WHITE
PAPER

COMMVAULT

# Cybersecurity in Higher Ed:

## Implementing a Data Protection Plan to Mitigate Risks

eCampus News.com

**83% of attacks** involve some form of data leakage, exfiltration, theft, or damage.

# Cybersecurity in Higher Ed: Implementing a Data Protection Plan to Mitigate Risks

Data presents a powerful resource and risk to higher ed institutions and individuals. Academic environments are rich with sensitive information, including student records and other personally identifiable information, financial aid and transaction data, healthcare information, and innovative, specialized research data. Bad actors are not only looking to exploit institutional and student data, but valuable intellectual property stolen or compromised could cause considerable damage beyond the institution's walls, including the threat to a university's reputation.

Cybersecurity attacks and their motives are evolving and with greater success - with 83% of attacks involving some form of data leakage, exfiltration, theft, or damage. For example, the 2022 Verizon Data Breach Investigations report highlighted that education and research institutions were victims of an average of 1,065 successful cyber-attacks per week in 2022, a 75% increase from 2020. Therefore, to mitigate and reduce any effect of a successful cybersecurity event, higher ed institutions are focusing more on the security of their data than just the security of their systems. Implementing a data resilience strategy, such as a data protection plan (DPP), ensures data safety and security within their organizations.

## Data Protection Plan Elements

As data is the most critical asset to any organization, the DPP's elements include data lifecycle management, access management, and storage management.

**Data life cycle management** addresses data creation, classification, storage, and retention policy – for all the data. For higher ed institutions, it helps them become proactive in understanding its information and in applying policies to information so it can protect while in use and over its life cycle. Its capabilities include data discovery, classification, encryption, obfuscation, and defensible disposition, allowing data to be disposed of after its business purpose has ended. These factors are critical to any institution to meet the ever-changing compliance requirements reflected in General Data Protection Regulation (GDPR), the Federal Educational Rights and Privacy Act (FERPA), the California Consumer Privacy Act (CCPA) compliance regulations, and other federal and state regulatory requirements regarding the protection of data.

**Data access management** allows institutions to authorize users, employees, and other stakeholders to access data that meets security, privacy, and compliance requirements. The zero-trust model assumes every connection and endpoint is a threat. Therefore, every device, user, and network flow should be authenticated and authorized. A zero-trust model's successful implementation can bring context and insight into a rapidly evolving attack surface. It also provides the framework for managing who, or which groups of people, have access to different data types and locations.

**Data storage management** refers to the processes that improve the performance of data storage resources. This process involves monitoring both software and hardware components. Higher ed and research institutions cannot afford long-term disruptions to operations due to a data breach or data loss; resuming operations as quickly as possible is vital to their operation and reputation. Robust data storage management that includes network virtualization, replication, mirroring, security, traffic analysis, process automation, and storage provisioning can speed up data retrieval, prevent data loss, meet data retention requirements, and reduce IT expenses.

**A one size fits all approach** to cybersecurity practices **does not work in higher ed** institutions due to their unique data elements, digital footprints, processes, and risks.

## Understanding The Institution

It is essential to note that while the principles are the same no matter the organization, higher education, and research institutions must consider their distinctive and unique attributes, including vast research data, data autonomy, and data compliance. A one size fits all approach to cybersecurity practices does not work in higher ed institutions due to their unique data elements, digital footprints, processes, and risks.

**Research Data**
These rich learning environments generate varied file sizes and types that can strain the storage infrastructure and affect the available storage solutions and sharing capabilities for that data.

**Data Autonomy**
University researchers are given a lot of autonomy as 'super users' of data storage, which is different from other organizations' hierarchical models. This autonomy challenges IT departments implementing a DPP data access management component.

**Data Compliance**
Data governance policies in higher ed policies vary in complexity and often 'tier' data types according to sensitivity and value. In addition, as cybersecurity and data protection regulations are escalating, institutions must consider their unique profiles, including academic and research activities, while at the same time ensuring the security of their data.

## Proactive Measures

Academic institutions can tailor four components of a robust data protection plan to protect sensitive data stored within their networks while accommodating the many needs of their staff, faculty, and students. These include cybersecurity risk assessments, mitigation plans, recovery plans, and continuous improvements.

### Cybersecurity Risk Assessment

Available attack surface forms potential vectors or pathways where threat actors can gain unauthorized access and privileges to confidential data in an institution's system using malware, viruses, email attachments, messaging, and social engineering. Higher ed institutions can reduce available attack surfaces by performing cybersecurity risk assessments on threats, likelihood, vulnerability, and consequences.

