SecureStrux

WHITE PAPER

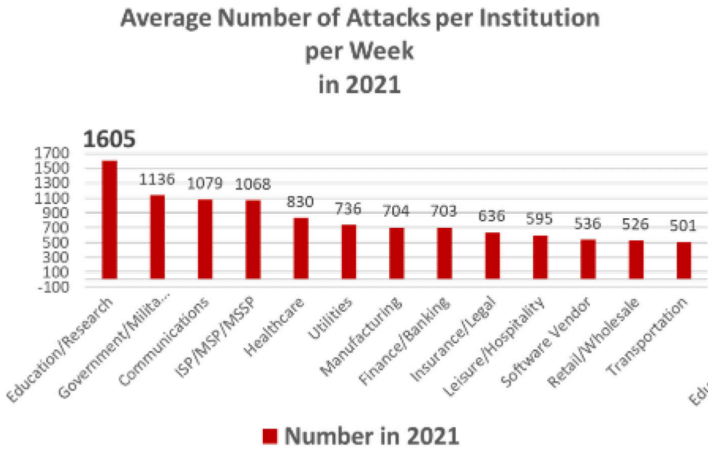
The State of Cybersecurity in Higher Education

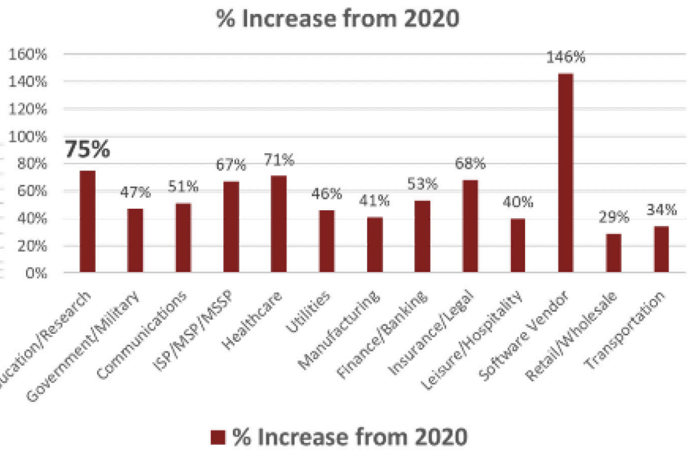
Institutions of Higher Education are Facing Increasing Cybersecurity Challenges

Institutions of higher education (IHE) face many cross-cutting challenges, including but not limited to the following: sustaining student satisfaction and enrollment, maintaining accreditation, funding demands, compliance regulations, changing learning and working modalities, digital transformation, information sharing, and protecting assets and data against cyberattacks. In recent years, cybersecurity challenges have surged in the higher education space, and the situation is expected to worsen.

According to Check Point Research, IHE was the top target for cyberattacks in 2021, with an average of 1,605 cyberattacks per institution per week, which is a 75% increase from 2020[1]. In comparison, other industries globally saw an increase of 50%.

IHE requires a top-down approach to develop cyber strategies for evolving threats.





The IHE must leverage information technology and cybersecurity governance, risk management, and cybersecurity best practices planned from the top down to protect the confidentiality, integrity, and availability of sensitive data and valuable assets from cyberattacks.

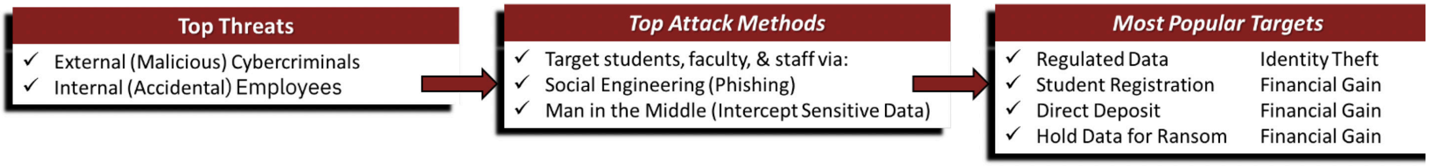
Target of Opportunity

IHE provides a target-rich environment from various perspectives.

