Kiteworks

2024 Analysis of Sensitive Content Communications in Professional Services: Security and Compliance Trends

HIGHLIGHTS

Communication Tools in Place	19%	7+
	21%	6
	19%	5
	21%	4
	16%	3
	3%	2
	1%	1
Exchange Sensitive Content With Third Parties	22%	Over 5,000
	29%	2,500 to 4,999
	21%	1,000 to 2,499
	16%	500 to 999
	12%	Less Than 499
Data Types Biggest Concern (Top 3)	49%	Legal Communications
	44%	Financial Documents
	43%	PHI
	42%	PII
	41%	IP
	38%	GenAI LLMs
	31%	CUI and FCI
	12%	M&A
Biggest Privacy and Compliance Focus (Top 2)	41%	U.S. State Privacy Laws
	40%	HIPAA
	34%	GDPR
	33%	SEC Requirements
	21%	CMMC
	19%	Country-specific Data Privacy Laws
	12%	PCI DSS
Most Important Security Validations (Top 2)	47%	SOC 2 Type II
	45%	NIST 800-171/CMMC 2.0
	43%	ISO 27001, 27017, 27018
	36%	IRAP (Australia)
	21%	FedRAMP Moderate
	8%	NIS 2 Directive
Number of Times Experienced Sensitive Content Communications Hack	12%	10+
	22%	7 to 9
	26%	4 to 6
	17%	2 to 3
	14%	1
	9%	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 professional services. This brief focuses on the key findings related to professional services, 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

59% of professional services firms have more than five communication tools to send and share sensitive content, which is higher than the full cohort average (53%); 40% rely on six or more communication tools. When it comes to tracking and controlling sensitive content, professional services was one of the most mature; 71% reported they can track and control sensitive content when it leaves an app.

Assessing the Third-party Risk of Sensitive Content

Due to the large number of third parties with which professional services companies send and share sensitive content, the risk of a third-party data breach is higher for professional services than most other industry sectors; 47% said they exchange sensitive data with 2,500 or more third parties (68% exchange with over 1,000). These numbers are significantly greater than the full cohort; 27% said they exchange sensitive content with 2,500 third parties and 54% indicated they do so with 1,000 third parties. The fact that tracking and control of sensitive data inside and outside organizations is problematic for many organizations makes it even more difficult to manage.

Assessing the State of Sensitive Content Compliance

96% of professional services respondents revealed their measurement and management of compliance for sensitive content communications requires some to significant improvement. This was significantly more than what all respondents reported: 88%.

Due to the breadth of cross-industry interactions conducted by professional services firms, the regulatory environment most certainly has a significant impact on them. Several compliance and data privacy regulations found their way to the top of the list of regulatory priorities of professional services firms; 41% listed the new U.S. state data privacy laws, 40% said HIPAA, 34% indicated GDPR, and 33% said SEC regulations.

The same close grouping of answers occurred with questions around security standards and validations: 47% listed SOC 2 Type II, 45% said NIST 800-171/CMMC 2.0, and 43% identified ISO 27001, 27017, and 27018 as one of their top two security validation and certification priorities.

Assessing the Risk of Sensitive Content Security

94% of professional services respondents indicated their measurement and management of security risk associated with sensitive content communications requires significant or some improvement, a significantly higher rate than the full cohort average (88%).

34% of professional services respondents reported their sensitive content was breached seven or more times. This is slightly higher than the full cohort average of 32%.

Use of advanced security tracking, control, and security is prevalent among professional services firms; 71% said they can track and control sensitive content when it is shared internally, while 60% said they can do so when it is sent or shared externally. This level of maturity here may reflect the significantly higher level of confidence in their ability to mitigate security risk (see above).

The same could be said about survey findings on the amount paid in data breach mitigation costs. Only 10% of respondents said they spend more than $7 million annually or 27% spend more than $5 million. This contrasts with the full cohort where 25% indicated they spend $5 million or more.

Knowledge and Categorization of Data Types

The data type of the most concern to professional services respondents is legal communications (49%), followed by financial documents (44%) and protected health information (PHI) (43%). 52% of respondents said they tag and classify around three-quarters of their unstructured data. Not all that unstructured data needs to be tagged and classified, however, 24% of respondents said more than 80% of their unstructured data should be tagged and classified; 53% indicated it is 60% or more. These numbers are significantly higher than the full cohort—which said 18% for all unstructured data and 40% for three-quarters—likely revealing a greater level of maturity for professional services.

Imperative for Robust Sensitive Content Management in the Professional Services 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 professional services sector.

Operationally, professional services firms spend a lot of time managing logs generated by the numerous communication tools they use to share and send sensitive content. 43% of respondents must reconcile over 11; this is lower than the full cohort (48%). Also, 9% of professional services respondents did not know how many logs must be reconciled. Finally, likely due to the nature of professional services, the number of staff hours required to generate compliance reports from logs is substantial when compared to most other industry segments. 38% spend over 2,000 staff hours annually and 78% spend over 1,500 hours.

Get the Full Report

June 2024

www.kiteworks.com