CYBERSECURITY IN EDUCATION

SAFEGUARDING THE FUTURE OF LEARNING

Honeywell

THE DIGITAL TRANSFORMATION OF EDUCATION

Across K–12 schools and higher education institutions, technology has become the backbone of modern learning.

Students rely on laptops and tablets. Teachers use smart boards and cloud-based platforms. Administrators manage operations through connected building systems. This digital transformation has opened new doors for personalized learning, collaboration, and operational efficiency.

But it has also opened new doors for cybercriminals.

As educational environments become more connected, they also become more vulnerable. Cybersecurity is no longer a back-office concern — it's a strategic imperative. The systems that power learning, safety, and comfort are now potential entry points for ransomware, data breaches, and operational disruption.

WHY CYBERSECURITY MATTERS MORE THAN EVER

The education sector has become a prime target for cyberattacks. In the first half of 2025 alone, ransomware attacks on educational institutions surged by 23%, with higher education accounting for nearly half of all incidents[1]. K–12 schools are also under siege, with 82% of schools reporting a cyber incident between July 2023 and December 2024[2]. Attacks such as these can disrupt learning, expose sensitive student data, and force institutions to pay ransoms or even rebuild systems from scratch.

What makes schools such attractive targets? They hold vast amounts of personal data including student records, health information, and financial and behavioral data. Many institutions also operate with limited IT resources, outdated infrastructure, and minimal cybersecurity staffing.
And while IT systems often receive some level of protection, operational technology (OT) — the systems that control HVAC, lighting, access control, and more — are frequently overlooked.

THE OVERLOOKED RISK: OPERATIONAL TECHNOLOGY (OT)

OT systems are essential to the daily functioning of educational facilities. They manage everything from classroom air quality to campus security. But unlike IT systems, OT may be characterized by legacy hardware, outdated security protocols, and limited monitoring. This makes it a prime target for attackers seeking to move laterally across networks or disrupt physical operations.

Honeywell's cybersecurity assessments frequently reveal unsegmented networks, outdated configurations, and unmanaged devices in educational environments. These vulnerabilities can allow attackers to bypass traditional defenses and gain access to critical systems — often without detection.

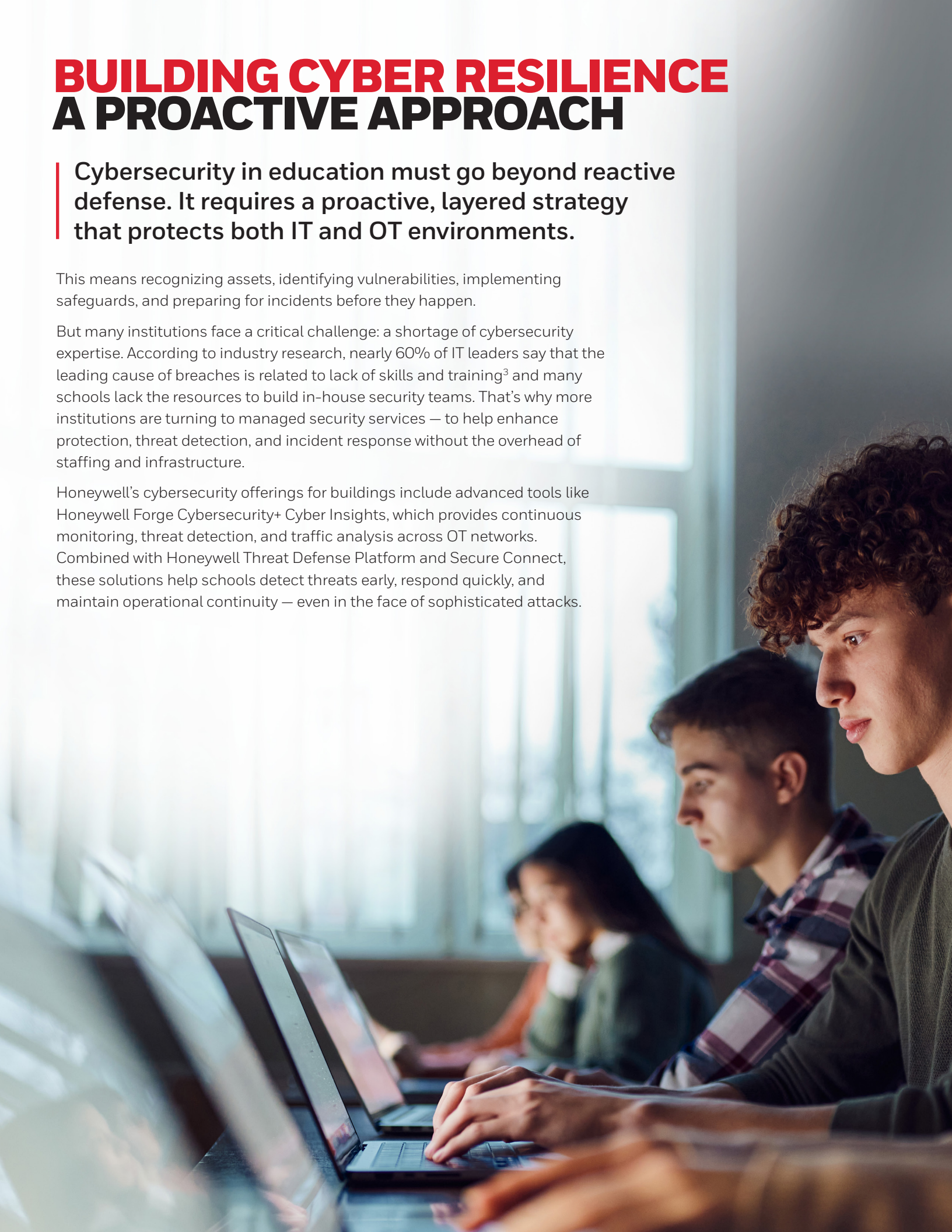
BUILDING CYBER RESILIENCE
A PROACTIVE APPROACH

Cybersecurity in education must go beyond reactive defense. It requires a proactive, layered strategy that protects both IT and OT environments.

