FROM DEVICE TO DATA:

Creating an Efficient Workflow with Security in Mind in K-12 Education

K-12 school districts store massive amounts of sensitive data — including student grades, health records, and other personally identifiable information (PII). Due to this, they are a prime target for cyber attacks. K-12 institutions must also comply with various state and federal regulations, such as the Family Educational Rights and Privacy Act (FERPA), to protect student privacy. Many schools and districts lack a formal information policy, which can make data vulnerable.

141 K-12 INSTITUTIONS DISCLOSED ONE OR MORE
CYBER INCIDENTS
IN 2016.[1]

74 INCIDENTS
WERE REPORTED DURING THE FIRST 5 MONTHS OF 2017.[2]

SCHOOLS ESTIMATE THE COST OF AN ATTACK AT
$200,000.[3]

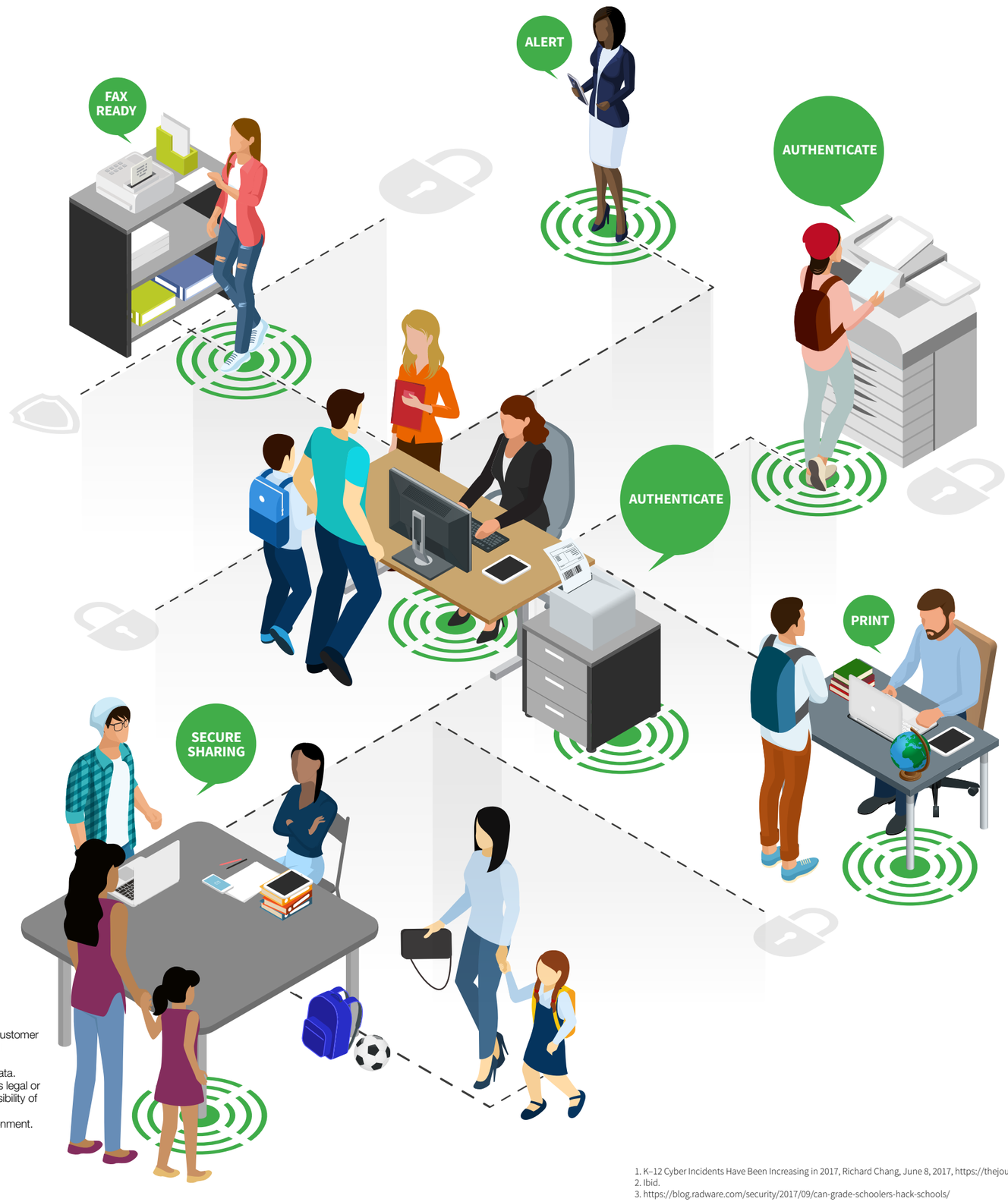
This infographic highlights some common areas of potential vulnerabilities in a typical K-12 digital workflow. It also shows the access controls and security features that can be layered on to help enhance document protection, increase efficiencies, and support compliance obligations — allowing K-12 schools and districts to focus on their core mission of improving student outcomes.

PRODUCED BY

CENTER FOR DIGITAL EDUCATION

SPONSORED BY

Canon



⚠ Layered Security ⚠

Layered security comprises device security, print security, and document security, resulting in a comprehensive approach to protecting student information.

