Canon
CANON SOLUTIONS AMERICA

CENTER FOR DIGITAL EDUCATION

NO ROOM FOR COMPROMISE:

SECURING STUDENT DATA ON THE TECH-DRIVEN CAMPUS

SMART CHANGE STARTS HERE.

CANON SEE IMPOSSIBLE

STUDENT DATA UNDER SIEGE

Higher education institutions are under cyber siege. Institutions of all sizes have been targeted for their valuable caches of personal student information and research data. In fact, in 2018 a textbook company was targeted in a massive hack. The data breach hit Pearson, a British company that produces educational tools including textbooks and digital textbooks. First and last names, email addresses, and dates of birth were taken during the hack.[1]

These cybercrimes are frequently blamed on foreign hackers, but the threat can sometimes be much closer to home. The actual number of students affected by the hack is unknown but it is certainly in the hundreds of thousands. The information-security officer for one school district in Nevada said data from 114,000 students enrolled between 2001 and 2016 were affected in the breach.[1]

Student data privacy is an important component of a safe learning environment. To maintain a competitive advantage, university leaders, administrators, business officers, CIOs, and procurement chiefs must develop security policies that support student data privacy without creating inconvenient bureaucratic hurdles or clunky technology workflows.

This Center for Digital Education (CDE) issue brief reviews the risks of security breaches; identifies technologies, systems and processes that leave systems vulnerable; and provides an overview of security controls higher education institutions can implement to better protect student data.

[1] *Kim Komando - School and University Data Breach Exposes Details on Thousands of Students https://www.komando.com/happening-now/585596/school-and-university-data-breach-exposes-details-on-thousands-of-students*

[2] *Cost of a Data Breach Study by the Ponemon Institute and IBM Security*

UNDERSTANDING WHAT'S AT RISK

In higher education, student data is a component of learning delivery and management systems, as well as longitudinal data systems that capture, analyze, and use the information to achieve statewide goals for improving student outcomes. However, parents and students alike are concerned these systems compromise privacy when vendors mine data for profit or marketing purposes.

Besides inserting some control over the way vendors use data, education institutions must also protect it from cybercriminals who have the know-how and will to breach networks and systems. Higher education student data is valuable because it holds academic and personally identifiable information, as well as student and parent financial and employment data.

A recent major data breach that affected thousands of university students was recently released. Personal information of the students was exposed when a popular education company's database was breached in November 2018. In December 2018, the personal information of 500,000 students and staffers in one California school district was stolen by hackers.

This incident involved phishing, which involves a hacker sending emails that look authentic but instead redirect recipients to fake login pages. Once a user tries to log into the fake pages, the hacker can steal their credentials.[1]

In addition to loss of data, an organization's reputation may take a hit in the event of a security breach. Schools will have to work to restore employee morale and student and parent trust. Students may be wary of further interactions with online systems and services, such as online learning.

There are also hard costs associated with remediating a data breach. Possible expenses include communication and IT contractors, forensics consultants, lawyers, call centers, websites, mailings, identity protection services, credit check services, and litigation. The actual price tag depends on the type of breach, location of breach, and the number and type of records affected.

In a recent Ponemon study, the average cost of a data breach in education is $4.77M. In the same study, it states the average cost per record is $142.[2] A massive 2013 breach at Maricopa County Community College District in Arizona, which exposed personal information, including Social Security numbers and banking information of more than 2 million people, cost more than $26 million to remediate.

TECHNOLOGIES, SYSTEMS AND PROCESSES THAT IMPACT STUDENT DATA PRIVACY

The proliferation of technology platforms, systems, applications, networks, and devices that collect and store data has created a complex higher education environment with numerous security challenges.

- **Decentralized IT systems.** Shared services and centralized IT departments have been slow to take hold in higher education. Historically decentralized, higher education technology systems are managed at the individual department level. Security complications include multiple IT, security, and privacy stakeholders; diverse security strategies; numerous interfaces among departmental and non-departmental systems; and large amounts of student data.
- **Wireless networks and mobile devices.** To remain competitive, education institutions must provide campuswide wireless access and the ability to access it via mobile devices—a necessity that carries with it the risk of access by unauthorized network-connected devices, a leading cause of security breaches. Institutions must keep unauthorized users off wireless networks and away from internal networks, systems, and data.
- **Cloud-based services and infrastructure.** Hosted services and applications allow students and educators to access the tools they need for teaching and learning no matter where they are, but they can pose a threat because data stored in an external application may not be fully under school control. In addition, the institution has limited control over an external vendor's security practices.
- **Technology-related threats to physical infrastructures.** Careless or improper treatment of technology equipment such as printers, copiers, scanners, multifunction devices, external storage, disks, and hard drives can compromise data privacy. For example, unauthorized persons may accidentally view paper copies containing confidential information. Cybercriminals can intercept documents sent to a networked printer and can hack into printers with hard drives. Additionally, external storage media is at risk for theft, loss, or malware infection.
- **Decommissioning and disposal of old equipment.** Because computers, mobile devices, servers, and printers all have hard drives that could contain confidential student information, decommissioning and disposing of them improperly poses a security risk through data reminiscence.
- **Access cards and badges.** Most higher education institutions use some type of contactless proximity or magnetic stripe swipe cards to allow authorized students and staff to enter buildings and rooms, check out library books, and purchase items. Students love the convenience of these so-called "one cards," but if the networked systems are breached, the hacker can enjoy access to a treasure trove of personal information.

