Canon

CYBERSECURITY SERVICES FOR LAW FIRMS

Tackling Cyber-Attacks Can Be a Team Effort

Today's law firms have a security problem. According to the American Bar Association, while 80% of surveyed law firms indicate they have security policies in place around technology governance, only about one-third have conducted a full security assessment performed by a third party.[1]

Clearly, legal practices have much at risk in the event of a security breach, ranging from lost business and client confidence to reputation damage and, increasingly, the possibility of being on the wrong end of a class action lawsuit. Unfortunately, while the stakes are high, law firms are stretched dealing with a multitude of potential cyber threats including:

Social Engineering Attacks
Emails, fake URLs and identities, "urgent" phone calls, and other deceptive practices designed to lure unsuspecting employees into divulging confidential information. These are gaining even greater traction with the aid of artificial intelligence.

Ransomware Threats
Bad actors that access mission-critical information and hold it hostage in return for payment.

Insider Threats
Employees who unwittingly or deliberately put data at risk by sharing information through unsecured applications or providing unmanaged access to sensitive documents.

Legacy Technology
Outdated patches, devices, and software updates that may lead to network vulnerabilities which are exploited by hackers to gain unauthorized access to rich stores of valuable practice data.

Denial-of-Service (DoS) Attacks
Cyber-attacks motivated by greed, revenge, activism, or competition that are designed to crash law firm systems or prevent lawyers from delivering typical services. Sometimes these involve multiple machines joining forces to create a Distributed Denial-of-Service (DDoS) attack.

Advanced Persistent Threats (APTs)
Prolonged and targeted cyber-attacks launched by adversaries with significant resources and expertise. The advanced persistent threat pursues its objectives repeatedly over an extended period, adapts to defensive measures, and is laser-focused on the level of interaction needed to execute its objectives.

[1] *American Bar Association 2023 CyberTech Security Report. Available from: 2023 Cybersecurity TechReport (americanbar.org)*

With so much at stake, and so many responsibilities, technology managers are challenged to monitor the evolving threat landscape, mitigate risk, and manage a multitude of other priorities related to improving operational efficiencies at law firms.

To effectively reduce risk and proactively protect valuable data, legal firms can turn to Canon U.S.A. to gain access to teams of cybersecurity professionals with a wide breadth of industry-wide knowledge in areas such as:

Email Protection and Incident Response

Through Barracuda Email Protection, Canon U.S.A. offers security awareness training as well as impersonation and domain fraud protection and the option to include incident response. These services teach users to understand and respond correctly to the latest phishing techniques, recognize subtle phishing clues, and prevent email fraud, data loss, and brand damage. And they provide real-time email protection utilizing artificial intelligence, deep integration with Microsoft 365, and brand protection via a cloud-based solution that protects against business email compromise, account takeover, spear phishing, and other cyber fraud.

Fleet Management

Canon U.S.A. offers Symphion's specifically designed turnkey Printer Fleet Cybersecurity as a Service (PFCaaS) solution to tackle an often-unaddressed gap in cybersecurity within many law firms today—printers and multifunctional devices. PFCaaS is the only device agnostic printer security management solution in the industry for firms with hybrid fleets (any brand, any model, any age) in single or multiple locations. Symphion evaluates current security configurations, identifies an appropriate security configuration "Gold Standard" for each business environment, and tests each configuration to help prevent interruptions in use. Because PFCaaS is a concierge service, law firm IT staff are free to focus on core techonology issues.

Managed Detection and Response

Managed Detection and Response (MDR) is a 24/7/365 service that combines continuous monitoring of an organization's digital assets with an "always-on" certified incident response team to help defend your network to first prevent, and ultimately to respond to, a cyber-attack.

Canon U.S.A. works with Rapid7 MDR to leverage seven detection methodologies: threat intelligence, proactive threat hunting[2], Network Traffic Analysis, Network Flow data[2], deception technologies, User Behavior Analytics, and Attacker Behavior Analytics derived from monitoring millions of endpoints. This threat intelligence is automatically applied to your law firm's data to continuously monitor, validate, and respond to potential threats.

Take the next step in protecting your sensitive data by enlisting the Canon U.S.A. team to help you stay a head of cybersecurity challenges. Contact your Canon U.S.A. sales representative or call 1-844-50-CANON to learn more about our cybersecurity services.

[2] Only available to MDR Elite customers.

Canon

1-844-50-CANON

usa.canon.com/security

Canon U.S.A. 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.

Canon U.S.A., Inc. is compensated to refer prospective customers to our cybersecurity providers (“Provider”). Customer acknowledges and agrees that: (i) Provider will provide products and services to you pursuant to an agreement between you and Provider; (ii) Canon U.S.A., Inc. shall have no obligation or liability therefore; (iii) you shall look solely to Provider as to any claim or cause of action arising from such products and services, or your agreement with Provider; and (iv) you waive your rights to bring any such claim or cause of action against Canon U.S.A., Inc.

Neither Canon Inc., nor Canon U.S.A., Inc., represents or warrants any third-party product or feature referenced hereunder. Canon is a registered trademark of Canon Inc. in the United States and may also be a registered trademark or trademark in other countries. All other referenced product names and marks are trademarks of their respective owners. Specifications and availability subject to change without notice.
Not responsible for typographical errors.