WHITE PAPER

Leading Cybersecurity in Higher Education

It's Not Just a Technical Challenge

Executive Summary

Higher-education institutions are experiencing a high volume of cyberattacks and greater vulnerability to threats. Today's educational technology environments connect a variety of endpoints—laptops, desktops, student management data, and email servers. They use Internet-of-Things (IoT) devices for managing environmental controls, security cameras, and door alarms. Both ends of the education spectrum gather, store, and use personal data from students and staff—and if they collect it, they must also protect it. As a result, schools need dedicated, skilled, and experienced executive leadership that is empowered, resourced, and responsible for campuswide cybersecurity issues.

"Risks to higher education institutions stretch far beyond the threat of a data breach or forced network outage. Universities, and the cities and states in which they operate, place great importance on their public image in order to attract new applicants, retain top talent, and stay ahead of the competition."[1]

The Complexities of Securing Higher Ed Environments

College and university technology needs are generally more complex than K–12 institutions in both scale and scope. Higher education typically demands much more data protection due to larger volumes and diverse data sets. This may include copyrighted research findings or patentable discoveries; personal data on research subjects; student healthcare and financial records; federal- or state government-provided information that may be controlled or even classified; information stored in special-purpose technologies, such as laboratory equipment, remote field sensors for environmental and oceanographic data, or other connected devices used for research (such as agricultural metrics, wind tunnels, or nuclear reactors).

Based on 2022 cyberattack summaries and expert projections for 2023, higher education will likely remain in the near-constant state of cyberthreats and activity. Among the 13 costliest cyberattacks for 2022 across all industries, universities occupy positions eight through 10.[2]

- At Florida International University, an ALPHV/BlackCat attack exposed large volumes of sensitive data, leading to class cancellations and assignments not being able to be submitted as scheduled.
- Another ALPHV/BlackCat attack at North Carolina A&T disrupted multiple learning management systems and academic tools with data loss.
- Austin Peay State University in Tennessee suffered a ransomware attack that caused the cancellation of spring final exams. Faculty had to rely on coursework alone to assign semester grades. In addition to campus computer labs closing, Austin Peay employees were also advised to use personal computers or university-owned Apple devices to access campus networks and email.

If these kinds of disruptions are not enough to influence educational leaders, the average cost of a breach in the educational community is currently $3.86 million.[3] Putting this kind of expense into relative perspective, those dollars could cover the salaries (including taxes and moderate benefits) of up to 17 staff or faculty earning around $125K per year. Those funds could also be used to provide technology and services needed to automate many university-level cybersecurity functions—enabling security leaders to control operating costs, alleviate the burden on under-resourced teams, and focus staff attention on critical tasks.

The Struggles of Higher-Ed Security Leaders

In addition to managing high volumes of cyberattacks and breach remediation efforts, today's education security leaders are still struggling for relevance while they do the hard work to gain a more visible seat at the table. Larger universities in the higher end of the spectrum have had professional cybersecurity staff and IT security leaders at the director or C-level for the past 15 to 20 years—and some for even longer. But smaller universities, technical colleges, and community colleges often struggle to have one or two staff that are articulate in cybersecurity technologies, processes, and compliance requirements.

Some higher-education institutions may have multiple technologists that each devote a portion of their week to cyber-focused tasks. But in these situations, few are proactively able to address critical risk management and incident response programs. This becomes a difficult business issue for decision makers. With the declining enrollment that comes with fewer college-age adults, schools cannot simply "sell more" product or raise prices to cover all the costs of a fully staffed security organization.

Top five education cyber threats

1. Phishing scams (including email, texts, and business email compromises)
2. Ransomware
3. Data breaches and leaks
4. Distributed denial-of-service (DDoS)
5. Technical debt from outdated technology[4]

Essential Cybersecurity Leadership Skills

The most important skill any education security leader needs is the ability to communicate problems and share successes up, across, and down the organization. Depending on where the security leader (CISO, security director, or IT security manager) stands within the campus community, this may include communications on policy, incident response, soliciting collaboration on security issues, or other kinds of internal/external outreach. Communications must be clear and accessible to those who do not necessarily share the CISO's enthusiasm for cybersecurity.

