Target: Education

3 things to know about ransomware in higher education, and how you can protect your institution

Ransomware is on the rise

Cybersecurity in higher education reflects a dynamic and evolving challenge. Breaches can lead to the compromise of personal information, intellectual property theft, and disruptions to learning. Ransomware in particular is a growing threat to educational institutions around the world.

Effective cybersecurity measures both protect confidential data and uphold the institution's reputation, ensuring a safe digital environment conducive to learning, research, and innovation.

Here's what your campus needs to know about the state of ransomware and cyberattacks in higher education.

intel vPRO

An Evo™ Design

Windows 11

Secure and scalable IT

Smarter technology for all

Lenovo

1 No other industry faces more cyberattacks

The education industry accounts for a staggering 80% of all reported malware.[1] No other industry comes close. When it comes to ransomware, mean recovery costs across all industries reached $1.82 million in 2023 — a number far harder to absorb at higher education institutions, whose budgets are impacted by limited funding and declining enrollment.[2]

Higher education colleges and universities have increasingly become prime targets for ransomware attacks due to a combination of factors that make them more vulnerable. Institutions typically house vast repositories of sensitive and valuable data ranging from student records and research findings to financial information. This wealth of data is an attractive lure for cybercriminals seeking to extort money through ransomware attacks.

Many colleges and universities have decentralized IT infrastructures in which numerous departments and faculty members manage their own systems and devices. This fragmentation makes it challenging to enforce uniform cybersecurity protocols, creating weak points that attackers can exploit. Combined with the education industry's tight budgets, this can lead to underinvestment in cybersecurity measures and outdated software systems — making breaches easier for attackers.

Lenovo ThinkShield can alleviate the IT workload and minimize downtimes with fully integrated and tested solutions. Leveraging cutting-edge predictive technology, ThinkShield automates tasks that could otherwise pose a significant burden.

The challenges higher education faces

Hover to learn more

2 The leading root causes

Attackers gain access in a number of different ways, and there are differences in root causes by industry. In higher education, exploited vulnerabilities are the most common avenue leading to a ransomware attack, followed by compromised credentials.[2]

Potential vulnerabilities can be the result of several factors. For example, outdated software and systems due to budget constraints or an inability to adequately maintain a legacy system can create an environment attackers can exploit. Other vulnerabilities include a culture of openness and collaboration at many institutions, as well as inadequate cybersecurity awareness.

With so many attack vectors, the best defense for any institution is a wide-ranging one. Lenovo ThinkShield creates an ecosystem that brings best-of-breed solutions together to ensure end-to-end security for your faculty and students in a borderless campus. It incorporates ThinkShield Threat Isolation by BUFFERZONE for browser, email, and application security; Absolute for device fleet control; ThinkShield Data Defense by Cigent for data security; and many other security solutions.

Root causes of ransomware attacks in higher ed[2]

Hover to learn more

3 Not all devices are created equal

At many institutions, students and faculty bring their own devices. Every phone or laptop that connects to your network brings with it its own set of vulnerabilities. The shift to a borderless campus, where learning takes place on- and offsite, opens up other potential routes of exposure to attacks.

Not every student stays up to date on the latest security patches for their personal devices. This is where built-in security measures can make all the difference. Out-of-the-box protections come standard on Lenovo devices like the ThinkPad® L13 or ThinkPad® X1 Yoga Gen 6 running Microsoft Windows 11 and powered by Intel vPro®, An Intel® Evo™ Design that's built for what IT needs and users want. These measures include features like Microsoft Secured-core PC, secure wipe, self-healing BIOS, a tamper switch, and a webcam privacy shutter. They help mitigate user behavior actions that could open up your institution to an attack.

Powerful protection

Safeguard students, faculty, and campuses from cyberthreats, no matter where learning happens, now and in the future.

Windows 11 is the most secure Windows yet with multiple layers of protection enabled by tightly integrated hardware and software.

Windows 11 is built on Zero Trust security principles, which provide comprehensive control over access to information, applications, and network resources from anywhere without compromising the user experience.

Microsoft has an unparalleled view of the evolving threat landscape across all types of devices, apps, platforms, and endpoints, and they integrate the learnings from vast signal intelligence and world-class threat intelligence into all the products and services they offer. Even better, higher education institutions can realize up to 60% cost savings when they use Microsoft security, compliance, and identity end-to-end solutions.*

* Savings based on publicly available estimated pricing for other vendor solutions and web direct/based price shown for Microsoft offerings. Price is not guaranteed and subject to change.

intel vPRO

An Evo Design

Windows 11

Secure and scalable IT

Smarter technology for all

Lenovo

Safeguard your borderless campus

Backed by the power of ThinkShield, which utilizes Intel® Hardware Shield for below-the OS protection, the Lenovo team can help protect your campus with a multilayered approach to cybersecurity. With a flexible security strategy, you can armor your borderless campus so faculty and students can work and learn without disruptions.

Learn more at www.lenovo.com/Higher-Education.

Sources

1 Microsoft Security Intelligence, "Global Threat Activity," August 2023

2 Sophos, "The State of Ransomware 2023"

CHECKLIST

Protect your institution

How does your borderless campus measure up?

These questions and considerations can help you assess your security situation.

☐ **Learning happens everywhere.** What security considerations are you making for remote and off-campus learning?

☐ **Old or outdated devices can be exploited by attackers.** What is your device refresh policy?

☐ **The most common root cause of ransomware attacks in education is exploited vulnerabilities.** What vulnerabilities has your team identified?

☐ **A top defense is a well-educated user base.** What security training do you provide to both students and faculty?

☐ **Email is another attack avenue with phishing or malicious links.** What protections do you have in place to minimize email risks?

☐ **The right devices can make all the difference.** What built-in security measures are included with your current devices?

☐ **Cybersecurity is constantly evolving.** Is your current security plan flexible and actionable? If not, do you need support?

Built-in security features like biometrics, an IR camera, PrivacyGuard, and Intel® Hardware Shield come standard on devices like the Lenovo ThinkPad® X1 Yoga running Windows 11 and powered by Intel vPro®, An Intel® Evo™ Design with the latest Intel® Core™ processors.

intel vPRO

An Evo™ Design

Windows 11

Secure and scalable IT

Smarter technology for all

Lenovo