CHRONICLE STUDIO | Google for Education

Safeguarding the Connected Campus: Supporting a Culture of Cybersecurity in Higher Ed

Shifts in higher ed, from hybrid and remote learning to increased usage of institutional data, is increasing the need for more secure systems.

Ransomware remains a big digital security threat to higher-education institutions.

Two-thirds of higher-ed institutions reported an attack last year. Each incident can cost upwards of $1 million to remedy, placing additional financial strain on already tight budgets.

However, ransomware isn't the only threat. Every day, researchers, administrators, and faculty face sophisticated phishing attacks. Meanwhile, data breaches put sensitive student information and valuable intellectual property at risk. And the Internet of Things (IoT) — which includes hardware like smart watches, home automation tools, and smart locks — introduces new vulnerabilities every day.

The rapid shift to remote and hybrid learning has further expanded the opportunities for bad actors, because more people are accessing sensitive information from off-campus or using their personal devices. This makes institutions more vulnerable than ever.

> "So the question becomes: From an OS level, software and hardware level, how can we create multiple levels of security that attackers can't get through."
>
> **Steven Butschi,**
> Google for Education, Director

To thwart these threats, institutions need a multilayered security approach that encompasses every level and every system, from the cloud and operating systems to the software and hardware of users. This approach should include robust endpoint management to secure and control all devices connecting to the network. It's a complex challenge that requires both technology and a culture of security awareness and robust policies.

Building a Robust Security Framework

Traditionally, IT administrators treated their infrastructure like castles. They protected their network with a moat and fortifications to keep attackers at bay, but assumed anything within the castle walls was safe.

Today's threats exist in a more complex environment. That means institutions need better solutions than just a binary "inside safe, outside unsafe" rationale.

As campuses become more digital and learning environments become more distributed, the line between "inside" and "outside" the network has blurred. Students access course materials on their smartphones, researchers collaborate over the cloud, staff work remotely — data is constantly on the move.

Use Zero Trust

In this fluid environment, IT departments have adopted a more flexible, adaptive security philosophy. Today, the most secure environments rely on a method called "Zero Trust".

Under a Zero Trust approach, all network traffic is assumed to be a threat. That means every user, device, and access request is scrutinized and verified using tools like multi-factor authentication.

Understanding Zero Trust Security

Zero Trust is a security model that assumes no user, device, or network should be automatically trusted. Key principles include:

- **Verify Always**: Every access request is authenticated and authorized, regardless of where it originates.
- **Least Privilege Access**: Users are given the minimum permissions necessary to perform their tasks.
- **Assume Breach**: The network operates as if it's already compromised, continuously validating security at every point.
- **Micro-segmentation**: The network is divided into small zones to contain breaches and limit an attacker's movement.

Administrators operate under the principle of least privilege, which means they give users the minimum access and permissions necessary to do their job effectively. They also segment the network to limit the impact of a security breach.

Embrace Proven Tech

To stay ahead of cyber threats, institutions should embrace cloud-first and cloud-native solutions like Google Workspace and secure operating systems like ChromeOS. Best practices like regular assessments, incident response planning, and continuous monitoring form the backbone of a proactive security strategy.

Advanced features such as Context-Aware Access (CAA) and Google Drive trust rules further enhance security.

CAA allows administrators to create granular access control policies based on attributes like user identity, location, device security status, and IP address. Meanwhile, Drive trust rules provide precise control over file sharing within and outside the organization, helping secure sensitive information and maintain compliance.

In practice it looks like this: A user logging in on a personal device that is behind on software updates in a foreign county, may only be able to access a subset of core applications. Compare this to a user logging in on a device provided by the educational institution that is up-to-date on all OS releases having access to all applications.

University of Arkansas at Little Rock

Identifying and Preventing Cyber Threats

- Detecting threats across a vast college network is complex
- Investigating cases is a slow, manual process that mismatches the speed at which cybersecurity issues escalate
- UA-Little Rock leans on Investigation Tool to detect triage, and remediate threats

Thwart Sophisticated Attacks With AI

AI and machine learning are making threat detection more thorough and response times faster, while cloud security tools are helping to manage increasingly complex digital environments.

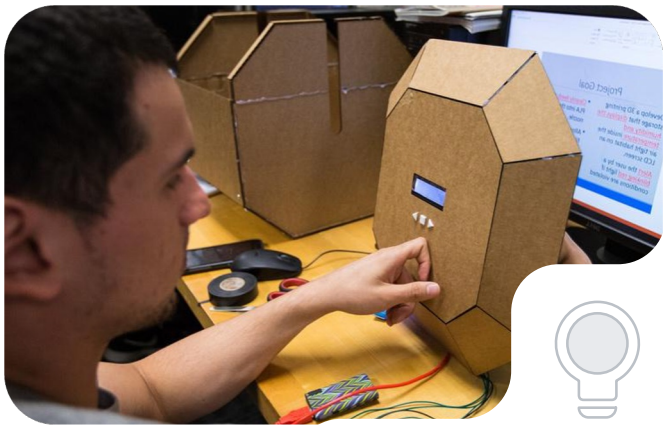
As an example, Johnnie W. Adams, Systems Administrator for the University of Arkansas at Little Rock, said he uses Google Workspace for Education's Investigation Tool daily to detect, triage, and remediate security threats across Workspace.

