Higher education is on high alert for cyberattacks

Boosted by federal stimulus funds and rising investment markets, 2021 was a year of resilience for the U.S. higher education sector, with colleges and universities enjoying better-than-expected operating results. However, ongoing disruptions from the pandemic and social and geopolitical impacts have increased strain on these institutions’ resources, heightening risks surrounding data privacy and security. As higher education institutions evolve to accommodate more hybrid working and learning environments and plan their response to imminent regulation on cyber breach disclosure requirements, cyber security remains a top concern for higher education institutions and their boards.

Examining higher education’s cyber security landscape

In today’s increasingly distributed technology environment, it is almost inevitable for a company or institution to experience a major cyber event. And the threat landscape is only expanding with cybercriminals employing increasingly sophisticated tactics and technologies to wreak havoc on their targets. Higher education institutions, and particularly those with significant research and development activities and academic medical centers, are prime targets for breaches. In fact, a number of higher education institutions have succumbed to high-profile attacks in recent years, resulting in data breaches, network outages and ransom payments.

Relative to other industries, education is uniquely vulnerable to cyber events. A 2021 EDUCAUSE report found that the sector experienced over six times more malware attacks than the next most affected industry. And the problem is poised to get worse. While higher education institutions are working diligently to improve their cyber security infrastructures, bad actors are moving more quickly. Cybercriminals do not adhere to an academic calendar; they work around the clock to find windows of opportunity to cause disruption. Their motives may vary: Some cybercriminals work on behalf of nation states to create chaos on U.S. soil, while others seek monetary compensation, intellectual property or other sensitive data.

At the center of higher education’s cyber security landscape is one common theme: Colleges and universities are high-value targets, and it is imperative that they accelerate the implementation of robust security processes and controls that continuously assess and mitigate cyber vulnerabilities.

Higher education’s unique vulnerability

Though no sector is truly immune from cyberattacks, we see several key explanations for higher education’s unique vulnerability:
Higher education institutions house highly valuable data in the form of research intelligence, patient medical records and student information. Research universities in particular may house lab equipment and other testing instruments that are gifted through grant money. In discussions with clients, we have heard that grant equipment is less frequently updated for security purposes.

Higher education institutions traditionally operate in more open and decentralized information technology (IT) environments. Relative to a highly centralized public company, these environments tend to have more entry points for bad actors.

The COVID-19 pandemic accelerated the shift to hybrid work and learning at colleges and universities. This shift created strains on technology bandwidths and quickened the adoption of new technologies.

Higher education lags other industries with respect to cyber spending, staffing and expertise at the board level.

There is an exclusive prestige to higher education institutions. Universities, and the countries where they operate, are very focused on building their competitive edge. Entities that place such a large emphasis on reputation have much to lose in a cyberattack.

As we shared in Three Lesson Plans for Higher Education Boards in 2021, the stakeholder landscape for higher education is among the broadest of any industry. It includes students, parents, faculty, staff, board members, alumni, donors, researchers, patients and the federal government and associated regulatory bodies. Higher education stakeholders make financial and strategic contributions to the institutional mission that are wide-ranging and important, but their varied interests also make quick decision-making a challenge. Colleges and universities must understand that fulfilling the needs and expectations of such a complex network of stakeholders undoubtedly gives rise to more cyber security concerns. To mitigate these, institutions must be willing to embrace cutting-edge security solutions that can manage the growing volume and sophistication of the threats they face.

**Recommendations for bolstering cyber security**

Paramount to higher education’s success in overcoming cyber security threats is accelerating the speed with which institutions assess their vulnerabilities, developing robust security policies and implementing them in a rigorous manner. Every second counts — no university wants to fall victim to a breach while cyber security policies await revision or proactive measures need sign-off.

In addition to approaching cyber security with a heightened sense of urgency, colleges and universities can enhance their internal protocols by:

- Implementing regular training, awareness campaigns, tabletop exercises and phishing simulations among students, faculty, staff and other key stakeholders.

- Narrowing the scope of access to secure systems. Colleges and universities should be mindful of limiting system access to those who truly need it. For example, visiting professors should not have remote access to an institution’s network once their teaching engagement is complete.

---

— Diligently deploying, tailoring, testing and refining baseline tactics. This means increasing the frequency with which colleges and universities conduct red teaming, penetration testing and system backups, as well as refreshing incident response playbooks on a more regular basis.

— Developing a comprehensive response playbook for ransomware. It is essential that institutions have a firm stance on their willingness to pay (or not pay) ransom before their systems are compromised. Purchasing ransomware insurance protection is a key component of this preparation, as is identifying the individual who will make the ultimate payment decision in the event of a breach.

— Establishing minimum cyber security standards for all vendors and regularly monitoring them.

— Understanding third-party risks associated with cloud-based systems. While cloud-based systems are typically more secure than on-premise systems, transitioning to the cloud is essentially outsourcing that function to a third-party vendor who then creates new access points to sensitive data. That vendor will require regular vulnerability assessments, and their internal controls will require independent assurance from an auditor.

With so much data and high-value information at stake, colleges and universities are at an inflection point and should focus on adopting a zero-trust mindset toward cyber security. The zero-trust security model is increasingly viewed as a viable security approach in the post-pandemic world. Zero trust represents a significant mindset shift in which cyber teams assume their systems will be compromised, and therefore make security decisions based on that assumption, with a focus on the identity, device, data and context of each entry into the system.\(^3\)

Of course, adopting such a dynamic response protocol is costly and will require institutions to allocate additional funds for cyber security technology and personnel. To ease this burden, lower-level threats and routine testing can be automated so that security professionals can prioritize matters that require human intervention.

**The role of the board**

IT auditors are highly experienced in identifying risks and gathering insights from an institution’s operations and policies. With decentralized IT environments that include both on-premise and cloud-based solutions, higher education boards and audit and risk committees must remain vigilant about overseeing how the institution is managing key vulnerabilities.

Boards, including audit and risk committees, can provide additional support to colleges and universities in their efforts to mitigate cyber risk by asking leadership the following questions:

— Do we have clear insights into our cyber security program’s maturity, gaps and threats? Does leadership have a prioritized view of investments needed to address areas of immaturity or highest risk? Are the institution’s most “valuable” assets adequately protected?

— Has the institution recently tested its incident response plan? Are penetration testing and red team testing regularly performed, and is there a formal process to address findings?

---

— Do we have a robust institution-wide data governance framework that makes clear how and what data is collected, stored, managed and used, and who makes related decisions?

— Do we understand the coverages, limits and underwriting criteria of our cyber insurance policy?

**Conclusion**

Today there are multiple bills sitting in Congress aiming to mandate more timely and comprehensive disclosures of cyber security events. If these bills are enacted, colleges and universities would likely not be exempt. Moreover, federal, state and other grantors increasingly consider the strength of an institution’s cyber preparedness and ability to protect private information as prerequisites for funding. It is in the best interest of higher education institutions to prepare now, before a major incident. Their stakeholders demand it, and their reputations depend on it.

**David Gagnon**
Partner, Audit
National Industry Leader, Higher Education & Other Not-for-Profits
KPMG U.S.
dgagnon@kpmg.com

**Tony Hubbard**
Principal, Advisory
KPMG U.S.
thubbard@kpmg.com

**Kathy Cruz**
Director, Advisory, Cybersecurity
KPMG U.S.
kathycruz@kpmg.com

© 2022 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee.