A REGROUP GUIDE

# Cybersecurity in Higher Education

## Strategies to Safeguard College Campuses from Cyber Threats

Regroup Mass Notification

# How to Safeguard Community College Campuses from Cyber Threats

Community college campuses are more connected than ever. Students rely on digital platforms for a range of activities, from registration and attending classes to interacting with faculty and peers. However, this increased connectivity also presents a growing challenge for campus IT teams as they face an escalating number of complex cyber threats.

Colleges can take proactive measures to help prevent cyberattacks and mitigate the damage if it occurs. This paper explores the primary methods institutions in higher education can use to build resilience in the face of a cyberattack.

# Overview of community college cyberattacks

### College of the Desert

In July 2022, the College of the Desert had to take down its phone and online services for nearly a month due to a malware attack. After nine months of investigation, the college reported that the personal data of 800 people were affected.

### Tennessee State and Southeastern Louisiana University

Tennessee State and Southeastern Louisiana University suffered from network issues and a data breach believed to be a ransomware attack in early 2023, forcing campus networks offline.

### Michigan State University

Michigan State University was hit by two cyberattacks in 2020, causing the ransom of personal data and an attack on their online university store.

These instances underscore the escalating threat of cyberattacks in higher education institutions and the urgent need for robust cybersecurity measures.

Cyberattacks against higher education institutions are rising, yet many incidents go unreported. Specifically, colleges and universities grapple with a higher frequency of ransomware attacks due to their decentralized organizational structure and wide range of users. These users include researchers, students accessing resources off-campus, community groups, faculty and administrators.

Community colleges accumulate and store substantial data from faculty, students, staff, vendors, visitors and more. And with the widespread adoption of hybrid or fully remote classes by many schools, this data collection has grown. Because of the extensive data storage within colleges and universities, they frequently become prime targets for hackers and other cyberattacks.

Some of the most common cyberattacks colleges and universities face

- Ransomware
- Phishing
- SQL injections
- Attacks on outdated technology
- Data breaches

**These threats underscore the urgent need for comprehensive cybersecurity strategies.**

# Four key security strategies for combating cyberattacks

## 1.Form a team and hire top talent

Forming a cyber safety team is indispensable for managing the cybersecurity equation. This team can help your school identify and solve the most pressing network, infrastructure and IT issues.

The cyber safety team sets forth the policies for cybersecurity, assesses the current security measures and procedures, reexamines them annually and prepares the communication and response measures in case of an attack.

In addition, hiring cybersecurity talent is one of the most essential steps colleges can take to protect their campuses. This is especially true when it comes to hiring a security auditor. Security auditors help you stay informed of the latest trends and best practices and help implement strong password policies, encryption standards and server access controls.

Before hiring security auditors, it’s helpful to understand the role they play. You need to understand what they do and how they can help. To do this, you can examine the duties and responsibilities of a security auditor and the qualifications required to get the job done.

Forming a cyber safety team is indispensable for managing the cybersecurity equation.

# 2. Understand the threat landscape with threat intelligence

### Cybersecurity concerns barrage campuses with threats daily.

The 2015 cyberattack on Penn State University's College of Engineering occurred over two years, where hackers gained access to usernames and passwords. At the time, the Vice Provost for Information Technology said that on an average day, Penn State managed more than 20 million cyberattacks, an average amount for a research university.

Although threats to IT security barrage campuses often, the saying, "you can't be everything to everyone," holds true for college cybersecurity teams. Given the many cyber threats colleges face, most school IT security teams cannot tackle every possible one with the same resources. Therefore, understanding the threat landscape or homing in on the threats campuses will most likely be exposed to help security teams focus their resources on the most likely threats to hit campus.

**Using threat intelligence is one way to understand the threat landscape to increase awareness about cyber threats.**

## What is threat intelligence?

Threat intelligence plays a crucial role in safeguarding colleges and universities from potential dangers. It involves gathering information about threats that could target educational institutions, including the methods and strategies employed by malicious actors to infiltrate systems and networks and the resulting emergency situations that may arise.

In essence, threat intelligence entails collecting and analyzing data points that highlight trends capable of negatively impacting a college or university. These trends encompass various hazards, such as potential cyber threats, service disruptions and reputational threats.

Threat intelligence is based on solid evidence and provides a valuable backdrop to understanding the mechanisms, context, indicators and insights of emerging or existing dangers to college campuses.

