BANK OF AMERICA

Higher ed is a top target for cyber criminals

Here’s how institutions can improve safety.

Colleges and universities have unique characteristics that make them vulnerable to cyber crime, but there are ways they can help protect themselves.

It’s no secret that higher education institutions have become top targets for cyber crime. News stories like those about a public health sciences university being forced to pay over $1 million to cyber criminals after a ransomware infiltration,[1] or a 157-year-old private college that had closed permanently after being targeted by criminals,[2] make that clear. This is in part because colleges and universities have unique vulnerabilities as well as attributes that make them particularly appealing targets.

Successful cyber attacks don’t just have financial implications for institutions, though. Security breaches can also result in loss of personal information, intellectual property and other sensitive data as well as reputational damage, which can be critical in an increasingly competitive market.

Why higher ed is more vulnerable

Characteristics of college campuses that make them uniquely interesting — such as the emphasis on independence, the free flow of ideas and the diversity of skills and backgrounds of both students and staff — can also make common goals such as cyber security more difficult. With Wi-Fi accessible across entire campuses — in dorms, libraries, classrooms, labs, dining halls, faculty and administrative offices — and a diffuse, diverse body of administrators, professors, employees and students used to connecting to school networks when and where they want, higher education institutions can be more vulnerable to cyber crime than corporate environments where strong security requirements can be more easily imposed.

In addition, the pandemic accelerated dramatic changes to the education technology landscape, including the expansion of remote learning and a steep increase in digital tools used in the classroom. Combined with a population of students who may be new to living on their own and less concerned with security risks, it’s clear why education and research institutions saw a 114% increase in cyber incidents between 2020 and 2022, and the sector experienced the highest volume of attacks in any industry every month in 2021 and 2022.[4]

Colleges and universities are not only more vulnerable, but they’re also target-rich environments, housing a tremendous amount of data, including valuable intellectual property as well as personally identifiable information (PII) from students, parents, staff and vendors. The volume of threats is only increasing, with stolen academic credentials among the most commonly trafficked by criminals.[5] To protect your institution, you must consider what the risks are and then follow best practices to reduce those risks to an acceptable level.

Education and research institutions saw a 114% increase in cyber incidents between 2020 and 2022, and the sector experienced the highest volume of attacks in any industry every month in 2021 and 2022.[3]

[1] University of California San Francisco, “Update on IT Security Incident at UCSF,” June 2020.

[2] IT Governance, “Lincoln College Shuts Down After 157 Years Following Ransomware Attack,” May 2022.

[3] Check Point Software, “Cyber Attack Trends: 2022 Mid-Year Report,” August 2022.

[4] Ibid.

[5] FBI, “Compromised US Academic Credentials Identified Across Various Public and Dark Web Forums,” May 2022.

Risks colleges and universities are facing

To keep an institution safe as a business and protect its networks, applications and people from cyber attacks, it's important to first understand the risks involved.

Be(aware) of the risks

- Ransomware/Double extortion
- DDoS
- Data theft
- Compliance requirements

Ransomware — and double extortion

As in almost every industry, the threat of ransomware in education is increasing at an alarming rate, with 64% of higher education organizations hit by ransomware in 2021.[6] But ransomware itself is just the tip of the iceberg. Whereas ransomware encrypts or blocks access to your systems and data until you pay a ransom, a bigger threat comes with so-called double (or even triple) extortion: when cyber criminals retain copies of your sensitive data and threaten to make it public unless you pay additional ransoms. Given that in 2021 70% of higher education institutions were able to use backups to recover their data, versus just 50% that paid ransom to do so,[7] the exfiltration of data may ultimately be the greater risk from ransomware attacks.

Distributed denial of service attacks

Ransom demands are also a component of distributed denial of service (DDoS) attacks, in which perpetrators disrupt an organization's website or other servers and networks by overwhelming them with malicious traffic. A common tactic of cyber criminals is to extort a ransom by threatening to carry out a DDoS attack. While DDoS incidents saw an overall decrease during the second half of 2021, those specifically targeting higher education rose 102% in that same period.[8]

Data theft

Whether it's intellectual property from research and development, PII from the student body, faculty and administrative staff, or the vast amount of financial information including departmental budgets, staff compensation, new student accounts and financial aid loans, the amount of valuable data stored at a college or university is an attractive payload for cyber criminals.

Compliance requirements

Besides the threat from criminal activities, colleges and universities must also be sure that they're following an ever-growing number of privacy laws and regulations, including but not limited to:

- Family Educational Rights and Privacy Act of 1974 (FERPA)[9] — Protects privacy of student education records.
- Gramm-Leach-Bliley Act of 1999 (GLBA)[10] — Requires financial institutions to detail information-sharing practices and safeguard sensitive data. A recent amendment to the GLBA stipulates that higher ed institutions participating in Federal Student Aid programs must comply with specific security mandates by June 2023.[11]
- Higher Education Act of 1965 (HEA)[12] — A reauthorization of the act in 2008 requires universities to provide important information to students about student record privacy and financial aid information, among other required disclosures.

