CLOUD SECURITY IN HIGHER EDUCATION

The Cloud Revolution Is Here. Is Your Campus Secure?

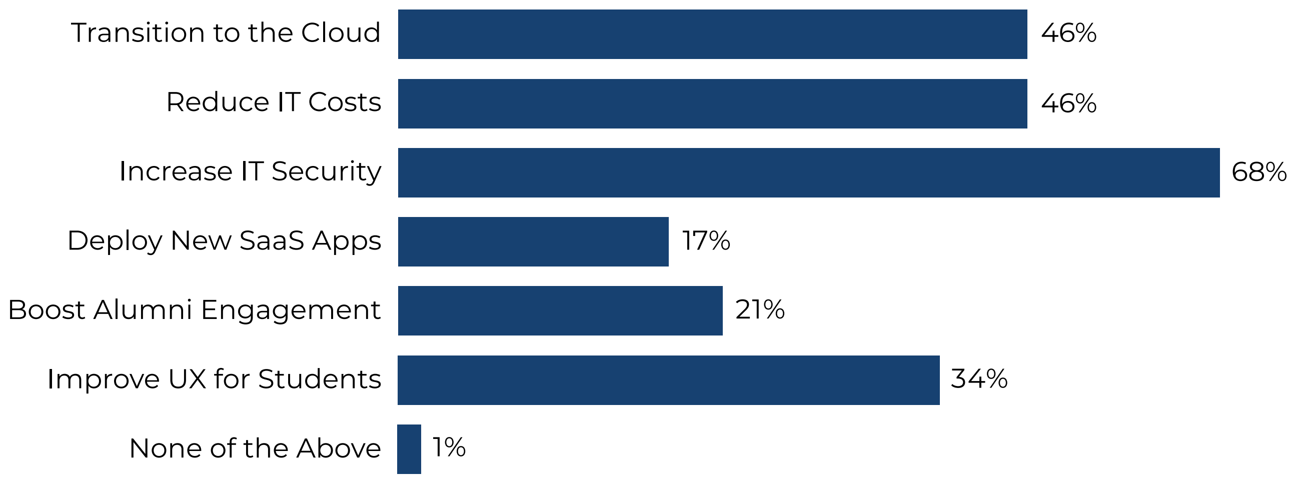
Managed Methods

Cloud applications such as Google G Suite, Office 365, Canvas, and Workday have become ubiquitous in higher education institutions. Digital native students and staff alike expect flexibility in access and collaboration. Meeting these demands requires cloud-based solutions that stretch the limits of campus information technology and security systems.

IT leaders and staff are challenged to meet user demands while building systems that are compliant with government regulations, such as FERPA. Cloud security is now a top concern among higher education CISOs, who report challenges in user behavior, lack of time and staff, and lack of security awareness training.

In this eBook, you'll explore the current trends that require higher education IT teams to invest in cloud security, and the solutions to help you do so.

Top Priorities for Higher Education IT Teams In The Next 12 Months



(GRAPH SOURCE: OKTA)

