Cybersecurity Landscape Assessment for Higher Education Systems

Prepared for: Monarch Internship and Co-op Office

Prepared by: Samantha Riggs, MICO Cybersecurity Intern

Date: March 27th, 2026

Old Dominion University

Introduction

Higher education institutions operate in a uniquely complex cybersecurity environment. They must balance open access to information and systems, (which are necessary for academic collaboration and research), with the responsibility of protecting large volumes of sensitive data. This includes personal, financial, academic, and health-related information for students, faculty, and staff.

As cyber threats continue to consistently evolve in both frequency and sophistication, colleges and universities have become increasingly attractive targets for cyber-criminals. The combination of high-value data, decentralized networks, diverse user populations, and reliance on third-party systems creates a broad and challenging attack surface.

This assessment provides an overview of the current cybersecurity landscape within higher education institutions. It examines the types of data commonly stored, the motivations behind cyberattacks, prevalent security strategies, notable risks, recent incidents, and the regulatory frameworks that guide institutional cybersecurity practices. The goal of this report is to inform stakeholders of key risks and consideration, and to support ongoing efforts to strengthen the institution's security posture.

Types of Information Stored by Higher Education Institutions

Higher education institutions maintain a wide range of sensitive information within their systems at any given time. This data spans students, faculty, and staff, and includes both personal and financial records. The sensitivity of this information makes universities and other higher education institutions a significant target for cyber threats.

Student Information

Institutions store extensive personal and academic data related to students. This includes Personally Identifiable Information (PII), such as names, addresses, dates of birth, and Social Security numbers. In addition, academic records are maintained and stored, including transcripts, enrollment status, class schedules, participating in athletics or student organizations, and any honors or awards received. Universities may also store student health records, which can include highly sensitive medical information.

Student Financial Information

Financial data associated with students is another critical category. This includes information collected through financial aid processes such as FAFSA, including household income details and tax documentation used for verification. Institutions also maintain records of tuition payments, financial aid disbursements, and, in some cases, stored payment methods such as credit card numbers or bank account details.

Faculty and Staff Personal and Financial Information

Similar to sensitive personal information about students, the same PII is also stored for faculty and staff as well. Financial records for employees are also held within institutional systems. These include direct deposit information (such as bank account details) and tax withholding records.

It is important to note that some faculty and staff information such as names, titles, office addresses, and office phone numbers, is often publicly available through university directories. While this information is not considered fully private, it is frequently stored within the same systems as sensitive data, increasing the potential impact of a security breach if those systems are compromised.

Why Higher Education Data is Appealing to Cybercriminals (1)

Cybercriminals are motivated by a range of factors, including financial gain, political or ideological objectives, espionage, revenge, and in some cases, simply the challenge of exploiting vulnerable systems. Among these, financial gain remains the most common driver. The types of data stored by higher education institutions, particularly senstivie personal, academic, and financial information as listed above, make these environments especially attractice targets. Such data can be sold on illegal markets online, used for identity theft and fraud, or leveraged in extortion schemes such as ransomware attacks.

In addition to the value of the data itself, higher institutions are often considered high-risk environments due to the structure and wide accessibility of their networks. Many campuses provide widespread public or semi-public Wi-Fi access, increasing exposure to a wide range of users and increasing potential attack vectors. This open-access model, while essential for academics and accessibility, presents significant security challenges.

Furthermore, typical universities have a large and complex attack surface. Thousands of users, including students, faculty, and staff, connect to institutional systems using a wide variety of personal devices. The presence of Internet of Things (IoT) devices, such as smart classroom technology and campus infrastructure systems, further expands the number of potential entry points. This diversity makes it more difficult to enforce consistent security controls across the network.

Another contributing factor is the reliance on third-party vendors and partner organizations. Higher education institutions often integrate external systems for services such as learning management, payment processing, and research collaboration. Each third-party connection introduces additional risk, as a breach in a vendor’s systems can serve as a pathway into institutional networks or expose sensitive data.

Together, the high value of stored data and the complexity of the institutional environment make higher education a particularly attractive and vulnerable target for cyber-criminal activity.

Common Cybersecurity Protections and Strategies in Higher Education (1)

Public higher education institutions have implemented a variety of cybersecurity protections and strategies to mitigate risk and safeguard sensitive data. These measures are designed to address both external threats and internal vulnerabilities, while supporting the open and collaborative nature of academic environments.

