Connected Device Security and Vulnerability Management for Higher Education

The education sector in general has experienced a substantial increase in malware attacks. Since 2023, the number of attacks against the sector has increased by 961%, according to Zscaler data. Education is another industry that tends to have limited investment in cybersecurity. The bulk of IT spend in education relates to increasing access for students and teachers.

Education tends to have the same low tolerance for downtime as healthcare. So it makes sense that education would be an attractive target for threat actors. When these attacks are conducted, the limited cybersecurity investment means that downtime is severe. Between 2022 and 2023, in fact, the average amount of downtime for educational institutions caused by ransomware disruptions has increased from 7.9 days to 11.6 days, while the average cost of a data breach in higher education remained fairly steady at $3.65 million.

They have large and complex attack surfaces, including many user-owned and Internet of Things (IoT) devices. This has the dual impact of being extremely challenging to secure and providing many potential entry points for cybercriminals.

Most have complex partner and vendor networks, placing them at high risk of third-party data breaches. Approval for adding devices to networks is often distributed by schools, departments or even individual faculty members.

IoT Risks for Universities

IoT devices are often insecure. They come with default passwords that are easy to guess and difficult to change before connecting to the internet. Their firmware is often built with speed to market instead of security at the forefront. Further, the reality that IoT devices lack agreed-upon security standards means that device manufacturers have no real best practices to adhere to. This creates what amounts to thousands of potentially insecure devices out in the real world. Even without the basic lack of security in IoT devices, however, cybercriminals still find the higher education sector a target-rich environment.

Top IoT Security Challenges

- Growing Attack Surface
- Connected Supply Chains
- Legacy Systems and Equipment
- Accurate IoT Inventories
- Third-party Security Standards
- Regulatory Compliance

Recent Attacks on Higher Education and the Consequences

Unfortunately, cybercriminals have realized that higher education institutions present an opportunity for profit. Until that changes—most likely through a significant additional investment in cybersecurity across the industry—high-profile breaches in the industry will continue to be a common feature in the media.

Most attacks are financially motivated, with attackers aiming to steal or encrypt sensitive data (or both) and demand a ransom payment for its safe return. However, there is a historic precedent for large-scale espionage attacks against higher education institutions, including by state-sponsored threat groups in Iran and China.

Verizon's 2023 Data Breach Investigations Report found that around 92% of attacks are financially motivated across the broader education industry, while 8% are espionage. In higher education, it's reasonable to assume a slightly higher rate of espionage, though it should be noted that many cyber espionage attacks go unnoticed due to high levels of attacker skill and the lack of overt demands.

The fact is that higher education institutions make excellent targets for cybercriminals for a number of reasons:

- Universities and colleges have a low tolerance for downtime, making them susceptible to paying ransom demands in an effort to "limit the damage" of a cyberattack.
- They have large and complex attack surfaces, including many user-owned and Internet of Things (IoT) devices. This has the dual impact of being extremely challenging to secure and providing many potential entry points for cybercriminals.
- Most have complex partner and vendor networks, placing them at high risk of third-party data breaches. Approval for adding devices to networks is often distributed by schools, departments or even individual faculty members.
- While they often spend heavily on IT, most of this goes on improving functionality and access for faculty and students—not on securing increasingly complex IT infrastructure.

In reality, many cyberattacks against higher education institutions go unreported in the media, and in many more cases, universities never publicly share the extent or cause of breaches. In all likelihood, the frequency and severity of cyberattacks in higher education are even higher than the reported figures suggest.

A few of the most recent attacks on universities and colleges include:

- The University of Michigan suffered a data breach in August 2023 that compromised data from 230,000 students, alumni, and employees. The university disconnected its campus network and launched an investigation into the source of the breach.

- The Stanford University Department of Public Safety was attacked in October 2023, with the Akira ransomware gang claiming they stole 430 GB of campus police data. The university confirmed the attack in November.

- Mount Saint Mary College in Newburgh, New York, confirmed a December 2022 ransomware attack following the group Vice Society claiming credit on its leak site. The college said in their statement that they detected and stopped the attack, months after keeping the incident silent.

- The University of Missouri System was caught up in the MOVEit file transfer breach through one of its third-party vendors used in enrollment operations. The university system said that some of its data had been compromised but did not clarify because of the ongoing investigation.

Unmanaged IoT Devices Leads to Increased Attack Surface and Risk

Shadow IT is one of the most persistent cybersecurity challenges today. Already, researchers estimate that 53% of departments refuse to use IT-approved tools and 80% of workers admit to using SaaS applications at work without getting approval from the IT department.

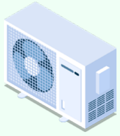
Connected devices often have at least a network interface, like ethernet, Bluetooth, Long-Term Evolution (LTE), Zigbee, Wi-Fi, 5G, or Ultra-Wideband (UWB). Once deployed in a network using these connection methods, IoT systems can be readily discovered and connected to the open internet. This is a major issue because they're not designed to have any setup protocols before connecting to the internet.

Once threat actors gain initial access into a network from a discoverable IoT device, they're able to laterally move deeper into the information architecture to achieve their goals. At the individual device level, IoT equipment is particularly vulnerable to common security pitfalls.