What traditionally required dedicated teams focused on data acquisition and analysis, there are now more options and tools available for colleges regarding threat intelligence. Given the ever-evolving cyber landscape and growing trend of remote learning, threat intelligence has become an indispensable tool for colleges and universities aiming to achieve resilience in the face of a cyberattack.

**Threat intelligence entails collecting and analyzing data points that highlight trends capable of negatively impacting a college or university.**

## Threat intelligence and risk management

Threat intelligence is one of the first components of a good risk management program. A risk management program takes the insights from threat intelligence to create long-term processes for mitigating risk and addressing longer-term vulnerabilities. It also ensures that resources are spent in the most critical areas, and school leaders know and have adopted the processes involved in responding to a cyberattack.

Risk management for higher education typically addresses mitigation processes for all campus activities, not just cyber threats, such as food service, health, security, science lab safety measures and transportation.

## 3. Prioritize Data Security

At the heart of cybersecurity concerns, data security is of utmost importance for colleges and universities because of the critical role personal data plays within these institutions. Eighty percent of data breaches in education occur at the college or university level. Although some data breaches are not reported at all, or immediately, in 2023, 11 data breaches have occurred at higher education institutions, including a possible security breach involving personal data in the University System of Georgia's software system.

The management and protection of personal data lie at the core of cybersecurity, influencing almost every aspect of a school's operations. As a result, ensuring data safety and security becomes a collective effort that requires the support of upper administration and active involvement from all individuals.

One crucial aspect of data security is safeguarding the information of everyone associated with the university or college, including current and prospective students, faculty, staff, administrators, vendors, visitors and alums. It is vital to implement robust measures to protect the sensitive data of these individuals considering the potential risks and consequences of data breaches.

**80%**

of the data breaches in education occur at the university or college level

**11 DATA BREACHES**

have occured in higher education institutions in 2023

## Legal responsibilities

The legal landscape governing data protection and colleges and universities is fragmented in the United States, varying in scope and coverage. Nonetheless, federal laws exist to safeguard specific data in higher education institutions that receive federal funding. These laws include the Family Educational Rights and Privacy Act of 1974 (FERPA), the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Federal Information Security Management Act of 2002 (FISMA).

Several states have enacted laws to address the gaps left by federal regulations to protect the data collected by higher education institutions. These state-level laws cover a wide range of data, including that of students, protective students, administrators, staff, visitors and vendors. These measures aim to enhance data security and privacy standards within educational institutions and foster a safe room environment for everyone.

Furthermore, international students, specifically from the European Union, present an additional consideration for data security. The EU's General Data Protection Regulation (GDPR), implemented in 2018, is a comprehensive data privacy law that applies to organizations collecting, storing or holding personal data belonging to individuals of EU member states. Higher education institutions must ensure compliance with GDPR requirements, which include minimizing data collection, limiting data storage and being accountable for data processing activities. Specific categories of sensitive data even require protection under GDPR.

By prioritizing data security, colleges and universities can protect the privacy and trust of their stakeholders, maintain legal compliance and mitigate the potential harm caused by data breaches. Implementing robust security measures that follow relevant laws and regulations is crucial to safeguarding the sensitive information handled within higher education institutions.

## 4. Communications plans and mass notification systems

During and after a cyberattack, an intelligent and streamlined communications plan that can reach many people quickly is key to informing the school community, bolstering campus operations' resilience, mitigating damage and helping with response and recovery. Since coordination is vital for the best outcomes during critical events such as cyberattacks, having a solid communication plan (and the technology to support it) is imperative.

A crisis communication plan outlines the roles, responsibilities and protocols that will guide a university or college in promptly sharing information with all of the school's audiences during an emergency or crisis, such as a cyberattack. The communication plan is part of a university's emergency management plan. The plan should cover students, faculty, staff, alums, parents, trustees, neighbors, city leaders, media, local community and state and federal officials.

The crisis communication plan establishes specific protocols to facilitate efficient information flow, ensuring that accurate and timely updates are provided. These protocols may involve using various communication channels such as email, social media, official websites, press releases, emergency alert systems and dedicated hotlines.

The plan also assigns specific responsibilities and roles to key individuals or departments, which empowers them to act promptly and effectively during the crisis. This includes designated spokespersons trained in crisis communication and possess the expertise to deliver consistent and reassuring messages.

Ultimately a well-constructed crisis communication plan serves as a vital tool for universities and colleges to mitigate the impact of emergencies, maintain trust and confidence among their diverse audiences and safeguard the institution's reputation and operations in the wake of cyberattacks or other crises.

