FROM DEVICE TO DATA:

Creating an Efficient Workflow with Security in Mind in Higher Education

Colleges and universities store massive amounts of sensitive data — including research studies, student health records, and other personally identifiable information (PII). Due to this, they are a prime target for cyber attacks. Higher education institutions must also comply with various state and federal regulations to protect student privacy, which can further complicate the data protection environment.

IN 2016, THE EDUCATION SECTOR MOVED FROM

THIRD TO SECOND

FOR THE HIGHEST NUMBER OF BREACHES BY INDUSTRY.[1]

THERE WERE

562 REPORTED DATA BREACHES

AT 324 HIGHER EDUCATION INSTITUTIONS BETWEEN 2005 AND 2014, WHICH REPRESENT ABOUT 15.5 MILLION RECORDS.[2]

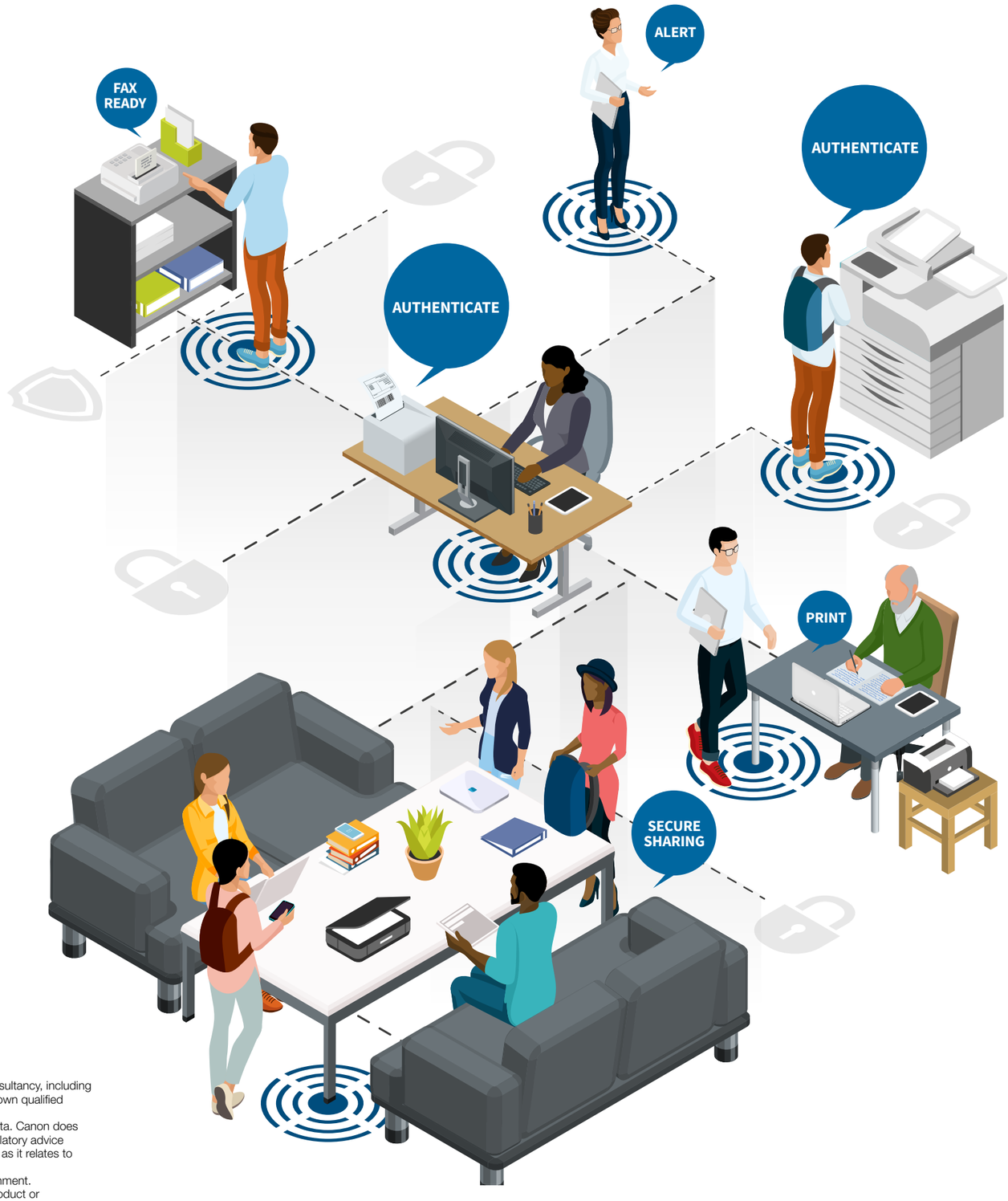
This infographic highlights some common areas of potential vulnerabilities in a typical higher education digital workflow. It also shows the access controls and security features that can be layered on to help enhance document protection, increase efficiencies, and support compliance obligations — allowing colleges and universities 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, an instructor can use a school-issued ID card to help gain the appropriate level of access.

PII Protection

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

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 collaborating with professors, staff, and other stakeholders, an enterprise information management solution can enable a seamless workflow for document owners and contributors throughout the document life cycle.

