DOCUMENT AND PRINT SECURITY: MITIGATING THE POSSIBILITY OF MURPHY'S LAW

The introduction of the GDPR (General Data Protection Regulation) and the proliferation of U.S. based privacy laws regarding personal information ensures that data security remains top of mind among law firms as well as businesses of all kinds. According to public disclosure records for breaches reported from 2007-2019, almost half of all law firm breaches (45%) are a result of external breaches such as hacking, phishing, or vendor incidents.[1]

Law firms are prime targets for malicious attacks because of the wealth of sensitive information they handle, from client trade secrets and details on mergers and acquisitions to litigation strategy, attorney-client privileged information, and personally identifiable information.

Unfortunately, due to a lack of time or resources, many firms continue to take an IT-centric approach to security tasks. Creating and enforcing policies and conducting risk assessments and audits can only go so far in mitigating your firm's risk of a security breach, because it is impossible to secure your data when you don't know what you have.

Effective and comprehensive information governance is the precursor to more successful security planning.

Your overall document management strategy should incorporate understanding the nature of the structured and unstructured data that lives in your firm and within cloud-based applications; developing policies for data retention, remote access, BYOD (bring your own device) and disaster recovery among others; and controlling access to sensitive information.

Closing the gap in document management

As document management becomes integral to the development of critical security initiatives, law firms must accurately assess their risk. To start, build a well-documented and detailed strategy for print security and management. A comprehensive plan identifies all potential sources of information leaks and should track normal workflows. To ensure that the plan meets the needs of the modern law firm, it should address both mobile and in-office print management. The firm should also implement systems that can deliver detailed usage metrics and management reporting; this data can be used to validate compliance and satisfy audit demands. Sophisticated tracking can help identify any discrepancies that indicate information loss or control issues.

It is important to develop a plan with a keen eye toward how it can best serve the firm and its staff. If the plan creates onerous policies or requirements that negatively impact productivity or profitability, users won't implement them consistently. If the revised security plan is too complex, staff will default to their own "workarounds" that may reintroduce security issues, effectively negating the effort spent to develop the plan.

Help ensure that network-connected printers don't create vulnerabilities

Increasingly, multifunction devices (MFDs) are fully functional computers that have print, scan, copy, and fax abilities as well as an email platform, cloud connectivity, local storage, wireless networking, and an operating system. While this is a major convenience for law firm staff as they more efficiently digitize their processes, it can be a potential security nightmare. A quick internet search reveals multiple examples of hackers who infiltrate internet-connected printers just for fun or to maliciously disable MFDs in exchange for a ransom. Effective management of endpoint devices such as MFDs requires IT professionals to have visibility over their multifunction devices, and the ability to respond to suspicious events in real time and empower the applications to automatically restore themselves when incidents occur.

5 best practices for establishing and maintaining improved information security

1 **Device Security** — Securing information at the device is a starting point. User authentication should be required for printing, copying, and scanning. It allows your administrator to monitor, measure, and report on how staff utilizes the devices and services—critical information if an issue arises. Policies can also assign specific document printing and management privileges to each user, based upon their role within the firm. Some users or guests may have access to very basic functionality, while partners would get more privileges. The system can then identify and document normal usage patterns, making it easier to rapidly identify outliers and examine individual events for a potential breach.

The authentication solution should support numerous methods for verifying the user, including PIN, password, employee badge, or other token/physical object. Administrators should be verified before accessing settings or the device's address book.

Device-specific security features should also be part of the solution. The system should support functions beyond usage tracking and privileges. Some examples of this include restricted access to the device's USB port or using secure, password-protected printing. It is important to be able to verify the security and integrity of any third-party software used on the device in order to help prevent malicious use or the introduction of malware.

These authentication tools must work with other identity management tools frequently used at law firms, one of the most common of which is Microsoft's Active Directory (AD). Finally, whether a firm has just a few MFDs or a hundred, the organization should have a single point of device management. This helps ensure that all activity is tracked and monitored. A centralized management console lets the administrator troubleshoot, identify unauthorized access, update user credentials, and perform other tasks to help ensure secure MFD use.

Your security and IT team need to have visibility into the infrastructure to stay aware of any perimeter and end-point security failures or anomalies that may indicate malicious activity. Deploying a security information event management (SIEM) system can aggregate security data from across your organization, help security teams detect and respond to security incidents, and create compliance and regulatory reports about security-related events.

