

Lenovo  
Education

## More savvy, more secure

The alarming rise of cyberthreats  
in higher education and what  
to do about it



Smarter  
technology  
for all

Lenovo

When it comes to cyberthreats in the education sector, the pandemic only served to accelerate and exacerbate an already concerning trend. Data breaches rose precipitously and ransomware demands skyrocketed.

Cybersecurity has become the number one priority of education IT leaders.<sup>1</sup> Like their counterparts in other sectors like business, healthcare, and government, they weathered an abrupt shift to remote work with its proliferation of BYOD, home networks, explosion of support needs — and off-the-charts security vulnerabilities. Students, faculty, and staff all needed digital tools to stay connected and productive from anywhere. And they still do.

With the shift to more connected, borderless campuses, security concerns are growing, and the need for swift and strategic response is growing with them. One key part of a solid strategy is choosing solutions that offer both strong performance and strong security — like the Lenovo ThinkPad® L14 laptop with the built-for-business Intel vPro® platform and Windows 11.





## Why target education?

Lucrative target + significant vulnerability. Score!

### Education leads the pack — and not in a good way

By August 2020, cyberattacks were up:<sup>2</sup>

**30%**

in higher education

**6.5%**

across all other industries

### What's wrong with this picture?

In fact, the upward trend of attacks became so concerning in March 2021 that it prompted the FBI Cyber Division to issue a warning specifically about targeted institutions, including universities and colleges.<sup>3</sup>



### Among higher ed institutions:

**87%**

were planning for hybrid instruction in summer 2020.<sup>4</sup>

**54%**

increased spending on online learning systems.<sup>5</sup>

**72%**

believe the split between online/in-person is here to stay.<sup>5</sup>

The more remote learning offered, the more dispersed the campus population and the more vulnerable devices, data, and networks become. The borderless campus is an exciting, emerging higher ed vision. But the same borderless campus that heralds new flexibility, collaboration, and personalized learning can spell big risk for IT leaders.

As the perimeter expands and endpoints multiply, IT is challenged to find the right balance between giving users the simple, timely access they need while protecting the institution and keeping it ready to handle the next disruption without a break in continuity. Solutions like Lenovo devices with Windows 11 and the built-for-business Intel vPro® platform offer built-in security to safeguard mobile teachers and learners wherever they are.

Detected ransomware attacks rose

# 715%

from 2019 to 2020.<sup>6</sup>

Higher ed had the

# highest

rate of any industry.<sup>7</sup>



## Higher ed is particularly appealing to cybercriminals.

### Why?

- **PII.** Sensitive personally identifiable information and plenty of it — black market gold
- **Research.** Data and intellectual property for highly confidential projects
- **Outdated infrastructure.** Easily exploited legacy systems
- **High-volume, untrained network users.** Lack of security awareness and precautions for devices and applications
- **Open environments.** Inherently accessible to the campus population and sometimes the public

## Tricks of the trade: What do hackers have up their sleeves?

Cybercriminals are usually after money, and they're devious about how they get it.

- **Socially engineering.** Phishing, spear phishing, and spoofing trick users into giving up personal information, especially login credentials, that's used to breach systems. This psychological manipulation is surprisingly successful.
- **Hacking.** Criminals identify and exploit system or network weaknesses to gain data access. Password-cracking algorithms are used to break into a computer system and steal resources.
- **Ransomware attacks.** This extortion tactic paralyzes systems and operations or threatens exposure of sensitive data unless a ransom is paid.



## Risk without reward

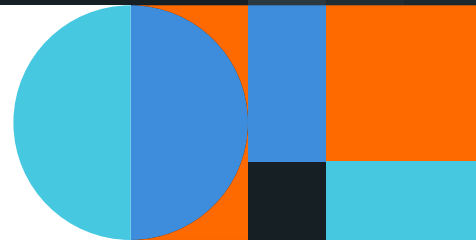
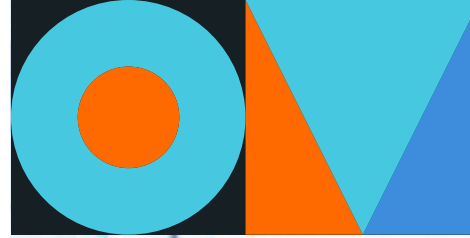
Perhaps no one but school administrators talks about one of the biggest risks of cyberattacks to higher ed institutions: reputation. Schools have a bond of trust with students, professors, and families. If that bond is broken, the consequences can be significant and long-lasting. They can affect the school's brand and enrollment — and even their insurance premiums if circumstances are considered unsafe.