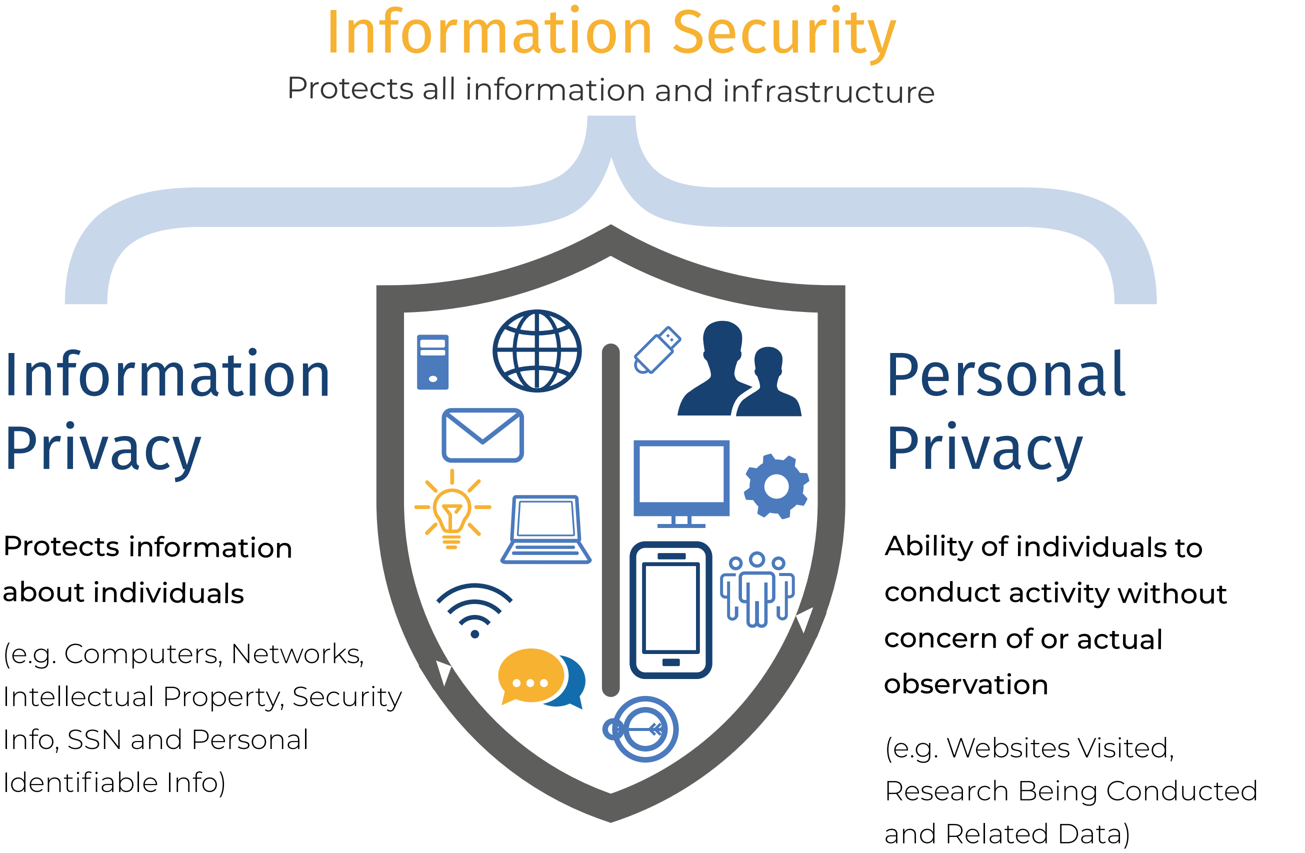
Why Higher Education Needs Cloud Security

Information security lies at the intersection between personal privacy and information privacy. Students have a right to both types of privacy, and information security plays a critical role in maintaining those rights.

Colleges and universities collect a massive amount of personally identifiable information, financial, and health information. Cyber criminals target this data to profit from sales on the dark web.

Higer education institutions also need to protect their information infrastructure, intellectual property, campus security information, and more.

For these reasons, colleges and universities are increasingly investing in information security and privacy training and hiring. Information security professionals are charged with managing the infrastructure and processes that keep schools compliant and people safe.



Information Security

Protects all information and infrastructure

Information Privacy

Protects information about individuals

(e.g. Computers, Networks, Intellectual Property, Security Info, SSN and Personal Identifiable Info)

Personal Privacy

Ability of individuals to conduct activity without concern of or actual observation

(e.g. Websites Visited, Research Being Conducted and Related Data)

Cyber Criminals Targeting Higher Education Institutions

Colleges and universities are increasingly becoming targets of cyber attacks due to the type and amount of data that can be obtained. Combined with relatively new cloud security infrastructures that lack the sophistication of companies of similar sizes, for cyber criminals the risk is low and the rewards are high.

