more each present their own levels of risk and potential for attack, especially when the majority of those users connect to the institution's network or

44

universities or colleges were hit by ransomware attacks in 2022

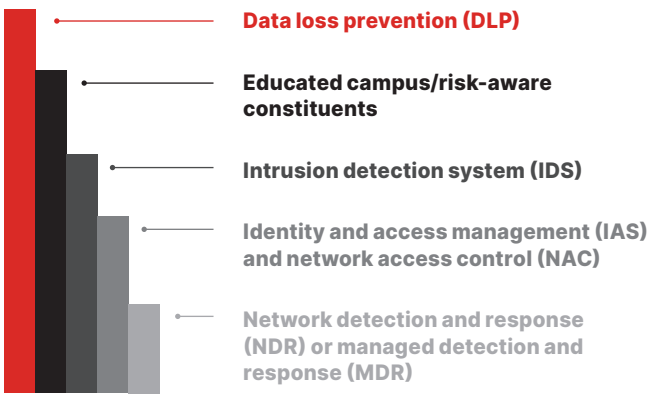
infrastructure using their own devices.

When respondents were asked what keeps them up at night, one wondered whether "people [are] having their data stolen because they don't know how to recognize a threat." Another expressed concern that "we have not established cybersecurity as a high priority amongst employees as a part of their onboarding process. By educating employees on their roles and responsibilities when it comes to upholding information security, our college could have a better, robust defense against cyber threats."

5 Most Critical Defenses

A January 2023 news report noted that at least 44 universities or colleges were hit by ransomware attacks in 2022, although many more incidents likely occurred that were not publicly disclosed. The increasing volume and sophistication of those threats mean that the education sector at large is more susceptible than ever to falling victim to stolen credentials and phishing attacks, potentially compromising the personal information of faculty and students, as well as the integrity of research data and intellectual property. The mix of human-centric protection and automation capabilities in use by institutions today underlines acknowledgement that humans represent the greatest risks to higher education networks and data.

Institutions' top five critical defense priorities are:



Alongside relevant cybersecurity and data protection tools and technologies, ongoing and up-to-date role-based user training serves as one of the most important components of an institution's cybersecurity strategy. Communication to users about emerging threats or the latest methods of attack also ensures users remain vigilant and work in partnership with cybersecurity teams rather than against an institution's interests. Required completion of online training modules reinforces key lessons or teaching moments, and ensures all institutional users can participate whenever or wherever necessary. Packaging lessons or training modules with informational campaigns ensures timely dissemination

32%

of institutions do not provide appropriate funding for cybersecurity

of information to network users and can help institutions meet a more regular cadence for communication; e.g., quarterly updates and trainings versus annual communication that's not as timely or beneficial.

Here are the tactics survey respondents said their institutions use most frequently:

Respondents detailed other approaches, including "e-mails to students on how to handle suspect e-mails and links that could attempt to infiltrate the college systems"; and "IT locked down our access to all non-USA websites, and unlocks on an 'as needed basis'"

Help Wanted

Almost a third of respondents (32%) indicated that their institutions do not provide appropriate funding or otherwise prioritize those five critical defense priorities and solutions. While a healthy portion of respondents noted that their annual cybersecurity budget recommendations were recently funded at 100% (27%), others must navigate budget shortfalls, noting that their requests were funded at only 70 to 79% (16%) or 80 to 89% (15%).

What was left on the table? When detailing the critical security pieces most recently left unfunded, responses varied from network access control and identity and access management to user awareness training and physical security, in addition to firewall upgrades and endpoint detection/response. Others indicated that critical staffing was left unfunded or not approved.

When it comes to documenting the need for all of these tools or resources, success appears split:

52%

report a successful ROI from their institution's cybersecurity efforts

52% of respondents noted that they've successfully proven a return on their institution's cybersecurity investments while 48% could not.

5 Emerging Solutions

As higher education weighs new approaches to addressing cyber risks and protecting the massive amounts of student data, research data, and intellectual property inherent to higher education environments, **IT leaders see new potential in the emerging cybersecurity solutions:**

AI-enhanced data analysis

AI-enhanced threat detection

ML/deep learning log tracking and threat detection

Automated security operations

Automated security response

Artificial intelligence-enhanced solutions and automation offer promise in their ability to sift and analyze massive amounts of network activity and threat data to detect anomalies and lessen reliance on signature-based detection systems that are only effective against known threats. Machine learning algorithms trained using vast amounts of data, such as historical threat data or data from the network and its endpoints, can identify patterns as well as detect and respond to known and unknown threats in real time. The ability to continuously learn and adapt ensures that as new threats emerge, the algorithms are trained on new data and their ability to respond only improves, providing more effective security and protection over time.

Shifting from human analysts to AI-powered tools and processes enables time- and resource-strapped teams to instead hone their focus on areas that truly require their expertise, or on those activities that more directly impact an institution's mission. Over the next year to two years, respondents expect that these emerging capabilities will bolster existing strategies and successful solutions, and only continue to impact their institutions' security operations.

Note: Findings are based on a Campus Technology online survey open for invitation-only response in spring 2023. After filtering for appropriateness of affiliation and completeness of answers, survey results represent 226 respondents.