This means recognizing assets, identifying vulnerabilities, implementing safeguards, and preparing for incidents before they happen.

But many institutions face a critical challenge: a shortage of cybersecurity expertise. According to industry research, nearly 60% of IT leaders say that the leading cause of breaches is related to lack of skills and training[3] and many schools lack the resources to build in-house security teams. That's why more institutions are turning to managed security services — to help enhance protection, threat detection, and incident response without the overhead of staffing and infrastructure.

Honeywell's cybersecurity offerings for buildings include advanced tools like Honeywell Forge Cybersecurity+ Cyber Insights, which provides continuous monitoring, threat detection, and traffic analysis across OT networks. Combined with Honeywell Threat Defense Platform and Secure Connect, these solutions help schools detect threats early, respond quickly, and maintain operational continuity — even in the face of sophisticated attacks.



HONEYWELL: YOUR PARTNER IN CYBERSECURITY FOR EDUCATION

Honeywell brings decades of experience in building systems and cybersecurity.

We understand the unique challenges of educational environments and offer a comprehensive suite of solutions tailored to schools, districts, and universities. Our approach is grounded in the NIST Cybersecurity Framework and spans the full cybersecurity lifecycle:

IDENTIFY

Every cybersecurity journey begins with visibility. Honeywell offers two levels of cybersecurity assessments — Essential and Enhanced — to help institutions understand their current risk posture. These assessments include on-site evaluations, vulnerability scans, compliance mapping (including NIST, ISO 27001, and ISA/IEC 62443), and detailed reports with prioritized recommendations. Whether you're a small district or a large university system, we help you identify gaps and build a roadmap for improvement.

PROTECT

Once vulnerabilities are identified, we help you implement targeted protections. This includes secure configuration and design of OT systems, endpoint protection through Honeywell Advanced Endpoint Security (HAES), application whitelisting, and Secure Media Exchange (SMX) to prevent USB-borne threats. These solutions are designed to harden your environment without disrupting daily operations.

DETECT

Detection is critical — and speed matters. Cyber Insights offers continuous monitoring of the OT network. Our deep packet inspection parses the OT network protocols to identify all of the assets connected to it, the vulnerabilities associated with those assets, and alerts on any malicious and anomalous user activities and device communications. Additionally, Honeywell's Threat Defense Platform (HTDP) uses deception technology to detect both known and zero-day threats. By deploying realistic decoy assets across your network, HTDP lures attackers into revealing themselves. This autonomous system provides deep visibility into attacker behavior.

RESPOND

When an incident occurs, every second counts. Honeywell helps you prepare with incident readiness planning, tabletop exercises, and stakeholder mapping. If a breach does happen, Honeywell's Threat Defense Platform provides deception-based threat detection and containment, while Secure Connect enables secure remote access and rapid response workflows. These tools help minimize damage and restore operations quickly.

RECOVER

Recovery is about more than restoring systems — it's about building resilience. Honeywell works with you to develop disaster recovery plans that align with your operational needs, recovery time objectives, and compliance requirements. We help you bounce back stronger, supported by Cyber Insights and our comprehensive assessment services that inform future defenses.

LET'S SECURE THE FUTURE OF LEARNING TOGETHER

Honeywell can offer the following in your next project:

- Deep expertise in both IT and OT cybersecurity
- Scalable solutions for schools, districts, and universities
- Vendor-neutral services that integrate with your existing infrastructure
- Award-winning technologies like HTDP and HAES
- Global support with local presence

Cybersecurity is essential to protecting students, staff, and the integrity of your institution. Whether you're modernizing a single campus, or securing an entire district, Honeywell is here to help you navigate the journey — with trusted solutions, expert guidance, and a commitment to education.

1. **Higher Ed Dive, Ransomware attacks in education jump 23% year over year, July 25, 2025 [Accessed August 20, 2025]**
https://www.highereddive.com/news/ransomware-attacks-education-jump-23-percent-h1-2025/754011/
2. **K-12 Dive, 82% of K-12 schools recently experienced a cyber incident, March 10, 2025 [Accessed August 20, 2025]**
https://www.k12dive.com/news/k-12-schools-experienced-cyber-incident-cis/741915/
3. **Fortinet Training Institute, 2024 Cybersecurity Skills Gap Global Research Report, June 20, 2024 [Accessed August 20, 2025]**
https://www.fortinet.com/content/dam/fortinet/assets/reports/2024-cybersecurity-skills-gap-report.pdf

Building Automation
715 Peachtree St NE
Atlanta,
Georgia 30308
www.honeywell.com

5403500-Cybersecurity in Education | 08/25

Honeywell