2 **Print Security** — Much of the data that moves throughout organizations is still paper-based. The next logical progression after securing printers and a multifunctional device fleet is to secure the output of those devices. Closing security gaps in your printing and imaging environment is an important piece of your overall security strategy. There are key features and functionality embedded in many print management solutions that can aid you in your security journey such as user authentication, pull printing, watermarking, keyword intercept, auditing, and device personalization.

Be sure to consider unauthorized reproduction security as well. As production printing migrates more and more from traditional analog offset print processes into the world of digital high-speed variable print processes, so must the security features used to secure crucial hard copy documents and documents with intrinsic value. Whether you need to prevent altering and copying-and-pasting from a digital document, or photocopying a hard copy original, the need for protection is paramount. You can help address your clients' concerns by demonstrating your ability to offer a variety of solutions to help protect their intellectual property and sensitive data.

3 **Document Security** — Information is one of your organization's most valuable assets and, as with any asset, it should be thoroughly protected, meticulously

managed, and easily accessible. However, as your organization grows, so does your volume of information. This can quickly become cumbersome, especially when employees apply their own disparate filing methods.

Protecting sensitive data both in transit and at rest is imperative for modern organizations as attackers find increasingly innovative ways to compromise systems and steal data. An enterprise content management (ECM) solution with a secure repository can help protect your information throughout the entire document lifecycle with system permissions that restrict unauthorized access to document repositories, customizable access permissions for specific content and data, anti-tamper measures to ensure document authenticity, automatic document back-up for disaster recovery, audit trail for tracking user and document activity, regular penetration testing, and automated retention policy configuration.

Furthermore, with the advent of international and domestic privacy regulations such as the EU General Data Protection Regulation (GDPR) and California's Consumer Protection Act (CCPA), an ECM solution can provide comprehensive eDiscovery capabilities in the event of a Subject Access Request (SAR) by a client or opposing counsel who either wants to verify what personally identifiable information (PII) your firm maintains, or wants to exercise their right to be forgotten.

Additionally, comprehensive ECM solutions can provide document governance and data classification as enhancements with access controls.

4 **Information Security** — What happens to information once it travels beyond an organization's walls? Most law firms, regardless of size, focus on protecting the perimeter through firewalls and the inside with malware and virus protection solutions, but few make the effort to protect their files when they travel outside of the organization through sharing and collaboration.

Seek out solutions that allow document owners to limit access through cloud-based encryption keys and set parameters around access privileges, editing rights, availability time frame, real-time revocation, audit trails that can't be edited, and global file tracking.

A complete security policy includes not only the device, but also information and data. A solution that requires users to be physically present at the MFD in order to print their documents can help ensure document and data integrity and reduce the threat of lost data or breaches. Pull-printing technology and secure "mailboxes" on each MFD can also enhance information security. These technologies help to ensure that documents can only be printed after the user authenticates and is present at the device to retrieve the documents.

Because many MFDs contain internal hard drives, print jobs should be encrypted and hard drive data should be password-protected. A complete solution helps ensure secure data deletion as well. A Trusted Platform Module (TPM) chip that stores passwords, encryption keys, and other sensitive data outside the hard drive can also enhance security. Other security features include secure watermarking, which embeds specific text that is only visible if a document is photocopied. It is also possible to embed tracking information that only administrators can see. Digital signatures are another common way to verify authenticity.

5 **Cybersecurity** — With the help of cybersecurity services providers, customers can help to secure their business without feeling like they must do it alone. It's important to work with a company that can help provide the human resources with top level skills to collaborate with you in developing a successful security posture.

Consider the addition of cyber etiquette training for your employees, virtual CISO (Chief Information Security Officer) services, and guidance with compliance efforts. Look for security provider experts who can conduct vulnerability assessments, penetration testing, consultation, training and awareness, incident response, and application testing.

Failure to evaluate and mitigate the vulnerabilities in your organization can cost you plenty in money, lost time, reputation, and loss of valued customers. Awareness training, due care, and due diligence are table stakes in sustaining the health of your business. Ask us how we can help you get started.

People—your weakest link or your best defense? Leverage phishing simulation training as a human firewall

Social Engineering has been the culprit of some of the most catastrophic data breaches to date. It has never been more critical to create awareness of this threat vector and to educate your personnel to not fall prey to phishing and pretexting as email has become weaponized and the medium of choice for malicious cybercriminals.