Then, of course, there are financial ramifications. Ransomware demands can run into the millions. The average cost of just one data breach in higher ed is \$3.79 million.<sup>8</sup> Lenovo devices, including the ThinkPad L14 laptop with Windows 11 and the built-for-business Intel vPro<sup>®</sup> platform, safeguard systems and data — helping stave off extreme consequences.

## It's not just about the devices

3 more places hackers love to visit?

- Networks
- Storage
- Cloud-based applications





## Cyberattacks hurt. How can you help?

Dive into a defense-in-depth (DiD) strategy. DiD is a well-rounded cybersecurity approach that layers protection in three categories: people, process, and technology. Functions like your access control, identity management, firewall, antivirus, and other solutions are fully integrated and working together with the rest.

Intentionally designed with redundancies, the strategy addresses security as a whole as well as individual attack vectors. DiD is often called the “castle approach” because it’s similar to the defenses of a medieval castle. You can complement your DiD strategy with devices that offer built-in security — like the ThinkPad L14 laptop with Windows 11 and the built-for-business Intel vPro® platform.

Educational institutions must brace themselves for a continuing onslaught of cyberattacks.

Malwarebytes

## People: Your biggest vulnerability and best defense

Employee mistakes cause 88% of today’s data breaches.<sup>9</sup> Cybersecurity awareness and training go a long way to prevent both skill-based and decision-based errors. Students, faculty, and staff will all benefit from training in these four Rs:

- Remember best practices
- Resist social engineering
- Recognize potential threats
- Report suspicious activity

Human behavior is the most important thing in cybersecurity.

Kelvin Coleman,  
executive director, National Cyber Security Alliance (NCSA)



## Defend your data

When you're considering data protection solutions, make sure the features are comprehensive and complementary. Here's a quick checklist to help guide your decision. Lenovo built-in security works with Windows 11 and the built-for-business Intel vPro® platform to cover all these bases and more.

- **Next-gen cloud-based, autonomous antivirus protection.** Predict, prevent, and stop even zero-day attacks, alerting the network and rolling devices back to a clean, known good (pre-breach) state.
- **Data encryption.** Encrypt from end to end so sensitive data can be safely shared whether it lives on a device, hard drive, or in the cloud.
- **Frictionless authentication.** Limit sensitive data access to authorized users with multiple authentication modes.
- **Secure disposal.** Protect your data, even when your device reaches end of life — with options to keep your hard drive or securely wipe the data and dispose of the device responsibly.



## Increase effectiveness and efficiency

One way you can free up time to focus on strategic planning and other priorities is with a Device as a Service solution. DaaS advantages include hands-off end-to-end management, the latest devices, and one predictable subscription fee.

Traditional monolithic approaches to cybersecurity are becoming less reliable.

Richard Rudnicki,  
security specialist, Deloitte

Cybersecurity demands a strategic approach because it is difficult, rapidly changing, and potentially devastating to a college or university.

Don Welch, vice president for information technology and chief information officer,  
Pennsylvania State University




# Looking for security solutions? Look for a partner.

As hybrid learning takes hold and evolves, most institutions are still feeling their way. The best technology providers go beyond selling components to work with you as a trusted advisor and true partner. Seek out technology leaders who collaborate with other leaders to deliver end-to-end solutions — compatible hardware, integrated software, and services that make your life easier — with one point of contact.

Lenovo delivers solutions to safeguard your institution no matter where learning takes place.



BUILT FOR BUSINESS

A collection of abstract geometric shapes in shades of blue and orange, including a large blue circle with an orange center, and several overlapping curved shapes in blue and orange.

Find out more about our built-in security that works together with Absolute® and SentinelOne® software, Microsoft Windows 11, and the Intel vPro® platform with business-like performance for the classroom. When you're ready, we're here to help.

Discover more at

[www.lenovo.com/Higher-Education](http://www.lenovo.com/Higher-Education).

#### SOURCES

- 1 EdTech magazine, "Cyberattacks Increasingly Threaten Schools — Here's What you Need to Know," June 2020
- 2 Check Point Software Technologies, "Not for Higher Education: Cybercriminals Target Academic & Research Institutions Across the World," September 2020
- 3 Inside Higher Ed, "FBI Warns of Increased Ransomware Attacks Targeting Colleges," March 2021
- 4 Institute of International Education, "COVID-19: Effects on U.S. Higher Education Campuses," July 2020
- 5 CDWG, "Building out blended learning environments for higher education," 2021
- 6 Bitdefender, "Mid-Year Threat Landscape Report," 2020
- 7 College is Education, "10 Concerning Stats About Cybersecurity in Higher Ed," May 2021
- 8 IBM, "2021 Cost of a Data Breach," 2021
- 9 Stanford University Professor Jeff Hancock and Tessian, "Psychology of Human Error," April 2020

© Lenovo 2021. All rights reserved. v1.00 October 2021.

Lenovo