**PROTOCOLS FOR CRISIS COMMUNICATION MAY INVOLVE**

- Email
- Social Media
- Websites
- Press Releases
- Emergency Alert Systems
- Dedicated Hotlines

## Communication technology

Cyberattacks can directly impact a school's operations, so having the right communication tools in place before, during and after a critical event is crucial. And as cyberattacks evolve, tools that are scalable and flexible are essential.

Mass notification, a technology many colleges and universities utilize for routine business, has its genesis in emergency alerting. Because of its multi-channel architecture, mass notification makes it possible to reach large numbers of people on their preferred devices, no matter where they are.

Because classes have become more dispersed or hybrid, relying on email alone has become an insufficient means of communicating. Adding a mass notification platform to the mix can better manage communications daily and during disruptions.

Mass notification systems promptly alert students, faculty, staff and other relevant stakeholders to help mitigate the potential damage caused by cyberattacks. These systems facilitate immediate response actions, such as instructing users to change passwords, avoid certain websites, update the security software or take other necessary precautions.

## What Makes Mass Notification Different

- **Multi-channel delivery**
- **Cloud-based and encrypted**
- **Unaffected by power outages**
- **Reaches people anywhere**
- **Enables two-way communication**

Mass notification makes it possible to reach large numbers of people on their preferred devices, no matter where they are.

Not all mass notification platforms are alike. For a system to provide the best tools for emergency alerting needs, one must consider the platform's features and capabilities. Before committing to any mass notification provider, make certain it provides the following:

### Easy-to-use interface

During times of emergency, sending and receiving important notifications must be simple and quick.

### Cloud-Based Fail-Safe Features

The platform should operate reliably even during power outages or cellular tower disruptions.

### Automated Alerts

Mass notification systems that integrate with the National Weather Service, National Oceanic and Atmospheric Administration (NOAA) and Integrated Public Alert & Warning System (IPAWS) can alert automatically during severe weather events.

### Two-Way Communications

The right solution allows two-way communications for advising others and getting updates from affected areas.

### Notification Templates

Predefined templates can help save time during emergencies and serve to ensure messages are accurate.

### Mobile Apps

The right solution should include a companion mobile app allowing people to receive alerts wherever they are.

### Desktop Notifications

Desktop notifications can be pushed out instantly to on-site or remote stakeholders.

### Geo-Targeting Functionality

A mass notification system that allows geo-specific alerts can help you target only those in an affected area.

