Kiteworks

2024 Analysis of Sensitive Content Communications in North America: Security and Compliance Trends

HIGHLIGHTS

Communication Tools in Place	24%	7+
	14%	6
	21%	5
	18%	4
	12%	3
	7%	2
	1%	1
Exchange Sensitive Content With Third Parties	13%	Over 5,000
	25%	2,500 to 4,999
	28%	1,000 to 2,499
	16%	500 to 999
	18%	Less Than 499
Data Types Biggest Concern (Top 3)	62%	Financial Documents
	46%	Legal Communications
	50%	GenAI LLMs
	40%	IP
	34%	PHI
	29%	PII
	20%	CUI and FCI
	21%	M&A
Biggest Privacy and Compliance Focus (Top 2)	63%	U.S. State Privacy Laws
	38%	HIPAA
	29%	SEC Requirements
	29%	GDPR
	17%	CMMC
	14%	Country-specific Data Privacy Laws
	10%	PCI DSS
Most Important Security Validations (Top 2)	46%	ISO 27001, 27017, 27018
	41%	SOC 2 Type II
	39%	NIST 800-171/CMMC 2.0
	34%	IRAP (Australia)
	32%	FedRAMP Moderate
	8%	NIS 2 Directive
Number of Times Experienced Sensitive Content Communications Hack	11%	10+
	22%	7 to 9
	22%	4 to 6
	23%	2 to 3
	12%	1
	10%	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 regions, including North America. This brief focuses on the key findings related to the North American region, 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

Nearly 6 out of 10 (59%) of North American organizations rely on five or more communication tools to send and share sensitive content, which is more than the 53% that do so globally. When it comes to tracking and controlling sensitive content, North American organizations are doing better than the global average; 70% claimed they can track and control more than three-quarters (compared to 61% globally).

Not surprisingly, unifying and securing sensitive content communications is a growing objective for many organizations. The top two priorities North American organizations cited (given the choice of ranking their top two) were 1) avoidance of operational outages and lost revenue (57%) and 2) prevention of leakage of confidential IP and corporate secrets (51%). This differed with global rankings where mitigation of lengthy and expensive legislation was the most frequently cited priority.

Assessing the Third-party Risk of Sensitive Content

Managing third-party risk is a critical concern for organizations in North America. 63% of North American organizations exchange sensitive content with over 1,000 third parties, which is slightly less than what was reported globally (66%). This is concerning since 31% of North American organizations indicated they can track and control sensitive data once it leaves an application about half the time.

Assessing the State of Sensitive Content Compliance

87% of North American organizations revealed their measurement and management of compliance for sensitive content communications requires some to significant improvement. This aligns with the global average of 88%.

North American organizations cited U.S. state data privacy laws as their biggest focus area over other data privacy and compliance regulations (63% ranked first or second). HIPAA was a distant second with 38% of organizations naming it as a top focus area. When it comes to vetting and selecting security validations or certifications, North American organizations listed ISO 27001, 27017, and 27018 (46%) as the most important followed by SOC 2 Type II (41%). This contrasts with the global averages of 53% for ISO 27001, 27017, and 27018 (15% higher than North America) and 26% for SOC 2 Type II (45% lower than North America).

Assessing the Risk of Sensitive Content Security

88% of North American organizations indicate their measurement and management of security risk associated with sensitive content communications requires significant or some improvement. 55% of North American organizations revealed their sensitive content was breached four or more times (33% said seven times or more), Even more disturbingly, 10% of North American organizations admitted they do not know.

Advanced security capabilities and practices such as encryption, multi-factor authentication, and governance tracking and control are only used for some sensitive content by North American organizations 29% of the time (2% fail to employ them altogether; 69% employ them all the time). While North American organizations use advanced security in higher numbers than those in EMEA and APAC, they are certainly not out of the woods and substantial risk exists.

Assessing the Cost of Security and Compliance

Survey data reveals North American organizations confront a serious risk when it comes to data breaches, with 33% of respondents indicating their organizations experienced over seven data breaches in the past year. This is slightly more than the global average where 32% reported over seven data breaches. Another 22% said they had between four and six data breaches. Just as concerning, 10% said they did not know.

When it comes to litigation costs, the survey found 27% of North American respondents indicated they spent over $5 million. This is more than the global average where 25% admitted their litigation costs were over $5 million. Further, 49% of North American respondents said they spent over $3 million versus only 45% globally.

Knowledge and Categorization of Data Types

20% of North American 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, though North America lags the global average of 29% that disclosed it is half or less.

These numbers take on larger significance with the answers North American respondents cited in response to the percentage of unstructured data that needs to be classified; 19% said they need to tag and classify 40% or less of unstructured data (and another 28% cited between 40% and 60%). 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 North America

The Kiteworks 2024 Sensitive Content Communications Report highlights the critical need for robust management of risk and compliance in sensitive content communications across organizations in North America. Nearly 60% of these organizations rely on multiple communication tools, surpassing the global average. Despite this complexity, 70% claim the ability to track and control a significant portion of their sensitive content, indicating a higher level of control compared to global peers. By prioritizing the avoidance of operational outages and the prevention of confidential IP leakage, organizations in North America are focusing on unifying and securing their communication tools to maintain operational efficiency and protect sensitive information.

A comprehensive and proactive approach to managing sensitive content is crucial for protecting organizational assets. With 87% of organizations in North America recognizing the need for improvement in security risk management and 78% experiencing multiple breaches, the importance of advanced security practices cannot be overstated. Although North America leads other regions in implementing encryption, multi-factor authentication, and governance tracking, there is still substantial risk. Addressing these challenges with a focus on enhancing security measures and improving data classification practices will be essential for maintaining data integrity and achieving compliance.

Get the 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.