EDUCAUSE research reports that information security is a top issue for IT departments in higher education. As school demographics shift to digital native students and faculty, expectations for easy accessibility challenges traditional data security infrastructure.

The proof is in the data. Lost, stolen, or compromised data records increased in higher education by 103% in the first six months of 2017 compared to the last half of 2016. There were a reported 118 successful cyber attacks on higher education institutions, representing 13% of all breaches that took place in the first half of 2017.

> **We need not to think, 'Will a data breach happen at my institution?' But 'When will it happen and how will I be prepared?'"**
>
> **– Susan Grajek**
>
> Vice President for Communities & Research
>
> EDUCAUSE

The Rising Cost of Data Breaches in Education

The financial impact of security breaches on higher education is measured in the millions of dollars. Ponemon Institute reports that the average total cost of a data breach increased by 6.4% in 2018 and that the average number of records stolen increased by 2.2%. In 2018, the average total cost of a single data breach for an organization across all industry sectors topped $7 million.

For higher education institutions, those costs don't take into consideration the costs and long-term damage that student identity theft due to data breaches inflict. Students, in particular, are usually just beginning to build their financial futures. Identity theft has lasting impacts, which can include the delay or cancellation of student loans, credit score downgrade, time invested in remediation rather than studies, and psychological and emotional stress

$7M

Average cost of
a data breach

28K

Average number of
breached records

$200

Average cost per
record breached

56%

Data breaches caused
by 3rd party vendors

(DATA SOURCE: EDUCAUSE)

Government Regulations Impacting Higher Education Data Security

There are several federal regulations covering student privacy and information security that higher education institutions must comply with. Until recently, state laws either relied on or mostly mirrored these federal laws. This is beginning to change as information security and privacy are becoming more important issues in the digital age.

Federal Regulations

Family Educational Rights and Privacy Act (FERPA)

FERPA is designed to protect the educational records of students, both in K - 12 and higher education. It requires universities to obtain students' written consent before releasing their personal records, and only allows records to be released for specific purposes.

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA establishes national standards to protect individual health information. It requires that the appropriate safeguards are put in place to protect personal health information, and sets conditions on the uses of health information. HIPAA also outlines notification requirements to individuals and others when a security breach does occur.

Health Information Technology for Economic and Clinical Health (HITECH)

HITECH was passed in anticipation of an expansion in electronic medical record storage and sharing. It broadens the scope of health information privacy protections created under HIPAA and increases the potential legal liability and enforcement criteria for non-compliance.

Government Regulations Impacting Higher Education Data Security

Children's Online Privacy Protection Act of 1998 (COPPA)

COPPA defines a child as anyone under 13 and has a greater impact on K - 12 schools. However, colleges and universities that offer events and programs for children must comply with COPPA regulations. COPPA broadly regulates the collection, use, and protection of both personally identifiable and non-personally identifiable information collected.

Federal Information Security Management Act (FISMA)

The intent of FISMA is to maintain the security and resiliency of federal information and information infrastructure. Universities that operate as a federal contractor, often through federally-funded research grants, are impacted by FISMA. FISMA requires that institutions institute information security programs and policies and periodically audit assets, assess risk, and review policies.

Gramm Leach Bliley Act (GLBA)

GLBA covers the collection, disclosure, and protection of personal and personally identifiable information that is collect and stored by a financial institution, such as higher education institutions that offer loans and financial aid to students.