⚠ Automatic Alerts ⚠

An administrator can be alerted should someone attempt to print, scan, or copy sensitive documents that contain keywords (confidential, faculty only, etc.).

⚠ Defense at Device ⚠

Before accessing a device to print, scan, or copy, a teacher can use an authenticated ID card to help gain the appropriate level of access.

⚠ PII Protection ⚠

An administrator can print student grades from a mobile device, which are then held on a server with security features until he or she enters a password at a printer to retrieve them.

⚠ Compliance ⚠

A layered approach to protecting your organization can establish an effective security posture and thus facilitate compliance with regulatory guidelines.

⚠ Collaboration without Complication ⚠

When communicating with teachers, staff, and parents, an enterprise information management solution can enable seamless collaboration among document owners and contributors throughout the document life cycle.

1. K–12 Cyber Incidents Have Been Increasing in 2017, Richard Chang, June 8, 2017, https://thejournal.com/articles/2017/06/08/k12-cyber-incidents-have-been-increasing-in-2017.aspx
2. Ibid.
3. https://blog.radware.com/security/2017/09/can-grade-schoolers-hack-schools/

TO STRENGTHEN DATA PRIVACY, START AT THE PRINTER

How security-focused print management helps K-12 institutions improve data protection practices without burdening users.

Printers remain a necessity in any school district, despite the move toward digital. But if not managed properly, printers can be a significant point of vulnerability. By taking a fresh look at how to manage printers, K-12 schools and districts can help improve data protection and their security practices.

Weak Confidence in Current Security

Given today's growing threat environment, it's vital that district IT staff and leaders have a high level of confidence about the security measures in place for all systems, applications, and devices. Yet only 29 percent of K-12 leaders surveyed by the Center for Digital Education (CDE) are "very confident" their print capabilities are highly secure.[1]

Poor information security can lead to costly consequences — schools estimate the financial cost of a single cyber attack at $200,000.[2]

Implementing redundant data protection by adding security layers for multiple touchpoints and functions — including for printers — in a workflow is critical for all organizations, especially those in education.

Why Strengthen Printer Security?

Education institutions might consider printers a lower priority than other information security investments. The CDE survey found that only about one-third of responding institutions have had discussions or trainings with staff about secure printing.[3]

However, several factors present a compelling case for strengthening security around printers and workflows. The first is that printers and printed documents can be a weak link in an organization's security strategy. According to one security consulting firm, 13 percent of incidents it handled in 2016 involved compromised paper records.[4]

Data breaches in education are not uncommon. In just under 18 months, one or more cyber incidents were disclosed by 141 schools or school districts in the U.S., with 74 of these incidents reported in the first five months of 2017.[5] The disruption of a data breach can be severe, leading to long-term impacts on productivity and a school's ability to thrive in a competitive education environment.

Growth of sensitive data is another concern. As schools continue to transition to online instruction and testing, they will store increasing amounts of personally identifiable information (PII) — an attractive target for cyber criminals.

At the same time, regulations on data privacy are becoming more stringent. Schools and districts may already have to comply with federal regulations for data security, such as the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), and the Children's Online Privacy Protection Act (COPPA). States are also taking a more active role in regulating cybersecurity. Since 2013, states have passed 94 new laws that address the privacy and security of data in education.[6]

Finally, printers today are more sophisticated than in the past. Desktop printers used in the classroom typically perform copy and scan functions. In a school or administration office, a shared printer is likely a network-connected device that communicates with core business applications on district servers or in the cloud.

Recognizing Potential Security Vulnerabilities in Printers

Network-connected printers — especially those that were not designed or configured with external security in mind — can create several types of vulnerabilities. A single printer with a weak administrative password or an open port configuration could potentially be used by hackers to gain entry into a school or district network for data theft, installation of ransomware and malware, or application attack. Hackers may also potentially intercept, without detection, sensitive documents as they are sent by a user to the printer. Confidential personal information, stored in files on the printer's hard drive, may be easy to view and copy — especially if the hard drive is not encrypted or wiped prior to printer disposal.

School and district leaders should be aware of security threats at the device. Even something as simple as leaving documents in an output tray can potentially expose sensitive information. Controls are also essential on printer functions for scanning documents, receiving faxes, or transferring documents to the cloud to reduce the risk of information disclosure and theft.