- First, IHE has a treasure trove of valuable information for cybercriminals. Research data is subject to compliance regulations. Digitized student records contain personal, medical, and financial data on one large campus-wide network.
- Second, IHE does not have enough resources to protect against increased cyberattacks. Educational institutions cannot keep up with the ever-changing threats and methods of cyberattack. Universities lack a comprehensive cybersecurity program built from the top down.
- Third, IHE has also become an easier target. The COVID-19 pandemic, most strikingly, increased the severity of this situation with multimodal platforms and remote work that increased the exposure footprint to cyberattacks. Consequently, digital information has become harder to protect and easier for successful cyberattacks.
- Fourth, IHE discovery and recovery times from a successful attack are incredibly long, allowing the threat actor sufficient time to cause severe damage. In 2021, 40% of higher education institutions took longer than one month to recover from a cyberattack. Only 10% of manufacturing and production companies averaged more than one month to recover[2].

Humans are the weakest link in the cybersecurity protection chain. Cybercriminals know it. Cybercriminals exploit it. Universities are prime targets for cybercriminals who use social engineering to disrupt services or access university assets.

Top Attack Methods



Top Threats

- ✓ External (Malicious) Cybercriminals
- ✓ Internal (Accidental) Employees

Top Attack Methods

- ✓ Target students, faculty, & staff via:
- ✓ Social Engineering (Phishing)
- ✓ Man in the Middle (Intercept Sensitive Data)

Most Popular Targets

✓ Regulated Data	Identity Theft
✓ Student Registration	Financial Gain
✓ Direct Deposit	Financial Gain
✓ Hold Data for Ransom	Financial Gain

Cybercriminals will persist in using low-skill, low-effort attack methods to access high-value data and assets for identity theft or financial gain. Social-engineering, such as phishing scams, deceives students, faculty, and staff, granting unauthorized access to valuable information. Man-in-the-middle attacks have also increased, tricking unsuspecting parents and students into paying tuition on websites that impersonate legitimate university payment portals.

Preparation is Paramount

Stricter Regulatory Requirements: Pennsylvania approves legislation barring state and local governments from using taxpayers' money to pay randoms and making it illegal to possess, develop, sell, or threaten the use of malware in Pennsylvania[3].

Despite the challenging outlook for IHE security, a robust cybersecurity program can minimize the impact of cyber attacks. It's not a question of if a university will face a cyberattack, but when. The key defense is to establish a comprehensive cybersecurity program involving all university stakeholders, beyond the conventional IT and cybersecurity staff.

Additionally, IHE must also consider outsourcing portions of its cybersecurity program to assist with the affordability, scalability, and relevancy of a resilient cyber program. Federal and state compliance regulations (i.e., FERPA, Sarbanes-Oxley Act, Gramm-Leach-Bliley Act. HIPAA, etc.) will continue to be updated. Balancing these evolving requirements adds to the workload of many resource-constrained universities.

Cybersecurity must be threaded throughout the fabric of the university to protect against cyber attacks.

Below is a high-level roadmap for developing or enhancing an IHE cybersecurity program. While note a step-by-step guide, these activities are minimum recommendations for the resilient program. Universities may have completed some of these steps, but updates may be needed due to evolving regulations.

Moreover, to reduce expenditures and resources, consider outsourcing some activities. Outsourcing offers benefits such as accessing skilled professionals with the right expertise at the right time, while also reducing implementation and sustainment costs compared to in-house development.

1. Institutionalize cyber governance, risk, and compliance to meet regulatory requirements
2. Define roles and responsibilities to include technical and non-technical roles
3. Categorize and document all data and identify compliance requirements
4. Define, implement, and maintain a resilient cybersecurity program with a cyber strategy and roadmap
5. Continuously monitor compliance with all regulatory requirements and cybersecurity frameworks
6. Repeat steps one through five on an ongoing basis.

Sources

1. Check Point Research, CPR Security Report for 2022. Retrieved December 2, 2022, from https://blog.checkpoint.com/2022/01/21/2022-security-report-software-vendors-saw-146-increase-in-cyber-attacks-in-2021-marking-largest-year-on-year-growth/
2. Sophos, The State of Ransomware in Education 2022. Retrieved December 4, 2022, from https://news.sophos.com/enus/2022/07/12/the-state-of-ransomware-in-education-2022/
3. Senate Bill 726, amending Title 18 (Crimes and Offenses) of the Pennsylvania Consolidated Statutes. Pennsylvania Approves Ransomware Bill. January 2022. Retrieved from https://www.infosecurity-magazine.com/news/pennsylvania-approves-ransomware/

Author

Tony Buenger (CCISO, CISSP, CISM, CGEIT)
Director, Governance, Risk, and Compliance
SecureStrux, LLC

tony.buenger@securestrux.com
LinkedIn

SecureStrux.com
(717) 262-2672
8 West King Street | STE 824
Lancaster, PA 17603

SecureStrux