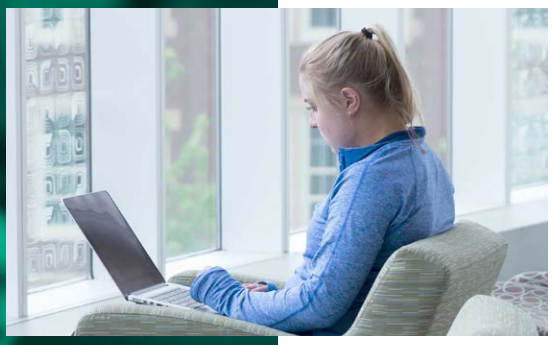
jamf

WHITE PAPER

Protecting Higher Education From Costly Data Breaches



Security breaches grab headlines and fill TV airtime

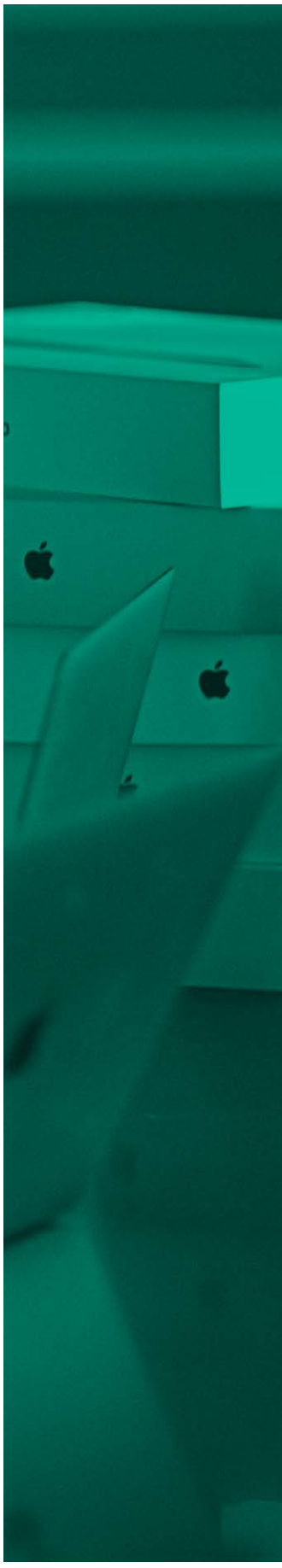
When big name retail, healthcare or financial brands suffer a breach, it's all over the covers of newspapers and the lead story on the evening news. How do news organizations know that security breaches are page-turners and must-see TV? Because everyone can relate to the fear of their Social Security number, bank accounts or other personal information being compromised or stolen. And, higher education institutions are certainly not the exception to the rule.

In higher education, students and families need to feel that their institution's reputation — often tied to their own identities or even future employment prospects — is one to be confident in and proud of. This extends beyond an institution's academics, athletics, arts or mission; data privacy and security reflects the trust and responsibility of an institution.

What is a security or data breach?
A breach is defined as an event in which an individual's sensitive, protected or confidential data is viewed, stolen or used without consent.

With large quantities of student and faculty information on hand, complicated information systems and distributed environments spread across departments, higher education institutions are subject to breaches in the same fashion and with the same magnitude as large corporations. According to a 2019 **study by the Ponemon Institute,** the average total cost of a data breach is $3.92 million, and for education institutions, the average cost is $4.77 million with average cost per lost or stolen records being upwards of $150. With this staggering amount per compromised record, the thought of even a small amount of breaches is a worst-case scenario for university presidents and department IT staffs.

To combat the threat of security breaches – and avoid the associated costs – IT departments all too often put a stronghold on what users can access and do on their devices. This amount of control can put faculty and staff at odds with IT, as users require access to apps, services and other resources to do their job. When IT is viewed as hindering an employee's productivity, the natural instinct is to go around IT and their guidelines in order to move projects forward and deliver the best learning experience to students. Without intending to, these well-meaning university employees are creating vulnerabilities in IT's security systems, simply because they're trying to get work done. Successful IT security management requires a delicate balance of user autonomy and smart IT controls.



Common types of data breaches

Although breaches come in all shapes and sizes, they can be categorized into three types: malicious or criminal attacks, system glitches and human error. In a recent study, malicious attacks accounted for 51 percent of all breaches. While not as prevalent, system glitches and human error are just as dangerous because they often go unnoticed for a lengthy period of time, allowing the problem to fester and open up more devices and data to unsafe practices. The same Ponemon study noted that it takes an average of 181 days to identify with an additional 61 days to contain a data breach caused by human error – an eternity – leaving the door open for data to be stolen.

Institutions and universities under attack

While all universities are subject to breaches, doctoral and master's institutions prove to be the most vulnerable. According to a Postal Regulatory Commission (PRC) report, 63 percent of breaches are attributed to doctoral institutions and 21 percent are attributed to master's institutions. These institutions are more susceptible because of their vast amounts of records and desirable research data.

Even with those astounding numbers for graduate institutions, bachelor and associate programs are not immune to their fair share of vulnerabilities. As several universities can attest, the result of a breach is painful, costly and time-consuming.

