SPANNING
A Kaseya COMPANY

CHECKLIST

FIVE STEPS TO SAFEGUARD YOUR STUDENT DATA

The dynamic landscape of the education industry has made digital transformation a cornerstone of learning environments. With the reliance on digital platforms soaring, educational institutions are finding it difficult to safeguard their student data. Ensuring the privacy and security of such precious information is vital, considering the sensitive nature of student records and the regulatory landscape. However, protecting student data presents a myriad of challenges.

The prevalence of cyberthreats exposes educational institutions to potential breaches and unauthorized access. Hence, a proactive approach to fortify security infrastructure is needed. Stringent data protection laws and compliance standards, such as the Family Educational Rights and Privacy Act (FERPA), adds another layer of complexity, requiring institutions to navigate a regulatory framework to avoid legal consequences and keep stakeholder trust. Also, there are unforeseen events, from hardware failure to natural disasters, that pose a threat to the continuity of educational operations. All of these make data loss a real and persistent risk.

EDUCATIONAL INSTITUTIONS ARE SOFT TARGETS FOR RANSOMWARE

The wealth of sensitive student data possessed by schools and universities, coupled with comparatively limited cybersecurity resources, makes them lucrative targets for cybercriminals. *As per a Malwarebytes report*, in the period between **June 2022** and **May 2023**, the education sector experienced a sharp rise in ransomware attacks, with an **84% increase** observed over six months.

The decentralized nature of educational networks, with multiple connected devices and users, amplifies the susceptibility to attacks. Often, the budgets for cybersecurity measures in educational institutions are underfunded. This creates a security gap that ransomware attackers exploit. Moreover, the inability of these institutions to have access to student data and carry out educational operations seamlessly during an attack makes them *around 80%* more likely to pay the ransom, fueling the appeal for malicious actors.

It is a challenge for schools and universities to safeguard their student data from ransomware because many K-12 districts have fewer resources to support cybersecurity and relatively open “Bring Your Own Device” (BYOD) policies.

SAFEGUARDING STUDENT DATA: FIVE KEY STEPS

To secure an educational environment, implementing effective measures for protecting student data is paramount. A strategic approach to fortify data protection ensures the confidentiality and integrity of vital student information. Proper implementation of cybersecurity measures, regular patching and updating of systems, comprehensive cybersecurity awareness training, strict access controls and user activity monitoring, and carrying out a thorough data backup and disaster recovery planning can help enhance the resilience of institutions like yours against evolving cybersecurity challenges.

Let’s explore these key steps in detail.

IMPLEMENT ROBUST CYBERSECURITY MEASURES

Fortify your educational institution against cyberthreats by embracing robust cybersecurity measures. From the usage of firewalls and intrusion detection systems to encryption policies and multifactor authentication, each of them contributes to creating a secure digital environment for student data.

MEASURES	TACTIC	
Firewall and intrusion detection systems	**Firewall** usage helps to monitor and control the incoming and outgoing network traffic. Configure firewalls to block unauthorized access and deploy **intrusion detection systems** to spot and tackle potential security threats in realtime.	
Encryption	Apply strong **encryption policies** for both data in transit (e.g., using SSL/TLS protocols) and at rest (e.g. encrypting databases and storage devices). Regular reviewing and updating of encryption methods helps adhere to the latest industry standards.	
Multifactor authentication (MFA)	Implement **MFA** to access sensitive systems and databases, ensuring that even if the login credentials are compromised, an additional layer of authentication is there. Users must be educated about its importance and encouraged to use it across all school/ university systems.	
Cloud detection and response	Leverage cloud detection and response to monitor, analyze and respond to threats within your SaaS environments, such as changes in access controls, elevation of privileges or removal of administrator accounts.	

REGULARLY UPDATE SOFTWARE AND SYSTEMS

Prioritizing regular updates for software and systems ensures the integrity of student data. This helps mitigate vulnerabilities and keeps your educational institution resilient against evolving cyberthreats.