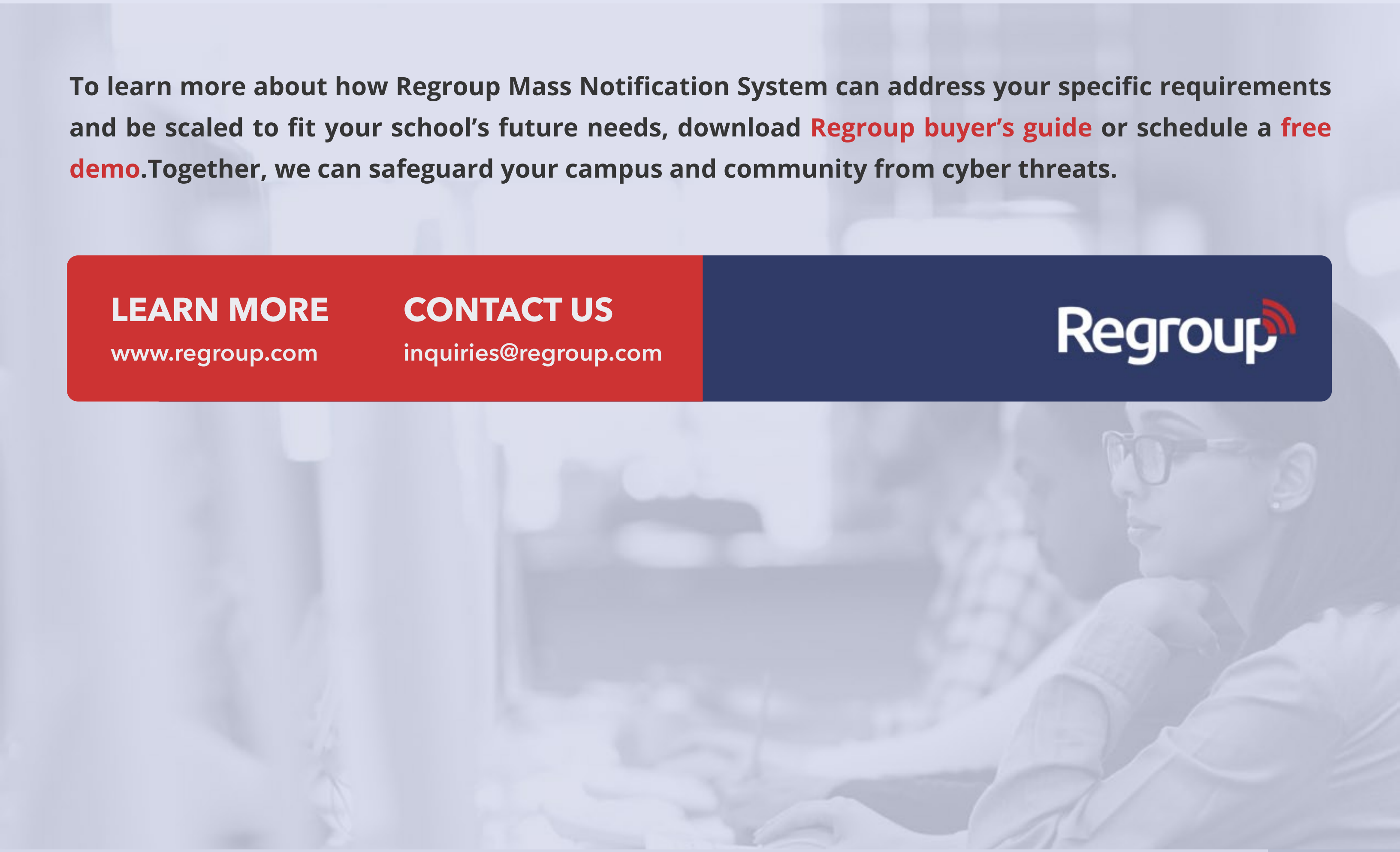
Mass notification systems are vital to a comprehensive cybersecurity strategy for higher education institutions. These systems enhance preparedness, response capabilities and overall cyber resilience. By leveraging the power of timely and targeted communication, schools can effectively safeguard against cyber threats and maintain a secure environment for their campus and community.

# Final thoughts

As college campuses increasingly rely on cyberspace for various activities, addressing cybersecurity threats becomes more urgent. With students using computers and smartphones more frequently and campus technology teams facing complex cybersecurity challenges, proactive measures are essential.

By implementing proactive measures, colleges and universities can safeguard their campuses, protect sensitive data and maintain trust among their stakeholders. The ever-evolving cyber landscape and the growing trend of remote learning make it imperative for institutions to prioritize cybersecurity and leverage the right tools and strategies to ensure a secure environment for their campus and community.

A mass notification system, such as Regroup Mass Notification, offers multi-channel delivery, cloud-based encryption and the ability to reach people anywhere, ensuring effective communication during cyberattacks. Features like automated alerts, two-way communication, notification templates, mobile apps and Geo-targeting enhance their functionality. These systems are indispensable components of a comprehensive cybersecurity strategy for higher education institutions bolstering preparedness, response capabilities and overall resilience against cyber threats.



**To learn more about how Regroup Mass Notification System can address your specific requirements and be scaled to fit your school's future needs, download Regroup buyer's guide or schedule a free demo.Together, we can safeguard your campus and community from cyber threats.**

**LEARN MORE**
www.regroup.com

**CONTACT US**
inquiries@regroup.com

Regroup

# Sources

https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/resources/information-security-guide/hot-topics/federal-data-protection-laws

https://studentprivacycompass.org/state-laws/

https://www.endpointprotector.com/blog/eu-vs-us-what-are-the-differences-between-their-data-privacy-laws/

https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Data Security and Management Training_1.pdf

https://cdn.ymaws.com/theatlis.org/resource/resmgr/documents/cyber/atlis_2022_cyberrecs.pdf

https://www.ncsc.gov.uk/collection/board-toolkit/understanding-the-cyber-security-threat

https://cyberscoop.com/verizon-dbir-report-hacking-2020/?__hstc=114028632.280d90bfcb0aff42c522aa53449bfe7d.1688393257309.1688393257309.1688393257309.1&__hssc=114028632.1.1688393257309&__hsfp=1390145134

https://www.fierceeducation.com/technology/top-5-cybersecurity-threats-facing-higher-education