Published on *The National Law Review* https://natlawreview.com

Data Breaches and Educational Institutions

Article By:

Marjorie Spivak

Taylor Ey

Consider these five steps during your summer break to address the protection of confidential information and combat cybersecurity risks before the start of fall semester.

1. Information Assessment: Identify what data your institution holds, how it is used, how is it protected, and who has access

Did You Know? Last year, according to Verizon's 2019 Data Breach Investigation Report, human error accounted for 35% of data breaches in the education sector.

Educational institutions hold valuable and sensitive data (paper files and electronic ones), such as personal, financial and medical data on prospective students, enrolled students and alumni, employment information about their faculty and staff, and research data. Data may include FERPA-protected student records, but also data that is subject to other laws as well, such as staff payroll and student payments. With an inventory of the types of data held, and for what purpose, institutions are empowered to identify departments and resources that deal with data privacy issues and need support, identify the laws or regulations that govern use of the data, and create a data protection program specific to the institution's needs.

2. Asset Assessment: Routinely assess network devices, systems and software platforms within the institution to ensure technical solutions; monitor for suspicious activity; and identify organizational solutions that minimize risk

Did You Know? Last fall, the FBI issued a public service announcement stating that the education sector was one of those most affected by a social engineering scheme designed to get unauthorized access to online payroll accounts.

The open and sharing environments of learning centers create vulnerabilities in this age of digitization and connectivity. Teachers and students communicate via email; educators use tablets and smart devices and access the internet in the classroom. Mobile devices are often lost (and the data on them accessed without authorization if not properly protected or remote wiped). Equipment that connects the school to the worldwide internet poses a threat. If an educator or student clicks on a bad link or replies to a phishing email, then the school could be subject to a hacker or other vulnerabilities. Institutions should routinely review their network activity, and determine a baseline for what activity on its network is considered “normal,” and likewise be able to identify any activity that would be considered “abnormal.” Knowing your network allows the institution to conduct a risk assessment to identify cyber threats and vulnerabilities within the institution’s environment, and tailor technical solutions including firewalls, encryption and authentication solutions accordingly.

3. Review vendor selection processes, vendor relationships and vendor contracts

Did You Know? When a school uses discontinued software, the school is at risk of a data incident because hackers look for out of date code. One example is the recent Stanford University data breach. **Stanford continued to use a software product after the company discontinued it, which led to a significant exposure of personal data.**

Schools share information with their service providers for a variety of purposes, including to process applications, to provide financial aid, to accept payments, and to host their websites and student portals. This means that more companies and people will access student, parent, faculty, or staff personal information than just the admissions department or financial aid office. Like other businesses, educational institutions should carefully vet their service providers prior to providing them access to personal information from members of the campus community. A school should not engage a service provider until the vendor has agreed in a written contract to protect confidential school data and has granted contractual, technical and operational protections for such data. Institutions should also routinely review their service providers to ensure that they are still supporting software solutions, and routinely providing updates.

4. Reassess insurance policies and consider identifying a chief information security officer (CISO)

Did You Know? Many cyber insurance policies exclude “voluntary parting” or “voluntary payments” (i.e., losses flowing from insured’s voluntary transfer of money to a third party). “Insurance Coverage for Social Engineering Fraud,” Westlaw Journal Insurance Coverage, January 26, 2018.

In the United States, institutions may take out cyber insurance policies to cover some of the risks associated with data breaches. But cyber policies have exceptions and not all cyber risk is insurable. In addition, cyber threats are constantly changing and your insurance may not keep pace. Summer is an excellent time to review policies and update as appropriate.

Schools can also assess whether they should hire a part-time CISO or full-time CISO. A CISO offers an expert voice on matters of information security, including reviewing and commenting on internal policies and procedures, assessing data management practices, and recommending technical solutions for mitigating security risks.

5. Prepare a cybersecurity incident response plan (CIRP)

Did You Know? In 2017 and 2018, the education sector (K-12 and higher education) experienced 49 events exposing over 48 million records according to the Privacy Rights Clearinghouse Chronology of Data Breaches.

Data security incidents can shut down the business of your institution. Three years ago, the University of Calgary paid $20,000 to release its operational computer systems from a software lockdown. When a recent data breach at Georgia Tech exposed up to 1.3 million records of students, faculty and alumni, and slowed certain aspects of school administration to a halt. A data security incident should not be the first time an institution thinks about whom in the administration to contact, how to remediate systems to stop the incident,
and otherwise how to respond to a data breach. Understanding the distinct nature of the environment, network, and information technology will allow the institution to create a CIRP tailored to the specific needs of your organization. The plan should cover preparation, detection and analysis, containment and eradication, recovery and post-incident analysis.

National Law Review, Volume IX, Number 199

Source URL:https://natlawreview.com/article/data-breaches-and-educational-institutions