One of the most widely adopted controls in multi-factor authentication (MFA), which requires users to provide a second form of verification beyond a password before gaining access to systems or networks. This is implemented through third-party authenticator applications, adding an additional layer of security against unauthorized access resulting from compromised credentials.

Many institutions are also adopting a zero-trust architecture model. This approach operates under the assumption that no user or device should be inherently trusted, even if it is inside the network perimeter. As a result, every access request is continuously verified, helping reduce the likelihood of lateral movements within systems if an account is compromised.

In addition to technical controls, cybersecurity awareness initiatives play a critical role in institutional defense strategies. These programs often include mandatory training for students, faculty, and staff, as well as regular phishing simulations to test user awareness. Institutions may also distribute ongoing communications from IT departments to reinforce best practices and highlight emerging threats.

Data protection measures are another key component of institutional cybersecurity. Sensitive information is commonly encrypted both at rest and in transit to prevent unauthorized access. Regular data backups are also maintained to ensure that critical systems and information can be restored in the event of data loos, corruption, or ransomware attacks.

Together, these strategies form a layered defense approach, helping higher education institutions reduce risk while maintaining the accessibility required for academic operations.

Key Cybersecurity Risks Facing Higher Education Institutions

Higher education institutions face a range of significant cybersecurity risks due to the sensitivity of their data, the openness of their networks, and the diversity of their users and systems. The following represent some of the most notable and prevalent threats in the current landscape

Ransomware Attacks

Ransomware remains one of the most serious threats to higher education institutions. These attacks typically involve cybercriminals encrypting systems or data and demanding payment in exchange for restoration of access. In many cases, attackers employ “double

extortion" tactics, in which they not only encrypt data but also exfiltrate copies of the sensitive information. They then threaten to publicly release this data unless an additional ransom is paid.

While many institutions mitigate operational disruption through regular data backups, the primary risk increasingly lies in the potential exposure of sensitive data rather than the loss of access alone. This can result in legal, financial, and reputational consequences even if systems are successfully restored.

Distributed Denial of Service (DDoS) Attacks

Distributed Denial of Service (DDoS) attacks involve overwhelming a system, server, or network with excessive traffic in order to disrupt normal operations and deny access to legitimate users. In higher education environments, such attacks can interrupt critical services, including learning management systems, email, and administrative platforms.

In some cases, DDoS attacks are also used as part of extortion schemes, where attackers demand payment in exchange for stopping the disruption.

Data Breaches and Theft

The theft of sensitive data is a persistent and financially motivated threat. As previously discussed, higher education institutions store large volumes of valuable personal, financial, and research data, making them attractive targets. The average cost of a data breach was estimated to be close to $4 million in 2023 (2), highlighting the significant financial impact of such incidents.

Beyond direct financial losses, breaches can lead to reputational damage, regulatory consequences, and a loss of trust among students, faculty, and stakeholders. Additionally, institutions engaged in research may face the theft of intellectual property or sensitive research data.

Human Factors and Insider Risk

Human behavior continues to be one of the most significant contributors to cybersecurity incidents. Errors such as falling victim to phishing attacks, using weak passwords, or mishandling sensitive data can create entry points for attackers. It is estimated that the human element plays a role in approximately 74% to 95% of cybersecurity incidents, underscoring the importance of user awareness and training as part of a comprehensive security strategy.

Recent Cybersecurity Incidents in Higher Education (3)

Recent cybersecurity incidents highlight the ongoing risks face by higher education institutions and demonstrate the real-world impact of vulnerabilities in academic environments. The following examples illustrate the scale, methods, and consequences of modern attacks.

University of Michigan (2023) (4)

In 2023, the University of Michigan experienced a significant data breach affecting approximately 230,000 individuals, including students, alumni, and employees. The compromised records contained highly sensitive information such as financial account details, Social Security numbers, driver's license information, and health data.

The breach occurred over a period of five days during which an unauthorized party gained and then maintained access to university systems. Upon detection, the university was forced to disconnect its campus from the inter and engage third-party cybersecurity experts to assist with investigation and remediation efforts.

Mount Saint Mary College (2022) (5)

Mount Saint Mary College was the target of a ransomware attack in December 2022. During the incident, attackers exfiltrated sensitive data and demanded payment in exchange for not releasing the information publicly. Following guidance from the FBI, the institution chose not to pay the ransom.