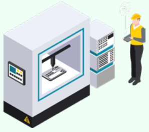
In terms of which categories of connected devices organizations tended to buy, Keyfactor research found that companies tended to deploy the following IoT solutions:

Hybrid work technologies	53%
Security cameras	53%
Real-time monitoring and location tracking	52%
Inventory and asset management	46%
Door locks or physical security	43%
Smart lighting	40%
Space utilization technology/tools	38%
Air quality monitoring	35%

Common Unmanaged IoT Devices


HVAC

Sensors


Equipment

Routers

Smart Energy Meters

Workstations

Drones

Printers & Scanners

TVs

Alarms

Badge Readers

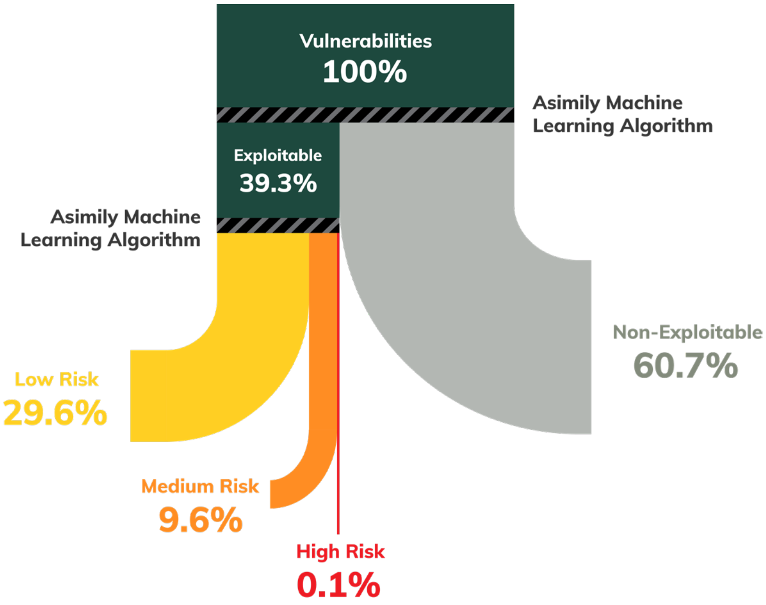
Security Cameras

Autonomous Vehicles

Secure Your Connected IoT Devices and Reduce Vulnerabilities 10x Faster with Half the Resources

Your reputation depends on timeliness and avoiding delays. When threats are kept out, everything stays on time and business can grow. Asimily IoT security solutions help you ensure that outside attackers don't affect your operations.

Asimily empowers vulnerability management teams to tackle the riskiest issues first. Instead of just giving you a list of vulnerabilities to fix, Asimily combines that information with unique Impact and Likelihood analyses to get a risk-ranked set of devices whose vulnerabilities can be mitigated.



Accurate Inventory & Unmatched Visibility

Harness Asimily's powerful protocol analyzer and deep packet inspection (DPI) to safely discover and automatically categorize your IoT assets, services, connections, and apps giving you the power to proactively manage risks, optimize resources, and fortify your security like never before.

Vulnerability Prioritization & Efficient Mitigation

Asimily's unique Impact, Likelihood and Utilization analyses show which vulnerabilities attackers will take advantage of in your environment. Allocate your resources to the riskiest devices first to promptly address vulnerabilities.

Threat Detection & Incident Response

Set device behavior rules that instantly identify any suspicious activities. Our engine swiftly spots deviations from normal behavior, ensuring that you can respond promptly to potential threats. Detect misconfigurations as well, keeping security posture high.

Risk Modeling & Simulations

Envision, predict, and act with unparalleled confidence, and unlock a new era of proactive risk mitigation. Calculate the least risk associated with a device before configuration and connection.

Connected Device Security, Reimagined

Securing the Internet of Things is far more complex than securing traditional IT equipment. Poor security practices at IoT device manufacturers paired with minimal visibility by IT and security teams make connected equipment a major security risk. The distributed and broadly installed nature of these devices means that a risk-based approach is required. This can be done, and thankfully Asimily can help companies implement and manage a risk-focused method of securing IoT devices for a more secure future.

Asimily's IoT Risk Management Platform

- Creates a complete IoT inventory, collecting 100+ attributes for each device;
- Identifies and prioritizes the riskiest vulnerabilities;
- Recommends simple, validated mitigation actions;
- Conducts a full flow analysis for each device, recording all communication patterns across the network;
- Calculates risk for every connected device based on device attributes, dataflows, vulnerabilities, anomalies, configuration, and overall criticality of the device on operations;
- Generates ACLs for targeted segmentation for use by a NAC;
- Flags anomalous device behavior based on profiling data from millions of IoT devices;
- Makes it easy to set policies to monitor accepted risks and identify suspicious activity proactively;
- Automates packet capture for forensic analysis of any IoT device to support root cause analysis;
- Documents when the device is being used so users can understand utilization and operational efficiency;
- Allows device configuration snapshots to be taken, to thwart ransomware and simply recovery; and
- Risk simulator helps determine the benefit of work before it is performed, increasing team efficiency.

Asimily can help enterprise organizations drastically reduce cyber risk while minimizing resource and time costs.

To see how Asimily can help your organization, **arrange a demo today.**

About Asimily

Asimily is an industry-leading risk management platform that secures IoT devices for medical, diagnostic, life sciences, pharmaceutical, and enterprise companies.

Connect With Us

info@asimily.com
440 N Wolfe Road
Sunnyvale, CA 94085
(833) 274-6459
(833) ASI-MILY