Electronic Communications Privacy Act (ECPA)

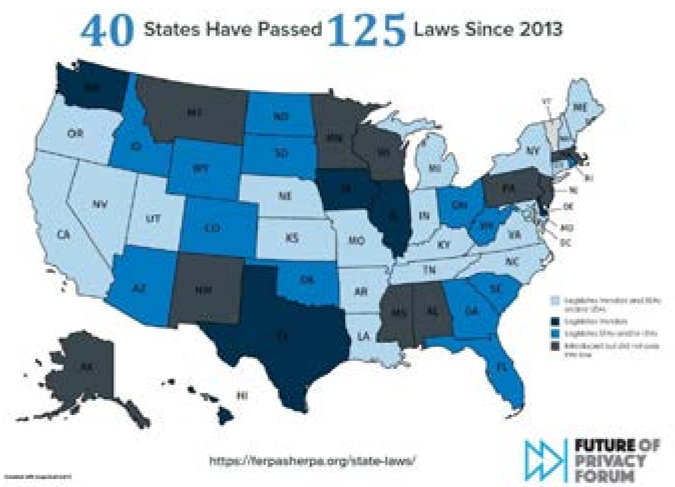
The ECPA is primarily designed to prevent unauthorized government access to an individual's private data. It restricts access to personal email, telephone conversations, and data stored electronically. Passed in 1986, this law was forward-thinking for its time but has not aged well. This is quickly becoming apparent as both institutional and personal data is increasingly stored in the cloud, and has become the centerpiece of ongoing lawsuits and litigation. There is also a push to update the laws protecting private data from government access, so expect to see more on this in the coming years.

Government Regulations Impacting Higher Education Data Security

For colleges and universities, it is important to know your role in the difficult balance between protecting student and staff right to privacy and coordinating investigations with the proper authorities under ECPA. With more and more data being stored in the cloud on college campuses, coupled with social volatility many campuses are experiencing, this regulation is highly likely to become an issue for campus administrators and IT staff.

There are additional regulations that higher education institutions need to comply with, mainly focusing on the sharing and storage of health information, such as the Americans with Disabilities Act (ADA), and financial information, such as the Fair and Accurate Credit Transaction Act (FACTA). This list is not meant to be comprehensive or to provide legal advice. It is merely meant to inform and provide context for higher education IT administrators and staff. For additional information and resources, visit the Higher Education Compliance Alliance.

State Regulations



CLICK IMAGE TO ENLARGE

As mentioned previously, states are increasingly jumping into the business of regulating student privacy regulations.

There are a variety of regulations at state and local levels and we're not going to get into each of them here. According to FERPA Sherpa, the number of state laws regulating student privacy has dramatically increased since 2014. Two main regulations that have been adopted in whole or in part by many states include SOPIPA and SUPER. Both mainly regulate companies that create tech products for K - 12 students and their use of student information.

The laws prohibit companies from sharing student data and using it for targeted advertising for non-educational purposes. They also require companies to delete student data if requested to do so by the school or district. The laws are targeted toward edtech software, such as Google for Education and Learning Management Systems (LMS), and do not apply to general audience websites, products, and services such as Google Search.

General Data Protection Regulation (GDPR)

GDPR made a big splash in the months preceding its launch in the spring of 2018. However, the broad scope and far reach of GDPR has been overlooked by many in higher education administrations. This new European regulation claims the power to discipline any company or organization that collects data from European Union (EU) citizens, even if the organization is located in a non-EU country. Higher education institutions that accept student applications, collect alumni donations, or communicate with faculty on sabbatical in the EU are subject to GDPR.

Despite all the hype, colleges and universities are unlikely targets for GDPR regulators—at least in the near term. Most agree that EU regulators will focus on cracking down on very large, global organizations and bad actors. Further, the true reach of GDPR is yet to be fully tested. Nevertheless, IT leaders should be aware that their institutions are, technically, required to comply with data management regulations outlined in GDPR and could face hefty fines to the tune of millions of dollars.

The Revolution: Cloud Adoption in Higher Education

Like many organizations, colleges and universities are moving to the cloud to reduce the costs of storing data, improve productivity, and enable collaboration.

Approximately 70% of higher education institutions have transitioned to cloud-based email platforms, while 50% are adopting cloud collaboration solutions. Furthermore, according to a recent survey, 39% of higher education apps run in the cloud today, and that number is expected to increase to 62% by 2021.

