SAFEGUARDING STUDENT DATA IN THE AGE OF DIGITAL LEARNING

Responsible privacy practices for K-12 school districts

DEPENDENT ON DIGITAL

As K-12 school districts become more dependent on digital content and curriculum, protecting student data has increased in importance, especially for parents who are concerned about how their children's information is used. A Center for Digital Education (CDE) survey found securing student data is a top priority for school districts, yet only 44 percent of K-12 educators said they believe their institution's student data is "highly secure."[1]

Limited IT budgets are one reason for this gap. Privacy and security solutions often compete for budget dollars with student computing devices and other classroom technologies. School and district IT staffs also are stretched thin, and many lack a full-time chief information security officer. Further, the regulatory environment is a patchwork of outdated and evolving state and federal mandates.

Education leaders must constantly balance the need for privacy with the ability to provide students and educators with access to tools and content. This CDE issue brief looks at the current threat environment for student data privacy, reviews the regulatory climate, and provides an overview of security controls and best practices schools can implement to safeguard K-12 student data.

Student Data at Risk?

A CDE survey found securing student data is a top priority for school districts, yet only **44 percent of K-12 educators** said they believe their institution's student data is "highly secure."

POTENTIAL VULNERABILITIES

As the number of networked and interconnected IT systems that collect and store student information increases, data becomes more challenging to protect. Education continues to be plagued by errors, social engineering, and inadequately secured email credentials. In a 2019 survey, there were a reported 382 incidents, 99 with confirmed data disclosure. The top two patterns are miscellaneous errors and web application attacks. The top threats came from external sources at 57% and internal sources at 45%. The number one motivator was Financial, rating at 80%. 55% of the data compromised was personal information.[2]

Any network-connected device—including personal computers, mobile devices, servers, and even printers—provides a potential opening for a data breach. The rapid emergence of mobility and cloud-based services makes security more complex. And districts must also manage technology-related threats to physical infrastructure. Following are some of the most vulnerable areas of a digitally enhanced school or district.

Wireless networks and mobile devices, especially as part of a bring-your-own-device (BYOD) initiative, carry with them the risk of unauthorized devices connecting to the network, a leading cause of security breaches. But since BYOD is increasingly seen as a viable way to achieve 1:1 computing within the confines of limited IT budgets, schools must provide secure wireless access for students while keeping unauthorized users off wireless networks and away from internal systems and data.

Cloud-based services and infrastructure allow students and educators to access the tools they need for teaching and learning no matter where they are, but these services may pose a threat because data stored in a hosted application is not fully under school control. In addition, the school has limited control over an external vendor's security practices. When choosing a service contractor, educators need to fully vet data protection and data ownership policies documented in comprehensive SLAs.

Physical infrastructure threats arise from careless or improper treatment of technology equipment such as printers, copiers, scanners, and multifunction devices; external storage, disks, and hard drives; and computing devices. For example, unauthorized persons may accidentally view confidential paperwork left on a printer tray. And networked printers are vulnerable to the same security risks as any network-connected device. Cybercriminals can intercept documents sent to the printer and hack into printers that hard drives for storing print, scan, fax, and copy jobs.

External storage, disks, and hard drives with confidential files are at risk for theft or loss, as are student mobile computing devices. In addition, portable USB drives, camera cards, and other storage devices used to transfer files among computers can easily be infected with malware.

Finally, decommissioning and disposing of old equipment poses a security risk because computers, mobile devices, servers, and printers all have hard drives that could contain confidential student information.

THREE LAYERS OF SECURITY

The federal and state legislation that regulates privacy (see "Be in the Know: Understanding Privacy Mandates" on page 3) requires schools and districts to take 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. Limiting 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. 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 information 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

Protecting physical machines and infrastructure—local computers and servers, storage media, printers, scanners, copiers, and multifunction devices—is 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.
- Regular implementation of security patches and updates for all PCs and servers is critical.
- Endpoints such as printers, MFDs and scanners should be "hardened" i.e., closing non-essential ports and utilizing secure transport protocols such as SSL/TLS and Ipsec.
- Ensure that all default administrator user names and passwords are changed immediately upon new deployment of any device.

6 BEST PRACTICES FOR SECURING STUDENT DATA

1 **Create a security culture.** Security professionals know compliance obligations are only the minimum effort required to protect their data and systems. Instead, it's important to create a culture where security and privacy best practices are ingrained into an organization's operational environment. This includes developing a security policy that is reviewed and adjusted annually.

2 **Develop and maintain a security and privacy team.** Appoint a chief information security or privacy officer to oversee and prioritize data security efforts and develop a top-down, leadership and supporting team as needed. Bridge knowledge gaps and supplement organizational capabilities by outsourcing or collaborating with other schools, districts, and government organizations.

3 **Create a strong data privacy policy.** Many districts have outdated privacy policies. Legal, privacy, and security experts can help draft policies that specify how vendors may collect, use, and transmit student data. The Consortium for School Networking (CoSN) has a free privacy toolkit (see resources at end of brief).