Deploying a phishing simulation platform in your organization can provide a flexible and consistent way to modify, test, and measure employee behavior with electronic communications. You can convert potential risk takers into front-line defenders. Using AI and machine learning to identify, flag, and quarantine potential phishing emails that are already living in user inboxes can further mitigate the risks of social engineering campaigns.

Canon Solutions America's approach to the document security problem

Canon Solutions America is committed to serving the legal community by helping firms evaluate their document processes and improve workflow efficiency, introduce business process automation, and strengthen IT infrastructure. Our extensive experience with cost recovery, security, and document distribution has helped rank Canon as a hardware and software solutions leader in the legal market. At the 2019 ASTORS Homeland Security Awards, Canon won the Platinum award for five MFD security solutions.[2]

Canon Solutions America's industry insight and experience can streamline your law firm's everyday work processes, provide enhanced security to protect against unwarranted breaches, and deliver innovative mobile solutions to address the emerging needs of today's evolving legal workforce.

Canon Solutions America's portfolio of hardware and software solutions and services can significantly reduce IT burden and strengthen your law firm's security posture:

- **Comprehensive Device Security** — The 3rd Edition of Canon's award-winning imageRUNNER ADVANCE series sports numerous security features out of the box including HDD Data Erase, HDD Data Encryption, Secure Watermark, SIEM Integration, Auto Certificate Update, Encrypted PDF, Encrypted Secure Print, and an Access Management System that controls access to device functionality based on roles. imagerRUNNER ADVANCE devices also feature Verify System at Startup that runs a process during startup to ensure that no tampering of the bootcode, OS, firmware and MEAP applications has occurred. If tampering does occur, the system will not start. Finally, McAfee Embedded Control allows only known programs contained in a dynamic whitelist to be executed on the MFD. Programs not listed in the whitelist are considered unauthorized and will not be permitted to execute.
- **Flexible Security Solutions** — Canon devices offer seamless integration with numerous industry leading software solutions that support secure collaboration, encrypted workflows, trackable audit trails, and the ability to grant and revoke access to files that have been copied, forwarded, downloaded or shared online, among others. In addition, Canon's proprietary one-platform solution, uniFLOW, helps law firms efficiently secure client data/documents, manage mobile access, print securely, and improve workflow while providing valuable analytics on printer usage and costs. Our software offerings are backed with implementation services performed by certified professionals with extensive experience in integrating Canon Solutions America offerings with existing Line of Business applications.
- **Cybersecurity Services** — Canon Solutions America cybersecurity partners are industry leaders with extensive experience in providing cybersecurity and phishing training and services ranging from identifying, tracking, and quarantining suspicious emails to conducting vulnerability assessments, penetration testing, and Virtual CISO duties. Learn more about our security capabilities at ***csa.canon.com/security***.

SUMMARY

Many information security plans have left MFDs and printed material on the backburner for far too long. However, as law firms begin to understand the extent of the problem, the idea of better document and printer management has started to receive greater attention. The good news is that the right plan, along with targeted solutions, can help reduce many of the vulnerabilities associated with printing, scanning, and faxing. With the benefit of Canon Solutions America's experience and expertise in print management, law firms can effectively eliminate the vast majority of today's print/output security risks. As compliance, audit, and privacy demands begin to include secured output, now is the time for law firms to implement effective solutions.

Endnotes

[1] *Law.com 2019 investigation of law firm breach reports from 12 states. https://www.law.com/2019/10/17/how-vendor-data-breaches-are-putting-law-firms-at-risk/.*

[2] *The 2017 ASTORS Homeland Security Awards Program, American Security*

Canon

CANON SOLUTIONS AMERICA

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

Canon Solutions America does not provide legal counsel or regulatory compliance consultancy, including without limitation, Sarbanes-Oxley, HIPAA, GLBA, 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; customers must have their own qualified counsel determine the feasibility of a solution as it relates to regulatory and statutory compliance. Some security features may impact functionality/performance; you may want to test these settings in your environment. Neither Canon Inc., Canon U.S.A., Inc., nor Canon Solutions America, Inc. represents or warrants any third-party product or feature referenced hereunder. All screen images are simulated.

Canon is a registered trademark of Canon Inc. in the United States and elsewhere. All other referenced product names and marks are trademarks of their respective owners and are hereby acknowledged.

©2020 Canon Solutions America, Inc. All rights reserved.

01/19-1046-3960