1. Symantec's 2016 Internet Security Threat Report, https://www.symantec.com/security-center/threat-report 2.Just in Time Research: Data Breaches in Higher Education, https://www.educause.edu/ir/library/pdf/ecp1402.pdf

SECURING INFORMATION IN OVERLOOKED PLACES

Better print management can help higher education institutions improve data protection and efficiency.

Printers are a fundamental tool for academics, administration, and student and staff services on a college campus. But printers can also be a significant point of vulnerability.

By taking a fresh look at print management, higher education institutions can help improve data protection and security practices.

Weak Confidence in Current Security

IT staff and leaders should have a high level of confidence about the security measures in place for all systems, applications, and devices. Yet only 19 percent of higher education decision-makers 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. The cost of a data breach in the education sector is estimated at $200 per record.[2] Additional costs for legal fees, regulatory fines, credit monitoring, IT repair, and other services can reach millions of dollars.[3]

Implementing redundant data protection by adding security layers for multiple touchpoints and functions — including for printers — in a workflow is critical.

Why Strengthen Information Security?

Colleges and universities store two types of information that appeal to hackers. First is the personal data of students, staff, applicants, alumni, parents, researchers, and study participants — including Social Security numbers, financial information, health records, and credentials. Second is intellectual property — research data, software code, and product development information that has significant commercial value.

An analysis of 2016 education breaches found more than half disclosed personal information and just over one-quarter disclosed intellectual property.[4] A breach can be highly disruptive and cause long-term impacts on productivity and a campus' ability to compete.

At the same time, data privacy regulations are becoming more stringent. Higher education institutions may already have to comply with regulations for data security, such as the Health Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry Data Security Standard (PCI-DSS). States are also taking a more active role in regulating cybersecurity. Since 2013, states have passed 94 new laws that address privacy and security of data in education.[5]

Recognizing Potential Security Vulnerabilities in Printers

Higher education institutions might consider printers a lower priority than other information security investments. The CDE survey found that less than half of responding institutions have had discussions or trainings with staff about secure printing.[6]

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 a security consulting firm, 13 percent of the incidents it handled in 2016 involved compromised paper records.[7]

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 be used by hackers to penetrate an institution's network for data or intellectual property theft, installation of ransomware and malware, or application attack. Hackers may also intercept sensitive documents sent to a printer. Confidential personal information stored in files on a 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.

Finally, campus leaders should be aware of security threats at the device. Something as simple as leaving documents in an output tray can expose sensitive information. Controls are also essential 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 institutions: efficient workflows with security features. In turn, this can add transparent layers of protection that enhance IT and network security measures already in place.

A print management solution gives IT more control over how information is acquired via printers and then distributed across the internal network, to private cloud storage or applications, or to a public internet site. For example, IT can manage printing services for students and faculty by applying user authentication according to the institution's printing policy, tracking available printing budgets, and determining information access according

What's in a Print Management Solution?

A print management solution coordinates all the print, scan, fax, and share processes across an institution.

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.

to credentials. This helps protect proprietary information by managing and providing an audit trail for information access and distribution across departments, projects, and research partners.

Print management tools can also help institutions meet their 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 printing a document. 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 staff productivity. For example, indexing and metadata features make documents easy to search while helping control access to those documents at input, distribution, and output points.

Workflows such as admissions, financial aid, and assessments require the ability to capture, move, and collaborate on information. With the right print management strategy, institutions can help improve collaboration by reducing repetitive tasks, making the right information accessible to those who need it, and developing consistent, secure processes for information sharing.

Navigating Culture Change

Stronger print management means new user procedures and a culture of security awareness. After all, students, faculty, and staff may not understand the risks involved with printers or how printing impacts regulatory compliance.

Best Practices for Securing Data with Print Management

- ✓ **Apply management principles and processes consistently across all printers in the institution.**
- ✓ **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 (including intellectual property) and regulatory requirements 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 campuses with this effort.**
- ✓ **Look at how print management can improve the availability of on-campus printing services, especially for students.**

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

Print management with intuitive security features can encourage faculty, students, and staff to accept new printing processes and printer access requirements. When information security is integrated with printing, it becomes transparent and helps users comply with the institution's information security policies and government regulations.

Training and professional development are also important to promote culture change and successfully adopt a print management solution. CDE found that only about half of institutionssurveyed offered discussions, training, or alerts to staff about secure printing.[8]

A Strategy for Better Security and Better Work

Security vulnerabilities will only continue to grow. By taking a proactive and strategic approach to print management, higher education institutions can create vital redundancies in security measures. In doing so, they can also improve workflows for more effective academic and administrative work.

Endnotes

1. Center for Digital Education survey of 162 higher education decision-makers on print security, 2016
2. https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN&
3. https://www.universitybusiness.com/article/0816-wisp
4. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/
5. https://dataqualitycampaign.org/wp-content/uploads/2017/09/DQC-Legislative-summary-0926017.pdf
6. Center for Digital Education survey of 162 higher education decision-makers on print security, 2016
7. https://www.dataprivacymonitor.com/cybersecurity/deeper-dive-protecting-paper-records/
8. Center for Digital Education survey of 162 higher education decision-makers on print security, 2016

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