This trend provides many benefits to institutions, staff, and students. Cloud-based solutions cost significantly less, particularly when taking ongoing maintenance and updates into account. They also help keep higher education agile in adjusting to changing needs and opportunities, while also effectively preparing students for life in the commercial world where cloud computing is the norm.

Risks and Rewards of Cloud Computing in Higher Education

Higher education has unique needs and responsibilities that businesses do not, which is impacting adoption rates. Colleges and universities need to foster openness and collaboration in dispersed locations across broad stakeholder groups while maintaining a high level of control and monitoring to comply with strict regulations.

IT teams also grapple with the responsibilities of allowing students to bring their own devices into the institution’s cloud environment. Students expect to be able to access information pertaining to classes and events anywhere, anytime, on any device. This raises unique challenges from a usability and accessibility standpoint, as well as a data security standpoint. The more endpoints that are brought into the campus cloud environment, the more vulnerable that environment is to malicious breaches.

The Revolution: Cloud Adoption in Higher Education

The good news is that cloud applications, such as Google G Suite and Microsoft Office 365, have the infrastructure in place to help colleges and universities provide scalable capacity and accessibility.

But when an IT team is dealing with thousands of users, and tens of thousands of endpoints, their ability to monitor and control accessibility is untenable.

This is where administration and IT leadership have the greatest opportunity to do more with the staff they have to make cloud accessibility and collaboration secure for everyone.

> "People think when you move something to the cloud that all of a sudden you don't have to be concerned about it and that's a fallacy."
>
> **– Sean P. Connolly**
>
> Director of IT, The George Washington University
>
> Speaking at EDUCAUSE

The Solution: Cloud Application Security

Cloud application security solutions use APIs native to cloud applications to track access, monitor, and report on activity going on within the app. This means that IT staff are gaining critical visibility, control, and protection of the institution's cloud environment and the data stored within them, without the need for gateways or proxies.

When moving away from private servers, IT staff find that they lost the visibility and control they require to keep their organization's environment secure. The cloud environment that looked so cost-effective before now requires up to three times more to upgrade to an enterprise level and access just some of the controls they were used to. This is where cloud application security comes in to help fill the gap with a more simple, cost effective solution that makes IT security administrators' lives easier.

At ManagedMethods, we're on a mission to enable the cloud revolution with simple, affordable cloud security. IT teams in higher education institutions have a lot to deal with. Our aim is to make securing the cloud environment a lot easier.

Data Loss Prevention

Data leaks happen from many sources when a higher education institution is operating in the cloud. Without proper data security, sensitive information such as student and staff Personally Identifiable Information (PII), Personal Health Information (PHI), Personal Financial Information (PFI), as well as institutional insider information is at risk.

The good news is that breach activity is fairly easy to detect when the right systems are in place. Suspicious activity includes triggers like logins from abnormal geographic areas and IP addresses, massive downloads of data, sharing of files with unknown domains and/or geographies, and more.

The Solution: Cloud Application Security

A cloud application security solution is built to recognize and pinpoint these activities among the thousands, or even millions, of events happening in a cloud environment. Using ManagedMethods, an IT administrator can set up rules to automatically quarantine sensitive files and notify the proper personnel of a potential threat.

Cloud Application Security Data Loss Prevention Overview

- Gain insight into data access and usage across cloud apps, pinpointing high-risk behavior from both internal and external threats
- Detect and remedy data exposure and documents containing sensitive using custom rules and policies
- Identify noncompliant third-party applications that have authenticated access to your domain, then automatically govern usage and ensure compliance

Threat Protection

Millions of malicious cyber attacks are launched into email inboxes and file sharing drives every day. These attacks include worms, viruses, phishing, spoofing, malware, ransomware... the list goes on. Whether an organization uses cloud applications, on-site servers, or a combination of the two, information systems are under constant attack.