THREE LAYERS OF SECURITY

The federal and state legislation that regulates privacy requires education institutions to take security measures to protect student data. An effective security approach includes an appropriate mix of administrative, technology, and physical controls.

Administrative Controls: Who Can Access Student Data?

Administrative security technologies limit user access to student and other data and applications. Controlling access with administrative controls is the most elemental step in cybersecurity.

This category includes tools that authenticate user identity; decide who can access specific applications and data and how they can use it; and help prepare for compliance audits by showing who accessed files and applications, made changes, printed copies, and transferred files to external storage.

Examples include:

- Identity and access management (IAM)
- Role-based user access
- Single sign-on (SSO)
- Self-service password management
- Two-factor/multi-factor authentication
- Audit trails and logging software

Technology Controls: Safeguarding Networks, Systems, Applications, and Data

Technology controls monitor on-premises, cloud-based, and hosted networks, data, applications, and systems for malicious activity and attempt to block it. Many of them use data analytics techniques to track and analyze device and user behavior to prevent and detect intrusions.

This category includes tools that screen and block inappropriate content and malware; monitor and control network traffic; and control mobile devices, applications, and data, among others.

Examples include:

- Data encryption
- Intrusion detection and prevention systems (IDS/IPS)
- Log management and event correlation
- Security incident and event management (SIEM)
- Mobile device management (MDM)
- Firewalls
- Content filtering/management
- Network patches and upgrades
- Virus, malware, spam and spyware protection

Physical Controls: Protecting Physical Machines and Infrastructure

Physical machines and infrastructure, such as local computers and servers, storage media, printers, scanners, copiers, and multifunction devices, are often overlooked in the rush to secure networks, applications, and associated data. Physical controls include:

- Industry best practices for equipment and storage life cycle management
- Software tools and third-party services to decommission old hard drives
- Pull printing features that hold a print job in the queue until the user is authenticated at the machine
- Printer-embedded security software for networked printers

CREATING STRONG PRIVACY AND SECURITY POLICIES

In the absence of specific federal and state laws that guide the use of data by vendors, colleges and universities should collaborate with legal, privacy, and security experts to develop or revise data privacy and security policies to regularly specify requirements on how vendors should collect, use, transmit, and safeguard student data.

To ensure student data is used only for educational purposes, frankly and directly discuss privacy and security concerns with vendors and contractors before signing contracts. Determine whether their policies for using student data for marketing purposes are compatible with your organization. Develop privacy provisions for insertion into contracts with any vendor or other third party that will be collecting or using student data.

Use the same due diligence when evaluating vendor technology, security controls, and security practices. Integrate security requirements into RFPs and contracts, and audit and monitor vendor data and security policies, procedures, and systems on an ongoing basis.

Pay special attention to the security practices of cloud-based services and infrastructures. Data stored in an on-premises application or school-controlled data center that's managed by others is historically viewed as safer than data stored on the public Internet or on shared servers. Yet as cloud services have increased in popularity, they are increasingly perceived as a safe alternative to on-premises applications.

BE IN THE KNOW: UNDERSTANDING PRIVACY MANDATES

Ostensibly, federal and state privacy laws protect student data. The primary federal mandate, the Family Education Rights and Privacy Act (FERPA), specifies institutions must have written parental and/or student consent prior to disclosing sensitive student data, including personally identifying data, billing and enrollment information, and educational records.

But FERPA was enacted in 1974, when the Internet, data analytics, and cloud-based learning didn't exist, so it's not specific to today's technology and learning environments, and has loopholes. For example, institutions may release directory information, including student name, address, telephone number, date and place of birth, honors and awards, and attendance dates without obtaining consent, though they're required to disclose the release and allow parents and students to opt out of directories. And, institutions may disclose student information to vendors.

A series of eight bills introduced into the House and Senate in 2015 aim to modernize FERPA, but these are largely silent on higher education, as are the majority of state student data privacy laws. That's a missed opportunity, said Elana J. Zeide, a privacy research fellow at New York University's Information Law Institute. "At least on the most basic level, federal privacy law recognizes that higher education students should have privacy rights as well," she said. "Even if they're not as vulnerable, higher education students can still suffer the harm that drives privacy concerns in the K-12 space."[3]

Besides FERPA, the other relevant federal data privacy law applicable to higher education institutions is the Health Insurance Portability and Accountability Act (HIPAA), which guarantees the confidentiality of health records.

CONCLUSION

Because the education environment relies heavily on IT platforms, systems, applications, networks, and devices to collect and store student data, protecting data privacy and security is a critical component of a safe higher education environment. Policies that support student data privacy help colleges and universities effectively manage the privacy and security challenges associated with the ensuing avalanche of student information.

Federal and state laws governing data privacy and security are a useful starting point. But security professionals realize compliance obligations are only the minimum effort required to protect their data and systems. Instead, they must create a culture where security and privacy best practices are ingrained into the operational environment.

When combined with thoughtfully crafted data privacy and security policies, a mix of administrative, technology, and physical controls is the most effective approach for keeping student data confidential and secure.

Security professionals realize compliance obligations are only the minimum effort required to protect their data and systems. Instead, they must create a culture where security and privacy best practices are ingrained into the operational environment.

[3] *https://www.insidehighered.com/news/2015/03/25/federalprivacy-bill-missed-opportunity-obama-administration-legalscholars-say*

This piece was developed and written by the Center for Digital Education custom media division, with information and input from Canon.