4 **Engage with vendors and contractors.** Have vendor discussions about privacy concerns. Find out their policies regarding using student data for marketing purposes. Share your data privacy policy with them, and use it to craft vendor contracts and SLAs. 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.

5 **Communicate and educate key stakeholders.** Buy-in from parents, elected officials, board members, and other key community members helps ensure broad acceptance of privacy and security initiatives, and can also help when it's time to request budget dollars. But many don't understand the benefits of using student data for non-commercial purposes such as personalized learning. Educate key stakeholders on the advantages for students, clarify the district's data privacy policy, and emphasize compliance with federal and state laws.

6 **Provide staff training and professional development.** Provide training to staff that handle student data so they understand the issues and challenges associated with accidentally exposing it. They'll also need ongoing training on how to avoid introducing security threats into the school's environment.

Be in the Know: Understanding Privacy Mandates

Several federal and state privacy laws exist to protect student data, but some of them were created at a time when digital education didn't exist. The primary federal mandate, the Family Education Rights and Privacy Act (FERPA), was enacted in 1974 when the internet, data analytics, and cloud-based learning were only a gleam in an engineer's eye. FERPA specifies schools must have written parental and/or student consent prior to disclosing sensitive student data, including personally identifiable data, billing and enrollment information, and educational records.

Other important federal laws governing student data include the Children's Online Privacy Protection Act (COPPA), which outlines how websites must protect the safety and privacy of those under the age of 13; the Health Insurance Portability and Accountability Act (HIPAA), which provides for the confidentiality of health records; and the Protection of Pupil Rights Act (PPRA), which protects students and parents participating in surveys, analyses, or evaluations funded by the U.S. Department of Education.

More recently, state legislatures have been working to modernize their own data privacy laws. In 2014, the state of California enacted landmark legislation that aggressively restricts the use of student data by vendors of online educational services. The Student Online Personal Information Protection Act (SOPIPA) prohibits vendors from selling or revealing personal student information, using their data to market products to them, or creating a student profile based on their information.

After President Obama issued a call for tougher federal data privacy laws in early 2015, federal momentum shifted. With SOPIPA as a model, a series of eight bills aimed at closing privacy loopholes and modernizing FERPA were introduced in the Senate and House. In 2018, the Federal Commission on School Safety called on Congress to modernize FERPA, though skeptics were doubtful the commission's report would carry enough weight to push an overhaul of FERPA through. Though none of the efforts to modernize FERPA have succeeded yet, it's safe to say it may soon be more difficult for vendors to use student data for marketing purposes.

CONCLUSION

Driven by the concerns of parents and privacy advocates, student data protection has become a top priority. Faced with continuing advancement of digital teaching and learning, school districts must effectively manage the privacy and security implications associated with the ensuing avalanche of student information.

As security and privacy concerns evolve, federal and state policies and mandates are also changing to provide specific guidance about collecting, using, and protecting student data. Industry associations and state and federal education agencies can help schools and districts keep track of changes in the regulatory landscape. They offer numerous resources on how to implement security tools and policies flexible enough to accommodate future changes.

By remaining informed about applicable laws and keeping open lines of communication among key community stakeholders and technology vendors, schools and districts can collaboratively develop, maintain, and enforce effective policies and multilayered security programs to protect student data.

RESOURCES

The Consortium for School Networking's (CoSN) Protecting Privacy in Connected Learning Toolkit: http://cosn.org/focus-areas/leadership-vision/ protecting-privacy

CoSN and the Data Quality Campaign's (DQC) 10 Principles to Guide the Use and Protection of Student Data: http://studentdataprinciples.org

The Future of Privacy Forum (FPF) and the Software & Information Industry Association's (SIIA) Student Privacy Pledge: http://studentprivacypledge.org/

Endnotes

[1] The Center for Digital Education surveyed 77 K-12 leaders in February 2019 to gain insights on printing, modernization ,and cybersecurity practices.

[2] 2019 Verizon Data Breach investigation report.

Contact your Canon Solutions America Bid Support team today and help ensure responsible privacy and security practices for your education institution.

Sponsored by:

Canon

CANON SOLUTIONS AMERICA

1-800-815-4000 CSA.CANON.COM

Canon Solutions America offers educational institutions a convenient, cost-effective way to acquire sustainable and secure printing and document management solutions and services. Our advanced technology provides cost-effective document distribution, secure information management, and Managed Print Services resulting in greater productivity for your organization. For more information, call 1-844-50-CANON or visit csa.canon.com. Canon Solutions America does not provide legal counsel or regulatory compliance consultancy, including without limitation, regarding Sarbanes-Oxley, HIPAA, GLBA, FERPA, Check 21 or the USA Patriot Act. Each customer must have its own qualified counsel determine the advisability of a particular solution as it relates to regulatory and statutory compliance. Canon products offer certain security features, yet many variables can impact the security of your devices and data. Canon does not warrant that use of its features will prevent security issues. Nothing herein should be construed as legal or regulatory advice concerning applicable laws.