On July 8, 2015, Washington State University encountered suspicious activity on its systems. After reaching out to information security experts and federal law enforcement, it was determined that a sophisticated attacker had illegally accessed their email and directory systems.

Southern New Hampshire University also endured a database breach of 140,000 records of student and class information being exposed to the public. And, Arkansas State University reported that as many as 50,000 people were impacted by its data breach in 2014.additional 61 days to contain a data breach caused by human error – an eternity – leaving the door open for data to be stolen.

How data breaches enroll at universities

Malware and viruses

Malware and viruses enter a university's systems with malicious intent or by accident. Either way, once in a university's system, malware and viruses go to work deleting files and stealing passwords, bank accounts and other sensitive information.can target devices that need to be updated, reconfigured or patched to improve their security posture. This is all done remotely and can be automated without IT physically touching the device.

Unsafe software and apps

Similar to malware and viruses, unsafe software and apps that are downloaded onto systems or devices open the floodgates for personal information to be shared with the world or cause hardware to completely shut down.

Personal services downloads

Most, if not all, faculty and staff at a university utilize personal email accounts and services such as Dropbox on their devices. While Dropbox in itself is not a harmful service, when personal services are downloaded and used outside of a university's scope, these seemingly safe services can be a vessel for data breaches. Unprotected services are subject to attack and often go unnoticed because IT is unaware that these services are being run on institutionally owned hardware.

Unsafe network practices

With today's workforce as mobile as ever, it's very common for faculty and staff to connect to their university's network from home or a coffee shop. If users are not utilizing the university's secure virtual private network (VPN), they can inadvertently leave the network vulnerable to attack.

Unencrypted devices

Faculty and staff are not immune to mistakes and can forget their device or a USB stick on or off campus. When devices are lost—or stolen—they are prime targets for data breaches.

In the face of these five security vulnerabilities, it's tempting to respond by simply locking down access and restricting unknown software. But, as we know, this course of action may have unintended consequences.

Working with faculty and staff To remain secure

In order to provide the best experience for users, while also ensuring their work and exploration doesn't punch holes in the university's security armor, IT should follow these guidelines to keep their users and institutions safe from data breaches.

Make endpoint protection standard to alleviate malware and viruses

There's no perfect defense against malware and viruses, but a good endpoint protection system can greatly decrease the risk of infection and provide IT with the tools needed to respond to a security breach. Choose the right mix of technology to both detect and monitor network traffic — at the device level — for suspicious activity. To maximize coverage, consider making endpoint protection for all devices —whether institutionally owned or personally owned. This task is greatly simplified with a mobile device management (MDM) tool that can install software on a managed device.

Make trusted software and apps available on demand

IT can create an internal app catalog where they offer university-approved software and settings for faculty and staff to download at their leisure. Only tested and approved apps are available and users never have to circumvent IT because they have easy access to the resources they need. If a faculty member requires an app that is not available in the self-service style catalog, they simply submit a request to IT and upon vetting and configuring the app to university standards, IT places the item in the catalog where users can download it on their own.

Know the status of devices and software

With MDM inventory features, IT can view which apps are being used and proactively test popular apps accordingly. If an app ever falls under suspicion, IT can see who has the app and immediately update or remove it – protecting the device while also preventing the "untrusted" software from spreading harm throughout the university's system.

What is MDM?

MDM is Apple's framework for managing devices. From deploying new hardware and gathering inventory, to configuring settings, managing apps or wiping data, MDM provides a complete toolset to address large-scale deployments and ensure device security.

Make IT services equivalent to personal services

If IT services are as good as what a user has access to outside of work, there is no need for them to go rogue and rely on their personal services. IT should utilize the services that users are most comfortable and productive with, and make them the standard. Email, backup, file sharing and collaborative services are all available in the cloud so the user can work in one, centralized environment whether at home or on campus. Once services are identified, managing them is the best way to mitigate risk and ensure security policies remain intact.

Make VPN readily available for secure network practices

Working with your cloud service provider, you can make it easy for users to utilize VPN. You can even go beyond simple password authentication and implement certificate-based Wi-Fi authentication to ensure only the devices you want can access the network. Instead of requiring users to type in passwords to access VPN, which could hinder users from utilizing the secure network, you can leverage your MDM tool to send them a certificate when they enroll in the management solution. This way, they use their secure certificate to access the network without any hassle.

Make data encryption mandatory

Universities can enforce encryption requirements and easily report on compliance across the entire institution. By leveraging built-in encryption technology, user devices won't take a performance hit from a third-party security addition, and IT can manage all recovery keys so they can quickly address password resets, device activation lock bypass, and remote lock and wipe.

Conclusion

With security practices that focus on the user and an MDM solution in place, IT has the tools to prevent hacks and malicious software from reaching university systems and faculty devices, while also delivering a great experience for users. IT is all too often a thankless job, but by following these guidelines, universities and their IT staffs can start down a path of being noticed for the right reasons and keeping their names out of the press for the wrong.

Request a Jamf trial today and take a monumental step into better protecting your institution.

Request Trial

Or contact your preferred reseller of Apple.