An effective education security leader also needs to occupy a prominent place in the organization chart. If your campus has an IT security manager buried five layers deep and reporting to an assistant director, that IT security leader will not be heard by executive decision makers—chancellors, presidents, deans, or directors. Institutions need a security leader that is aligned and able to actively engage with other leaders in the distributed governance food chain in order to encourage coalition participation in key security planning, operational issues, and reporting functions.

Another critical skill for leading a successful education cybersecurity program today is the ability to manage security complexity. Many security teams are dealing with framework fatigue and having to constantly shift focus. They need someone in charge who is skilled at leading others across multiple roles. Leaders should excel at creating opportunities to innovate and deal with a diversity of use cases, tools, and talent across the institution. A skilled CISO will also be able to coordinate and certify the campus' ability to address both known and unknown threats.

Navigating the shifting tides of compliance means knowing and enforcing the rules. An effective higher-ed CISO needs to understand how law, policy, and doctrine work for their institution's benefit. Knowing where flexibility exists will provide structure for compliance without having rigid rules that ultimately encourage others to cut corners.

Finally, the security leader needs to apply top intelligence sources and threat data management tools to find the proper balance between people, processes, and technologies for the institution.

What's Expected of an Effective Security Leader?

Successful security leaders in education are mentors, coaches, and advisors to those vocal about their commitment to the organization's goals. Like their private industry corporate counterparts, education security executives deliver well-planned cybersecurity risk management and incident response programs complete with the requisite procedural documentation, automation, and upgrades. They also deliver just-in-time problem remediation while securing the costly and complex digital transformation projects needed to improve the quality of education for students year after year.

To achieve this, IT and security executives need technology architects, planners, and visionaries. Wisdom demands they have experts who are up to speed with other industries. This means people who understand digital acceleration pathways as well as potential cost-speed-performance issues in order to keep their institutions ahead of the curve in attracting top-quality teaching and research staff. These critical role-players also need to work and play well with the rest of the security teams.

Operationally, colleges and universities need reactive responders to attend to a variety of technology- and operator-driven issues that may disrupt research or teaching at any moment of any day. Teams will also need ongoing security training and practice with incident response and investigation protocols. Additionally, they will need to be very well-versed in securing multiple technologies—including those that may be conflicting.

The education cybersecurity leader has to understand how to build, equip, and orchestrate all of the above. They also need well-written and frequently exercised processes that use a stable suite of capable and complimentary tools.

Higher-ed institutions need leaders with relevant experience and the will to press forward with consistent processes and the ability to build or buy the necessary improvements to achieve program maturity. Leaders must be comfortable talking to chancellors and presidents, deans and directors, technologists and faculty, researchers and administrators, staff and students. And they must be able to deliver the messages that users need to hear—whether it's about cyber hygiene, data governance, privileged access, or remote location security.

The Education Cybersecurity Leader's Wish List

Education security leaders should be empowered by senior executives to do the right thing, at the right time, and at the right cost. They need clarified responsibilities and aligned relationships with other leaders throughout the institution.

A cohesive cybersecurity program must also address distributed governance. Security leaders need a clear picture of the campus to determine which components may be at risk—regardless of technology, data, or operational sensitivity. They must be able to identify and understand campus applications, resources, and technical skills. This may include standardizing compliance reports and tracking shadow applications by inspecting cloud-based services and data storage. But to achieve effective governance, security leaders also need cross-campus cooperation to help remove barriers that impede visibility of assets.

In addition, effective security leaders need tools for streamlining risk management, as well as the ability to implement converged security and network management solutions, such as SD-WAN and secure access service edge (SASE) architectures.

The education CISO's wish list

1. **Empowerment:** Endorsements from leadership to do the right thing
2. **Governance:** Contributions and cooperation from campus leaders and technologists
3. **Cooperation:** Help from campus "business units" in creating visibility for connected systems, applications, and cloud objects
4. **Data consolidation:** Including technical, procedural, and intelligence with staff who understand available data and data governance strategies

[1] "How to address cyber threats against higher ed," Higher Ed Dive, June 6, 2022.

[2] "The 13 Costliest Cyberattacks of 2022: Looking Back," Security Intelligence, December 29 2022.

[3] "Cost of a Data Breach Report 2022," IBM, July 26, 2022.

[4] "Top 5 Cybersecurity Threats Facing Higher Education," Fierce Education, July 5, 2022.

February 11, 2023 2:22 PM

1918374-0-0-EN