As a result, the stolen data was published online by the attackers in February 2023. In response, the college offered affected individuals free credit monitoring and identity theft protection services to mitigate the impact of the breach.

University of Pennsylvania (2025) (6)

In 2025, the University of Pennsylvania experienced a cyberattack involving identity impersonation and social engineering techniques. Attackers gained access to multiple official email accounts and used them to impersonate legitimate university representatives.

This access was leveraged to deceive individuals and gain entry into systems containing sensitive data. The group responsible claimed to have stolen over one million records, including PII related to donors, alumni, and students. This incident demonstrates the growing sophistication of attacks that exploit human trust in addition to technical vulnerabilities.

Key Regulations and Cybersecurity Frameworks in Higher Education (7)

Higher education institutions are subject to variety of legal, regulatory, and industry standards designed to protect sensitive data and ensure strong cybersecurity practices. Compliance with these requirements is essential not only for legal and regulatory reasons, but also for maintaining trust and reducing institutional risk.

Privacy Laws and Regulatory Requirements

Institutions must comply with multiple federal regulations governing the protection of sensitive information:

- The Family Educational Rights and Privacy Act (FERPA) (8) protects the privacy of student education records and applies to all institutions that receive funding from the U.S.

Department of Education. It governs how student information is accessed, shared, and disclosed.

- The Health Insurance Portability and Accountability Act (HIPAA) establishes standards for safeguarding sensitive health information. It applies to any health-related data maintained by institutions, such as student health services records.
- The Gramm-Leach-Bliley Act (GLBA) of 1999 (9), also known as the Financial Services Modernization Act, requires institutions to explain how they collect, use, and share financial information. It also mandates safeguards to protect that data and allows individuals to opt out of certain types of information sharing with third parties.

Cybersecurity Frameworks and Standards

In addition to regulatory requirements, institutions often adopt established frameworks and standards to guide their cybersecurity programs:

- The NIST Cybersecurity Framework provides a flexible, risk-based approach to managing and reducing cybersecurity threats. It is widely used across both public and private sectors due to its adaptability.
- ISO/IEC 27001 is an internationally recognized standard for information security management. It requires organizations to establish, implement, maintain, and continuously improve an Information Security Management System (ISMS) to manage data security risks effectively.
- The Higher Education Community Vendor Assessment Toolkit (HECVAT) is specifically designed for higher education institutions to evaluate the security posture of third-party vendors. It is commonly used when assessing services such as cloud platforms, learning management systems, and financial service providers.

Conclusion

The cybersecurity landscape in higher education is defined by a combination of high-value data, complex IT environments, and persistent, evolving threats. Institutions must contend with risks ranging from ransomware and data breaches to social engineering and human error, all while maintaining the accessibility and openness that are fundamental to their mission.

Although many institutions have implemented important safeguards, such as multi-factory authentication, zero-trust principles, user awareness training, and data protection measures, these controls must continuously evolve to address emerging threats and vulnerabilities. Recent cybersecurity incidents demonstrate that even well-resourced organizations remain susceptible to attacks, particularly those that exploit human behavior or third-party dependences. Compliance with regulatory requirements and adoption of established cybersecurity frameworks provide a strong foundation for risk management. However, effective cybersecurity ultimately requires a comprehensive, layered approach that integrates technology, policy, and user behavior.

Sources

1.) Bank of America, "Cyber Attack Protection for Schools & Universities", n.d.
2.) Edward Cost, Upguard, "Human Factors in Cybersecurity in 2026", January 5, 2026
3.) Asimily, "4 Cyberattacks that Shook Colleges and Universities in the Last Year", 2024
4.) Lauren Coffey, Inside Higher Ed, "Hackers Accessed Data of Up to 230,000 at University of Michigan", October 25, 2023
5.) Mount Saint Mary College, "Cybersecurity incident at MSMC", February 9, 2023
6.) Kriti Tripathi, Seceon, "The University of Pennsylvania Data Breach: What It Reveals About Cybersecurity in Higher Education", November 12, 2025
7.) Sentinel One, "Cybersecurity in Higher Education: Risks, Best Practices & Frameworks", February 2, 2026
8.) U.S. Department of Education, "Protecting Student Privacy - FERPA", n.d.
9.) Federal Trade Commission, "Gramm-Leach-Bliley Act", n.d.