For more information on federal student privacy laws, see the U.S. Department of Education's Protecting Student Privacy site.

> Not only have cyber attacks disrupted classes and exams at many universities,[13] but also breaches at education institutions cost close to $4 million on average in 2022.[14]

Best practices for keeping institutions safe

Cyber crimes can cause costly and irreparable damage to universities. Not only have cyber attacks disrupted classes and exams at many universities,[15] but also breaches at education institutions cost close to $4 million on average in 2022[16] — not to mention less-quantifiable reputational damage as well as

[6] Sophos, "The State of Ransomware in Education 2022," July 2022.
[7] Ibid.
[8] Netscout Systems, "Netscout Threat Intelligence Report, Issue 8: Findings from 2nd Half 2021," March 2022.
[9] The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g).
[10] Gramm–Leach–Bliley Act (GLBA), also known as the Financial Services Modernization Act of 1999, (Pub. L. 106–102).
[11] Kristal Kuykendall, Campus Technology, "FSA Details Data Security Requirements Taking Effect June 9," February 2023.
[12] Jennifer Gregory, IBM Security Intelligence, "Ransomware Attackers Target U.S. Colleges and Universities," October 2022.
[13] Ibid.
[14] IBM and Ponemon Institute, "2022 Cost of a Data Breach Report," July 2022.
[15] Jennifer Gregory, IBM Security Intelligence, "Ransomware Attackers Target U.S. Colleges and Universities," October 2022.
[16] IBM and Ponemon Institute, "2022 Cost of a Data Breach Report," July 2022.

theft of data and ideas. To keep your institution protected, follow these best practices:

- Educate
- Authenticate
- Update
- Safeguard
- Prepare
- Motivate

Countering cyber crime

1. **Educate: Train faculty, staff and students on cyber hygiene.** It's critical to build cyber security training into every person's schedule. Given the heavy workloads typical in a higher education population, it's important to embed cyber security awareness into the daily culture rather than make it a once-a-year event.

2. **Authenticate: Strengthen user access protocols.** In addition to using single sign-on and multifactor authentication, consider adopting continuous authentication, a variation of a zero-trust model that assesses user behavior patterns to confirm identity in real time on an ongoing basis.

3. **Update: Ensure all software is up to date.** Ensure that anti-malware tools are installed or available to the entire university population and that security patch management for operating systems and applications is automated and up to date.

4. **Safeguard: Plan for protecting both institutional and student data.** In addition to planning for data resilience with a strong backup methodology to reduce the risk of data loss, it's critical to protect key data throughout its lifecycle. By using methods such as encryption or segmentation, you can reduce the risk of sensitive data exposure in the event of a security breach.

5. **Prepare: Document and test an incident response plan.** Develop and implement comprehensive measures for responding to cyber security events. Being prepared can help you take action before lasting damage is done.

6. **Motivate: Reach across the organization to build a culture of cyber security.** Use cyber security frameworks and engage leadership from every department to get a holistic view and buy-in from across the institution. This includes ensuring your board members understand the risks and liabilities involved so that they are prepared to budget for the resources, technology and education to reduce risk to an acceptable level. And finally, empower your students by not only educating them, but also including them in your detection and planning processes.

Understanding the risks that are making higher education institutions more vulnerable to cyber attacks and embedding security awareness into the daily activities of students, faculty and staff can help build a culture of cyber security and keep an institution's valuable data, finances and reputation protected.

BANK OF AMERICA

"Bank of America" and "BofA Securities" are the marketing names used by the Global Banking and Global Markets divisions of Bank of America Corporation. Lending, other commercial banking activities, and trading in certain financial instruments are performed globally by banking affiliates of Bank of America Corporation, including Bank of America, N.A., Member FDIC. Trading in securities and financial instruments, and strategic advisory, and other investment banking activities, are performed globally by investment banking affiliates of Bank of America Corporation ("Investment Banking Affiliates"), including, in the United States, BofA Securities, Inc. and Merrill Lynch Professional Clearing Corp., both of which are registered broker-dealers and Members of SIPC and, in other jurisdictions, by locally registered entities. BofA Securities, Inc. and Merrill Lynch Professional Clearing Corp. are registered as futures commission merchants with the CFTC and are members of the NFA.

Investment products offered by Investment Banking Affiliates:	Are Not FDIC Insured	Are Not Bank Guaranteed	May Lose Value