Kiteworks

Legal/Law Firms: 2023 Sensitive Content Communications Privacy and Compliance

Industry Findings and Takeaways

HIGHLIGHTS

Communication Tools in Use	**1.5%**	6+
	50%	5
	54.5%	Less than 4
Average Annual Budget for Communication Tools	**13.4%**	$250,000+
	46.3%	$150,000 – $249,999
	40.3%	$100,000 – $149,999
Number of Third Parties With Which They Exchange Sensitive Content	**95.5%**	1,000 – 2,499
	3%	500 – 999
	1.5%	Less than 499
Attack Vector Weighted Score (based on ranking)	**100**	Rootkits
	97	Password/Credential Attacks
	86	Malware (ransomware, trojans, etc.)
	79	Zero-day Exploits and Attacks
	77	SQL Injection
	67	URL Manipulation
	64	DNS Tunneling
	64	Cross-site Scripting
	59	Session Hijacking
	50	Denial of Service
	50	Insider Threats
	42	Phishing
	36	Man in the Middle
Exploits of Sensitive Content Communications in Past Year	**1.5%**	7+
	41.8%	4 – 6
	47.8%	2 – 3
	9%	1
Level of Satisfaction With 3rd-party Communication Risk Management	**18%**	Requires a New Approach
	34%	Significant Improvement Needed
	31%	Some Improvement Needed
	16%	Minor Improvement Needed

Cybersecurity: The Soft Underbelly of the Legal Industry

Cybersecurity remains one of the most challenging issues faced by the legal industry. The protection of confidentiality is a critical concern for legal departments, law firms, and the courts. One of the reasons for the heightened vulnerability of law firms is that cybercriminals have identified them as lucrative and relatively easy targets: 27% of law firms encountered security breaches in 2022, and 46% of attorneys acknowledged their firms having a cyber-liability insurance policy.[1] Lax security and governance are two of the reasons for these alarming numbers. For example, one study found that less than half of law firm respondents in a survey utilize file encryption (43%) and only 40% use two-factor authentication and intrusion detection.[2]

Proliferation of Communication Tools Creating Vulnerabilities

Kiteworks' 2023 Sensitive Content Communications Privacy and Compliance Report found that law firms, as compared to other industry sectors, do not use as many communication tools, though 50% still use five or more. This is likely related to the size of their organizations compared to other industry respondents (hundreds or a few thousand employees compared to tens of thousands by others). Introducing numerous communication tools expands the attack surface for cybercriminals. Each toolset represents a potential entry point for malicious activities, increasing the likely attack vectors like malware distribution or phishing, which were among the top cybersecurity exploits with scores of 27% and 14%, respectively. Further, policy management and reporting across disaggregated toolsets is virtually impossible, which concurrently ratchets up security and compliance risks for legal firms.

Risk of Third-party Content Communications

Email stands out as the communication channel with the highest risk within law firms. 18% gave it a number one rank, followed by file sharing and mobile apps, which both received 15% of number one ranks. Despite its widespread use and convenience, email is an easy cyber target—from social engineered to vulnerability attacks—that can expose sensitive information to potential cyber threats. For law firms that rely heavily on email for client communication, sharing of legal documents, and conducting business transactions, this can pose a serious risk.

Heightened awareness is necessitated based on survey findings. Only 4.3% of legal industry respondents—the fewest of all industries included in the

91% of law firms experienced 2 or more sensitive content communications exploits in the past year.

39% of respondents indicated their law firms needed significant improvement in how they measure security risk for sensitive content communications.

survey—said they manage or restrict third-party access to folders using digital rights management capabilities like content permissions, expiration, locking, and versioning. Similarly, only 7.5% of law firms track and record third-party access to sensitive files and folders. These two findings alone should give law firm partners legal palpitations.

Better Digital Risk Management Required

One outcome from the above is that digital rights management should be critical for the legal industry that must protect sensitive data, maintain compliance with regulations, facilitate secure collaboration with external parties, and enhance internal efficiency. However, it is troubling that only 7.5% of law firms track and record all instances of third-party access to sensitive files and folders across all departments. This was very low compared to the other industries. And while 16.5% acknowledged they do track and record third-party access, this practice is inconsistently applied, implying the need for greater consistency and standardization in their digital rights management protocols. Finally, 10.5% of the law firms indicate they lack centralized content communications controls with third parties, reflecting a gap in their overall approach to safeguarding sensitive information. Inadequate security and compliance governance in legal firms are a red flag for both themselves as well as their clients that entrust them with highly sensitive content. Respondents ranked employing least-privilege access as their top choice when it comes to protecting these sensitive communications.

Kiteworks and Sensitive Communications for Legal

Controlling and tracking access to highly sensitive client information is mission critical for law firms. Clients place immense trust in their attorney relationships and expect their private data to remain private—whether due to inadvertent or malicious exposure. FedRAMP Authorized and ISO 27001, 27017, and 27108, SOC 2, and FIPS 140-2 certified, Kiteworks provides law firms with the ability to send, share, receive, and store sensitive content easily, securely, and compliantly. Further, Kiteworks seamlessly integrates with iManage, providing law firms with a centralized zero-trust policy management platform for secure and compliant sensitive content communications.

[1] "2022 Cybersecurity Tech Report," American Bar Association, 2022.

[2] "TechReport 2020: Cybersecurity," ABA Tech Report, October 2020.

Get the Full Report

Kiteworks

Kiteworks 2023 Sensitive Content Communications Privacy and Compliance Report

Seeking to empower private and public sector organizations to manage their file and email data communication risks better, Kiteworks began publishing an annual Sensitive Content Communications Privacy and Compliance Report in 2022. Rogue nation-states and cybercriminals recognize the value of sensitive content and target the communication channels used to send, share, receive, and store it—email, file sharing, managed file transfer, web forms, APIs, and more.

The 2023 Sensitive Content Communications Privacy and Compliance Report surveyed 781 IT, security, risk, and compliance professionals across numerous industries and 15 different countries. The in-depth report, which is based on their survey responses, explores a range of issues related to file and email data communication risks—how organizations are addressing those today and plan to do so in the coming year. The analysis includes a look back to 2022 data and what changes were observed in 2023.