With a -cloud application security solution cloud access security broker in place, IT teams gain the upper hand over criminals. ManagedMethods will automatically scans both emails and shared drive files for malware threats. It also The system scans file content and links when they are uploaded into the environment, as well as email senders, subject lines, attachments, and body content. All without delaying the user experience due to the use of a gateway or proxy.

The Solution: Cloud Application Security

IT administrators can also set up custom policies that will prompt the system to quarantine, analyze, and delete emails and files if necessary, before they are unleashed in the cloud environment.

Cloud Application Security Threat Protection Overview

- Notification of emails sent and received, files uploaded, shared, and downloaded
- Analysis of both cloud-based email and file sharing environments
- Scan and alert for malware, phishing, and data loss prevention risks
- Quarantine and/or delete an email if a threat exists

Visibility and Reporting

No cloud application security solution is complete without the ability to provide system administrators with the visibility and control they need to keep the cloud environment secure. The CASB must provide the ability to audit accounts, activity, and emails and files in the cloud environment, and produce usable reports on those audits. And they must be able to do this quickly so that IT can focus on what matters—keeping systems running and secure.

Auditing a campus cloud environment includes analyzing user access and files in the account. It should be done on a regular basis—automatically—to provide the team with crucial visibility. The system is then able to provide a report on active and inactive accounts, uncover malicious files, and flag files with sensitive information that is being shared inappropriately. When an audit finds potential security threats, the system can quarantine, delete, and/or notify the security team for remediation action.

Reporting allows IT leaders the ability to analyze the efficacy of the security infrastructure and measure its success. This is particularly important in higher education institutions where decisions are made on a consensus basis and results of programs (and budgets) are often carefully scrutinized. Cloud security reporting also helps campus administration detect data breaches and notify stakeholders promptly, as required by law.

With ManagedMethods, reporting is made easy with report templates and customizable reporting. IT administrators can set the types of reports they want to pull to help them best understand the nature of cloud application security in their environment, and schedule those reports to send on a periodic basis.

Cloud Application Security Audit and Reporting Overview

- Analyze user access and files enabled in campus accounts
- Uncover malicious and potentially threatening files
- Flag files containing sensitive information that is not in compliance with sharing policies
- Customize and schedule frequent reporting on data and insights that matter most to your institution

Cloud Security in Your Cybersecurity Infrastructure

Cloud security is not the silver bullet to higher education cybersecurity challenges. Rather, it is meant to be used within a layered security architecture.

IT teams need to evaluate and decide on the best course of action for their own security infrastructure. The best will take a layered approach to their security technology stack that includes levels of access, employing firewalls, gateways, and proxies with VPN access to secure the perimeter.

Cloud security fits into the cybersecurity infrastructure where IT teams need to pair open access to information and files with tight control and visibility. It secures the behavior happening within the cloud environment, and acts as an additional shield to incoming threats.

Students, faculty, and staff alike expect to be able to collaborate and share information within the virtual campus environment. To pretend like IT administrators can forbid the use of cloud applications is foolish. This simply results in the unsanctioned use of cloud applications that your security team will have zero control over. Higher education IT needs to embrace the move to the cloud and equip their security teams with the tools to make campus cloud applications accessible and secure.

Conclusion

The days of on-site server housing and maintenance at scale are largely over. While there will always be a place for on premise information technology and security infrastructure in large organizations with highly restricted information, the vast majority of the world is moving to the cloud.

IT teams and administrators in higher education institutions that resist this movement will only do greater harm to the very systems they are trying to protect.

About ManagedMethods

ManagedMethods offers the most efficient way to gain visibility into how data is stored, accessed, and shared in popular cloud applications, such as Google G Suite and Microsoft Office 365, including email. ManagedMethods is the industry's only cloud application security solution that can be deployed in minutes with no special training, and with no impact on users or networks.

Learn more at managedmethods.com.

Phone: +1 (303) 415-3640

General Questions: info@managedmethods.com

Managed
Methods

managedmethods.com
info@managedmethods.com
(303) 415-3640