He offered one scenario where an email impersonated the school's chancellor to try and trick the recipient. As soon as Adams learned about the spoofing attack, he turned to the Investigation Tool.

Higher Ed's Unique Challenge: Protecting Sensitive Data

Higher-education institutions must safeguard vast amounts of sensitive data while maintaining an open, collaborative environment. This balancing act requires specific strategies and tools.

Student privacy is governed by strict regulations like FERPA (Family Educational Rights and Privacy Act).



To comply, institutions must implement access controls, encrypt data, conduct regular audits and provide staff training on best practices for data handling.

Other categories of data, like research information, also need protection. This can take the form of secure file sharing, data loss prevention systems and granular access policies.

Beyond tools, institutions should adopt a comprehensive data governance strategy.

Once an institution knows what data it has, institutions need to set policy on how that data is stored, shared, and used. IT teams must conduct regular risk assessments to identify and address security vulnerabilities, then create a plan to respond to data breaches.

> "[The Investigation Tool] allows me to investigate what's going on. I find out what's happening. Once I find out what's happening, I can then report on it. And then, of course, you can take action with it directly in the tool. I no longer shudder when I get complaints like spam emails."
>
> **Johnnie W. Adams,**
> University of Arkansas at Little Rock, Systems Administrator

Proper data governance without compromising on open collaboration involves policy measures, monitoring, and mitigation.

Effective policy measures include setting target audiences to control who can access specific information within an organization and implementing data loss prevention tied to data classification features like Google Drive Labels.

Once those measures are in place, institutions must monitor their systems. Tools like the Alert Center and Security Center make this job easier by offering real-time security notifications and providing comprehensive threat detection. IT teams can dive into BigQuery logs for in-depth analysis and conduct regular audits of their data.

To mitigate threats, colleges and universities need a blend of browser-level security controls, like those offered by Chrome Browser Cloud Management, and they need rules in place around compliance and data protection.

Accounting for the Human Factor in Security

User education is the frontline defense against many cyber threats. A well-informed campus community can recognize and respond to potential security risks, effectively turning every user into a human firewall.

Effective higher-ed IT departments use a mix of online training and frequent written updates to keep users informed on best practices for digital security. "To help with user education, we've created security best practices to teach people how to keep safe online, and we've built notifications and alerts into our products too," Butschi said.

He points to advanced security features, like the Gmail Security Sandbox. This tool scans email attachments in a virtual environment, helping to identify malicious software traditional antivirus tools might miss.

Implementing email authentication best practices — such as Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication Reporting and Conformance (DMARC) protocols — helps prevent email spoofing and phishing attempts, further safeguarding institutions from email-based threats.

An often overlooked vulnerability unique to higher education is that universities and colleges tend to treat student accounts differently.

Many universities apply less-stringent security measures to student accounts, such as weaker or no multi-factor authentication (MFA) enforcement. This disparity can result in increased threats to the institution as a whole, as compromised student accounts can serve as entry points for broader attacks.

That makes frequent, thorough workshops on best practices for security even more important, according to Adams.

He says institutions can't promote user education enough because there's always someone out there trying a new technique to get around all of your protections.

Staying Ahead in Campus Cybersecurity

Continuous vigilance and adopting Zero Trust principles should drive higher-ed cybersecurity policies

Universities and colleges still operate best when they are places of openness, accessibility, and collaboration.

But that means it's even more critical to continue to adopt and implement Zero Trust principles, using features built into Google Workspace for Education, such as Target Audiences, Trust Rules, and Context-Aware Access.

To that end, institutions must continue engaging with their peers at other institutions and gather insights from private industry security experts to refine their internal best practices.

A single breach can compromise years of research, tarnish an institution's reputation, and betray the trust of thousands of students and staff. But with proactive measures and a commitment to continuous improvement, higher education can defend against threats and lead the way in innovative cybersecurity practices.

"We've managed to do a pretty good job of educating our users on avoiding phishing, avoiding social engineering. Those soft skills are so important when it comes to knowing not to respond to something, to be able to use a little bit of judgment and say, 'this doesn't look good."

Johnnie W. Adams,
University of Arkansas at Little Rock,
Systems Administrator

University of Arkansas at Little Rock

Key Takeaways

- Detecting threats across a vast college network is complex
- Investigating cases is a slow, manual process that mismatches the speed at which cybersecurity issues escalate
- UA-Little Rock leans on Investigation Tool to detect triage, and remediate threats

Learn How Google Workspace for Education Can Keep Your Campus Safe