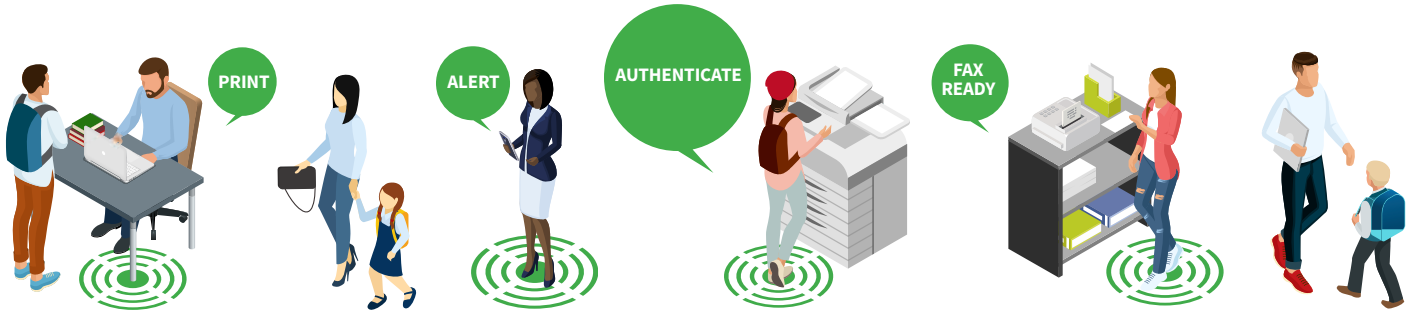
Improving Information Security with Print Management

Effective print management can bring a big benefit to schools and districts: efficient workflows with security features. In turn, this can add transparent layers of protection that enhance other IT and network security measures employed by the school or district.

A print management solution can give IT more control over how information is acquired via printers and then distributed across the internal network, to private cloud

What's in a Print Management Solution?

A print management solution coordinates all the print, scan, fax, and share processes in a school or office.



Access Control

Require user authentication via username and password or access card.

Control user access to authorized content and device functionality via role-based permissions.

Document Security

Protect sensitive data at the device with HDD Encryption and while in transit with Encrypted Secure Print.

Set visual and audible alerts for sensitive documents using control words.

Create an audit trail of user actions with documents.

Data Protection

Erase images when job is complete.

Protect printer passwords and encryption keys with separate, tamper-resistant element.

Wipe data from hard drive and print certification.

Network Security

Prevent data from entering or leaving the network without authorization with secure printing from mobile devices.

Intercept and prevent scans and prints from being sent using control words.

Route incoming faxes to a password-protected network folder before printing.

storage or applications, or to a public internet site. For example, a print management solution can help connect Google Chrome devices and integrate with cloud services such as Google Classroom in K-12 while helping to reduce security vulnerabilities.

Print management tools can also help schools and districts meet regulatory compliance obligations by helping to prevent unauthorized access to student and employee data on printed documents. Features such as authentication require users to verify their identity with a password or access card before a document prints. Predefined user credentials can also be used to restrict access to certain printer functions and document types based on a person's role.

Streamlining Workflows and Productivity

A print management solution can also streamline workflows to improve school or district staff productivity. For example, indexing and metadata features make it easy to search for documents while helping control access to those documents at input, distribution, and output points.

Grading and testing are two areas that can also benefit from improved workflow, particularly when school districts share that information in federal and state reports. With the right print management strategy, districts can improve reporting by reducing repetitive tasks, making the right information accessible to those who need it, and developing consistent reporting processes.

Best Practices for Securing Data with Print Management

- ✓ **Apply management principles and processes consistently across all printers in the district.**
- ✓ **Distribute security policies for your device fleet and monitor the policies continuously.**
- ✓ **Consider how user, device, and application workflows can be modified to help improve security and efficiency.**
- ✓ **Identify the specific information types that need protection and your regulatory obligations for data access and distribution.**
- ✓ **Plan a change management process with ongoing training to continually update users on new security threats and protocols and encourage good practices for protecting information. Many print services or management providers can help schools with this effort.**

Navigating Culture Change

Stronger print management means new user procedures and a culture of security awareness. After all, teachers and school staff may not know the risks involved with printers or how printing may impact their regulatory compliance.

If a school adopts an information security policy without streamlining technology and processes, users will not necessarily embrace the change. Instead, implementing easy-to-understand, seamless, and reliable print management technology can encourage users to safeguard confidential, restricted, and sensitive information, especially personal data.

Simple printing processes and reliable print management technology — as well as the right training and professional development — can support a change in culture. Print management with intuitive security features can encourage teachers, students, and administrative staff to accept new printing processes and printer access requirements. When information security is integrated with printing, it becomes transparent to users and helps them comply with their internal security policies and regulatory requirements.

Simpler Printing, Stronger Security

A print management solution can mean changes to familiar printing tasks. But with the right solution, users will feel the overall process is simple, consistent, and helpful for getting their work done. More importantly, the right solution can help administrators track printing activity and consumables, plan for future implementations based on actual user behavior, improve workflows, and strengthen protection for sensitive data.

Endnotes

1. Center for Digital Education survey of 128 K-12 education decision-makers on print security, 2016
2. https://blog.radware.com/security/2017/09/can-grade-schoolers-hack-schools/
3. Center for Digital Education survey of 128 K-12 education decision-makers on print security, 2016
4. https://www.dataprivacymonitor.com/cybersecurity/deeper-dive-protecting-paper-records/
5. https://thejournal.com/articles/2017/06/08/k12-cyber-incidents-have-been-increasing-in-2017.aspx
6. https://dataqualitycampaign.org/wp-content/uploads/2017/09/DQC-Legislative-summary-0926017.pdf

This piece was developed and written by the Center for Digital Education Content Studio, with information and input from Canon.

PRODUCED BY

CENTER FOR DIGITAL EDUCATION

SPONSORED BY

Canon