
TitanHQ
Defending Higher Education from Common Cyber-Attacks

Defending Higher Education from Common Cyber-Attacks

Cyber-criminals aren't looking for a challenge. They want targets with insufficient cybersecurity allowing them access to valuable data. Educational institutions struggle to keep up with the latest threats, and universities contain valuable information for students, teachers, and administration. In the UK, over 87% of universities suffered from a successful data breach according to a recent VMWare report. With the rise in cyber-attackers targeting universities, it's clear that they need to review current cybersecurity infrastructure and find much more effective ways to stop threats.

Research Data, Student Information, and Professor Material are Also Targets

As with any financially motivated attack, personally identifiable information (PII) is valuable information attackers want to sell on darknet markets. Financial data is also valuable, especially validated credit cards linked to the owner's PII. Currently, a validated credit card number and PII with a $5000 balance is worth $120 on darknet markets.

This value is just one card, so imagine stealing 1000 records, and your payout would be up to $120,000. Most databases store many more records, so cyber-criminals can earn millions from one data breach.

Universities have valuable personal and financial data, but they also store intellectual property (IP) from researchers that could be worth millions to a competitor, pharmaceutical company, or healthcare organization. Other valuable data includes graduate dissertations, professor lecture material, exam results, and student credentials. With the right sophisticated threat, an attacker could earn much more in one data breach compared to a breach with a standard enterprise organization.

Universities Have an "Open Door" Policy Leaving Them Vulnerable

Traditionally, universities are much more open about their environment than a standard enterprise organization. You can walk into a university campus with few restrictions and gaining access to their registrar functions requires little information. You don't need to authenticate into a university site to see class schedules, professors, and course materials. This open-door policy goes against the common cybersecurity mantra that users should have access to only the data necessary to perform a function. The "principle of least privilege" is combined with zero-trust architecture (ZTA) to lower risk and protect sensitive data.

What Can Be Done to Help Universities Against Cyber-Threats?

Universities and administrators responsible for safeguarding data must strike a balance between openly giving access to research data and course information and protecting infrastructure from unauthorized access. Administrators can still leave an opening, welcome environment for learning across all age groups and the internet, but they must implement cybersecurity architecture, policies, and training necessary for data protection.

Cybersecurity Training

Everyone from executives to professors and administrators should understand the anatomy of a cybersecurity attack, especially phishing and social engineering. Most attacks start with phishing and end with ransomware, malware, and data theft. Everyone within the university should be trained to recognize an attack

.

An added extra is training students to understand the consequences of phishing to protect their data as well. Stealing student credentials is a valuable threat to their data. With student credentials, an attacker can access their social security number, exam scores, schedules, financial data used to pay for services, and their home contact information.

Apply Business Strategies to University Cybersecurity Policies

In an open-door environment, it's difficult for administrators to enforce business-level policies used to keep data safeguarded. Business cybersecurity strategies aren't perfect and don't reduce risks entirely, but they do reduce risks significantly. Most universities must follow at least one regulatory framework, so any cybersecurity policies must be compliant. Always verify cybersecurity policies follow the latest regulatory standards and following them will improve university defenses against threats common in the business world.

The threats used to compromise a university are like – and sometimes exactly like – the ones seen in the business world. Using business strategies will help mitigate and stop these threats, so incorporating better cybersecurity policies within standard university workflows for administrators will only improve data protection. Everyone responsible for safeguarding sensitive data should be trained to follow policies and procedures.

Universities Under Attack

43% have had student data attacked, including dissertation materials and exam results.

25% have experienced critical intellectual property theft.

28% have had grant holder research data attacked.

Consider Migrating to the Cloud

The cloud offers numerous benefits to any environment with cybersecurity is critical to business continuity. It's not a bulletproof solution to cybersecurity, but it can help reduce risk especially when the university uses legacy architecture. Any legacy architecture can be migrated to the cloud and offer better availability, integrity, and security. Administrators still must configure cloud infrastructure properly for it to safeguard data. Misconfigurations are common in data breaches in the cloud, so ensure that administrators are aware of the pitfalls. For administrators unfamiliar with cloud configurations, consult help from experts to review any configurations and train them on proper setup, deployment, provisioning, and maintenance.

Don’t Forget Email Security

Most threats begin with a simple email. It only takes one person to fall victim to a phishing attack for a successful system compromise. Containing threats after a compromise is much more difficult than stopping them before they access the environment. Training users to recognize phishing is beneficial, but human error is still a risk. Insider threats are common in universities when administrators open malicious attachments or execute malware on their system connected to the network environment.

Email security with TitanHQ SpamTitan phishing protection stops threats that begin with a malicious message. According to Deloitte, 91% of attacks start with a phishing email, so using SpamTitan eliminates most university risks including malware, ransomware, credential theft, and other threats that start with an email.

Universities Don’t Need to Be a Target

Universities must take a holistic approach to security, striking a balance to ensure critical data is adequately protected without prohibiting or impeding researchers. Many universities are falling behind in terms of IT security. It is imperative that they are adequately able to defend against cybercrime investing in the appropriate technologies as necessary. Most cybersecurity strategies don’t take a complete overhaul of an environment. They can be provisioned and deployed without much effort, making it convenient for administrators to incorporate policies. Planning is always key for effective cybersecurity, but administrators can employ several simple changes to lower risks.

Ready to maximize your ability to secure your school, college, or university and staff to cut security incidents and related costs?

Train staff and students to recognize threats but take the human element out of cybersecurity and incorporate email security from TitanHQ. SpamTitan protection works in the cloud, requires few configurations, and immediately starts protecting university email once it's deployed. It stops malware, ransomware, stolen personal data, stolen financial card details, and blocks malicious binaries from installing on university computers.

GET IN TOUCH