Kiteworks

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

HIGHLIGHTS

Communication Tools in Place	16%	7+
	21%	6
	29%	5
	16%	4
	13%	3
	3%	2
	0%	1
Exchange Sensitive Content With Third Parties	13%	Over 5,000
	30%	2,500 to 4,999
	27%	1,000 to 2,499
	10%	500 to 999
	20%	Less Than 499
Data Types Biggest Concern (Top 3)	50%	Financial Documents
	46%	PHI
	44%	PII
	43%	GenAI LLMs
	39%	IP
	37%	Legal Communications
	23%	CUI and FCI
	17%	M&A
Biggest Privacy and Compliance Focus (Top 2)	53%	U.S. State Privacy Laws
	44%	GDPR
	31%	HIPAA
	29%	SEC Requirements
	19%	Country-specific Data Privacy Laws
	16%	CMMC
	9%	PCI DSS
Most Important Security Validations (Top 2)	50%	ISO 27001, 27017, 27018
	53%	NIST 800-171/CMMC 2.0
	36%	SOC 2 Type II
	37%	IRAP (Australia)
	21%	FedRAMP Moderate
	11%	NIS 2 Directive
Number of Times Experienced Sensitive Content Communications Hack	10%	10+
	20%	7 to 9
	37%	4 to 6
	16%	2 to 3
	9%	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 financial services. This brief focuses on the key findings related to financial 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

66% of financial services firms rely on five or more communication tools to send and share sensitive content, which is more than the 53% of respondents that do so globally. When it comes to tracking and controlling sensitive content, 57% of financial services firms said they can track and control sensitive data sent and shared internally, whereas 49% indicated they can do so when it is exchanged externally.

When it comes to sensitive content communications privacy and compliance priorities, preventing leakage of confidential IP and corporate secrets and mitigating lengthy and expensive litigation costs were the two top priorities for financial services firms (57%). Globally across all industries, these two priorities were number one and two, respectively, though at lower rates—56% and 51%. The lowest priority checked by financial services respondents was avoidance of detrimental brand impact (15%).

Assessing the Third-party Risk of Sensitive Content

Managing third-party risk is a critical challenge for financial services firms, with 43% reporting they exchange sensitive content with over 2,500 third parties. An astounding 70% have over 1,000 third parties in their content supply chain (over the 66% average across all industries).

This picture is concerning since 44% of financial services respondents said they can track and control sensitive content once it leaves an application about half the time.

Assessing the State of Sensitive Content Compliance

82% of financial services organizations revealed their measurement and management of compliance for sensitive content communications requires some to significant improvement. This is less than what all respondents reported: 88%.

Financial firms cited U.S. state data privacy laws as their biggest focus area over other data privacy and compliance regulations (53% ranked first or second). With 18 individual state laws now passed, this is not a huge surprise. GDPR received the second-highest listing with 44% of organizations listing it as one of their top two. PCI DSS came in last for financial services with 9% checking it first or second.

When it comes to vetting and selecting security validations or certifications, financial services firms had a closer bunching as compared to all survey respondents. For example, 53% cited NIST 800-171/CMMC 2.0 as one of their top two. This was followed by 50% for ISO 27001, 27017, and 27018. The NIS 2 Directive, which goes into effect later this year, had the fewest priority citations with 9%. NIST 800-171 coming in at the top of the list is a bit of a surprise since it is primarily applicable to organizations conducting business with the federal government and DoD.

Assessing the Risk of Sensitive Content Security

88% of financial services organizations indicate their measurement and management of security risk associated with sensitive content communications requires significant or some improvement (same as the global cross-industry result).

57% of financial services firms revealed their sensitive content was breached five or more times (30% said seven times or more). Nearly 1 out of 10 respondents in finance 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 by financial services firms 36% of the time (4% fail to employ them altogether; 60% employ them all the time). These findings lag global survey responses across different industry sectors, revealing a potential concern for financial services.

Assessing the Cost of Security and Compliance

Like most industry sectors, survey data reveals financial services has a serious risk when it comes to data breaches, with 30% indicating they experienced seven or more in the past year. This is slightly better than the global average where 32% reported over seven data breaches. Another 37% said they had between four and six data breaches.

When it comes to litigation costs, the survey found 36% of financial respondents indicated they spend over $5 million annually. This is more than the global average where 25% admitted their litigation costs were over $5 million. Further, 55% of financial services respondents said they spent over $3 million versus only 45% globally.

Knowledge and Categorization of Data Types

19% of financial services organizations indicated they tag and classify less than 25% of unstructured data; another 23% admitted they tag and classify less than half. These percentages align with the global averages; 20% tag and classify less than one-quarter.

But not all unstructured data needs to be classified, at least most respondents indicated that is the case. 20% of financial firms said over 80% should be classified and another 23% said over 60%—or 43% said over 60% must be classified. This reveals a gap, especially when compared to global averages where 22% tag and classify less than one-quarter and 35% tag and classify between 40% and 60%.

Imperative for Robust Sensitive Content Management in Financial Services

The Kiteworks 2024 Sensitive Content Communications Report highlights the critical need for robust management of risk and compliance in sensitive content communications in financial services firms. Financial documents were cited as the data type posing the greatest risk by respondents (50%), though others also were frequently cited. Financial firms are certainly a target of malicious actors; two-thirds experienced five-plus data breaches last year.

Operationally, financial organizations spend a lot of time managing logs generated by the numerous communication tools they use to share and send sensitive content. Almost half (48%) of respondents must reconcile over 11, and 8% of respondents did not even know how many must be reconciled. This compiles into a huge report logjam; 11% spend 2,500 hours or more annually and another 20% spend over 2,000 hours.

Get Full Report