Institutions have multiple avenues to conduct periodic or continual risk assessments on their networks and data. These include hiring security professionals and penetration testers to assess or invest in risk assessment software. For example, Commvault's risk assessment tool determines an institution's level of ransomware protection and delivers solutions and features to improve ransomware protection and recovery capabilities. Risk assessment is not merely testing something. It includes processes, technical tools, and techniques to mitigate risks. In addition, upon request and as resources are available, the Cybersecurity and Infrastructure Security Agency (CISA) conducts risk and vulnerability assessments (RVA) that find vulnerabilities that cybercriminals could potentially exploit to compromise security controls and provide institutions with data, tailored risk analysis, and ways to improve their cyber security.

## Risk Mitigation Plan

The second component of developing an institution's data protection plan is to create a systematic approach where the institution proactively identifies risks across the organization and then plans necessary actions to mitigate them, improve their resiliency, and meet compliance goals.

### Updates and Use of Automated Delivery

Immediately updating all available software through automation and vendor-provided software can deter threat actors from studying patches and creating exploits, often soon after a patch is released. However, with the constantly evolving and changing nature of online threats and the general attack surface, institutions must be vigilant in keeping software systems and IT infrastructure up to date.

### Inventory

Institutions must know what devices and software are on their networks and remove unwanted, unneeded, or unexpected hardware and software from the network. This is the basis of protecting your data. Starting from a known baseline reduces the attack surface and sets up control of the operational environment.

### Backups

Regular data backups, following appropriate sensitivity/use of data, ensure that data is highly available and safe. Based on the impact of data loss on an institution's daily operations, automated backups should use suitable tools and systems to make them more manageable. Depending on the institution and relevant data regulations, these backups should be stored securely for a defined time.

In addition to traditional system backups, institutions should create an isolated recovery environment (IRE), a tertiary solution for vertical data. This dedicated, secure recovery environment has resources to verify and recover data from an immutable or unchangeable backup copy impervious to ransomware, rogue insider actions, or accidental deletions.

**Building a cybersecurity awareness culture** where all stakeholders understand the requirements under the institution's data protection plans, laws, and regulations can reduce the number and gravity of cyber threats.

## Cybersecurity Recovery Plan

A cybersecurity recovery plan is at the heart of an institution's resiliency posture. This comprehensive plan protects critical data and ensures the continuity of operations due to malicious threats and ransomware. The recovery plan should detail steps to stop losses, end the threat, and move without jeopardizing the institution's future. The measures include minimizing data accessibility to hackers, identifying the security breach with sufficient recovery time, communicating with stakeholders, and implementing a rapid restoration using SIEM/SOAR ecosystem solutions to protect applications and networks for forensic analysis and network monitoring tools. These plans should not be shelf-ware; they should be frequently updated and exercised. It is one thing to back up data, but how fast and in what sequence can it be recovered?

## Continuous Improvement

A data protection plan involves any steps taken to safeguard critical organizational data, including protecting information from cyberattacks or other threats or restoring backed-up information when compromised. One of the most crucial steps after a cyber incident is to analyze security gaps and learn what to improve. This step could involve strengthening security protocols and implementing reasonable and practical policies, controls, tools, processes, and technologies. Even leveraging experienced internal and external cybersecurity resources to ensure appropriately configured technical solutions and governance-related protocols are structured can reduce the risk of another attack.

Building a cybersecurity awareness culture where all stakeholders understand the requirements under the institution's data protection plans, laws, and regulations can reduce the number and gravity of cyber threats. It can also enhance the collaborative and shared learning environment as it relates to institutions of higher learning.

## Simplicity and Completeness

Simplicity and scalability are critical when ransomware strikes to minimize disruption and resume organizational operations quickly. Additionally, organizations must protect, detect, and recover from ransomware threats through multi-layered security and Zero Trust Principles for on-premises, SaaS applications, cloud, and hybrid infrastructures with a unified customer experience.

COMMVAULT®

Commvault provides data protection & recovery services regarding cybersecurity in higher education. Its data management and protection unify data management and protect data at scale for all workloads across on-prem and hybrid/multi-cloud environments. Through a Zero Loss Strategy, built on Zero Trust Principles and implemented through their multi-layered security framework, higher ed institutions can better plan, manage, and reduce ransomware risk and ensure their data is ready and available for their businesses. Additionally, with Commvault's' detection technology, Metallic® ThreatWise™, higher educational institutions can implement an early warning system that proactively surfaces unknown and zero-day threats to minimize compromised data and business impact due to potential cyber-attacks. Start today with Commvault's Ransomware Protection Assessment.

eCampus News.com

**This white paper was produced by eCampus News**, the leading online platform that delivers daily technology news and information to higher-education administrators, educators, and technology professionals, and dedicated to the advancement and wise use of technology to improve teaching and learning for all. eCampus News offers ed-tech decision makers a wide range of informative content—including newsletters, webinars, case studies, white papers, websites, and more—that provide in-depth coverage of the latest innovations, trends, and real-world solutions impacting the education community. www.eCampusNews.com