MEASURES	TACTIC	
Patch management	Establish a **patch management** framework to quickly apply security patches to operating systems, software applications and network devices.	
Vulnerability assessments	Conduct **regular vulnerability assessments** to identify and address potential flaws in the school's or university's IT infrastructure.	

PROVIDE CYBERSECURITY TRAINING FOR STAFF AND STUDENTS

A robust security awareness training for students and institution staff elevates awareness of phishing threats and instills best practices for password security.

MEASURES	TACTIC	
Phishing awareness	Conduct simulated **phishing awareness** exercises to train the students and staff on recognizing phishing attempts. In this process, setting up clear communication channels to report suspicious emails and incidents is necessary.	
Password security	A **strong password policy** must be enforced. This includes regular password changes and complexity requirements. Password managers must be promoted to encourage the creation of unique and secure passwords.	

ADOPT STRICT ACCESS CONTROLS

Another key method to enhance the security of student data is to adopt stringent access controls. Be it the implementation of role-based access controls (RBAC) or leveraging user activity monitoring tools, the primary aim is to minimize the risk of unauthorized data access.

MEASURES	TACTIC	
Role-based access controls	Implement **RBAC** to restrict permission based on job responsibilities, ensuring that individuals have the minimum level of access required to perform their duties.	
User activity monitoring	Leveraging user **activity monitoring tools** provides a comprehensive overview of system interactions. It is useful to track and analyze user behavior, helping to identify and respond to any anomalous or suspicious activities.	

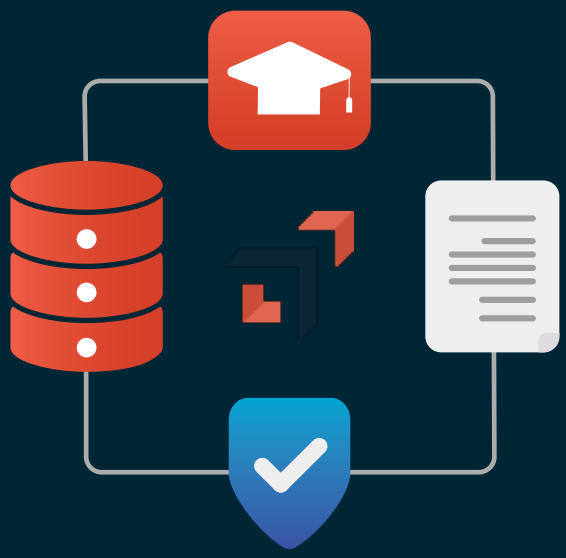
EMPHASIZE DATA BACKUP AND DISASTER RECOVERY PLANNING

Proper backing up of critical student data gives peace of mind that the data is safe and secure. Along with foolproof disaster recovery planning, it guarantees swift restoration of the data in the face of unforeseen events.

MEASURES	TACTIC	
Regular backup procedures	Conduct **regular, automated backups** of critical student data and ensure the backup systems are secure from unauthorized access. Data restoration procedures must be examined periodically to confirm data integrity and availability.	
Disaster recovery planning	Develop a robust **disaster recovery (DR) plan** that will showcase the steps to take in the event of a data breach, system outage or other emergencies. Conducting regular drills and simulations will help test the effectiveness of the DR plan.	

With the proper application of these detailed measures, you can set up a more resilient approach to protecting your student data in an ever-evolving threat landscape. In addition to that, regularly reviewing and updating security measures are vital to stay ahead of the emerging security challenges.

Start protecting your student data with Spanning Backup



An ideal backup and recovery solution seamlessly manages complex data protection in the cloud, allowing your organization to focus on what it does best — educating minds, driving research and sparking innovation.

As the No. 1 SaaS backup for education, Spanning does that and more. Get automated daily backups to securely store your data in the cloud and a fast, easy-to-use restoration process to recover it whenever you need it.

So, start protecting your student data with our *14-day FREE trial today.*

SPANNING
A Kaseya COMPANY

13012025