Kiteworks

2024 Analysis of Sensitive Content Communications in the Legal Sector: Security and Compliance Trends

HIGHLIGHTS

Communication Tools in Place	20%	7+
	15%	6
	25%	5
	20%	4
	15%	3
	0%	2
	5%	1
Exchange Sensitive Content With Third Parties	5%	Over 5,000
	35%	2,500 to 4,999
	20%	1,000 to 2,499
	15%	500 to 999
	25%	Less Than 499
Data Types Biggest Concern (Top 3)	71%	Financial Documents
	58%	Legal Communications
	42%	GenAI LLMs
	33%	IP
	29%	M&A
	25%	PHI
	25%	CUI and FCI
	17%	PII
Biggest Privacy and Compliance Focus (Top 2)	40%	GDPR
	40%	U.S. State Privacy Laws
	30%	HIPAA
	30%	SEC Requirements
	30%	Country-specific Data Privacy Laws
	20%	CMMC
	10%	PCI DSS
Most Important Security Validations (Top 2)	55%	NIST 800-171/CMMC 2.0
	50%	IRAP (Australia)
	35%	ISO 27001, 27017, 27018
	30%	FedRAMP Moderate
	25%	SOC 2 Type II
	5%	NIS 2 Directive
Number of Times Experienced Sensitive Content Communications Hack	20%	7 to 9
	20%	4 to 6
	40%	2 to 3
	15%	1
	5%	Don't Know

The 2024 Kiteworks Sensitive Content Communications Privacy and Compliance Report provides an in-depth analysis of the challenges and trends in managing sensitive content across various industry sectors, including legal. This brief focuses on the key findings related to the legal sector, highlighting the tools used for sensitive content communications, cybersecurity concerns, third-party communication risks, specific cyber threats, and compliance implications.

Managing All the Sensitive Content Communications Tools

60% of legal firms rely on five or more communication tools to send and share sensitive content, which is more than the full cohort average (53%). When it comes to tracking and controlling sensitive content, 60% of law firms said they can track and control sensitive data sent and shared internally, whereas 45% indicated they can do so when it is exchanged externally. Both are slightly better than the full respondent averages of 51% and 43%, respectively.

When it comes to sensitive content communications privacy and compliance priorities, preventing leakage of confidential IP and corporate secrets was by far the highest priority for legal respondents (75% listed it as either their top priority or second-highest priority). This was the highest of any industry sector and much higher than the full cohort percentage (56%). Avoiding regulatory violations and associated fines and penalties and mitigation of lengthy and expensive litigation were tied for the second-highest priority (45%).

Assessing the Third-party Risk of Sensitive Content

Managing third-party risk is an important priority for legal firms, with 40% reporting they exchange sensitive content with over 2,500 third parties (lower than the global cohort at 44%) and 60% doing so with more than 1,000 third parties (slightly less than the full respondent average of 66%). When it comes to tracking and controlling sensitive content once it leaves an application, legal is one of the more mature industry sectors with 60% indicating they can track and control over three-quarters of sensitive content when it leaves an application.

Assessing the State of Sensitive Content Compliance

75% of legal firms revealed their measurement and management of compliance for sensitive content communications requires some to significant improvement. This was less than what all respondents reported: 88%.

GDPR and new U.S. state privacy laws were ranked first or second by legal respondents 40% of the time. HIPAA, SEC requirements, and country-specific data privacy laws were tied at 30%. The emergence of different U.S. state laws makes it increasingly more difficult to conduct business between different states, especially with variance existing between each of these new state laws. With law firms dealing with a global clientele with operations around the world, the highest percentage of legal respondents listing country-specific data privacy laws makes sense.

When it comes to vetting and selecting security validations or certifications, legal firms listed NIST 800-171 as the first or second priority by 55% of the respondents. This was followed with 50% listing IRAP as first or second. As most legal firms conduct business directly with federal government agencies or their clients do so, this finding is not a huge surprise (much higher in both instances than the full global cohort).

Assessing the Risk of Sensitive Content Security

80% of legal firms indicate their measurement and management of security risk associated with sensitive content communications requires significant or some improvement; 20% said they require no improvement. The latter is higher than most other industry segments. But as the data breach data reveals, simply having a higher confidence level does not equate to lower risk.

40% of legal firms revealed their sensitive content was breached four or more times (20% said seven times or more). These are lower than the cross-industry cohort where 32% admitted to seven or more data breaches and 55% said they had four or more. In addition, 5% of legal respondents said they were not certain how many data breaches their organizations experienced.

Advanced security capabilities and practices such as encryption, multi-factor authentication, and governance tracking and control are only used for some sensitive content sent 50% of the time internally and 45% of the time externally. While this is better than the full cohort (39% and 38% respectively), significant areas of improvement remain.

Assessing the Cost of Security and Compliance

When it comes to litigation costs, the survey found 45% of legal respondents indicated they spend over $3 million annually. This is the same as the global average. 10% of legal firms admitted they do not know their annual data breach litigation costs.

Knowledge and Categorization of Data Types

55% of legal firms indicated they tag and classify over three-quarters of unstructured data; this is slightly less than the full number of respondents where 58% admitted the same. When asked how much of their unstructured data needs to be tagged or classified, 60% said 40% or more—which may reveal why the numbers are lower on what is tagged and classified.

Imperative for Robust Sensitive Content Management in the Legal Sector

The Kiteworks 2024 Sensitive Content Communications Report highlights the critical need for robust management of risk and compliance in sensitive content communications in the legal sector. Legal respondents listed financial documents as their top data-type concern (71%) followed by legal communications (58%). This is a bit of a surprise, as one would assume legal communications would have been their top concern. Accordingly, both are higher than the full cohort ranking where financial documents were listed 55% of the time and legal communications 44% of the time.

Operationally, legal firms spend a lot of time managing logs generated by the numerous communication tools they use to share and send sensitive content. 30% of respondents must reconcile over 11 (though lower than the 48% average of all respondents); 15% of legal respondents did not know how many logs must be reconciled. This compiles into a huge report logjam; 45% spend 2,000 hours or more annually while 75% spend over 1,500 hours.

Get Full Report

Kiteworks

Kiteworks' mission is to empower organizations to effectively manage risk in every send, share, receive, and save of sensitive content. The Kiteworks platform provides customers with a Private Content Network that delivers content governance, compliance, and protection. The platform unifies, tracks, controls, and secures sensitive content moving within, into, and out of their organization, significantly improving risk management and ensuring regulatory compliance on all sensitive content communications.