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

HIGHLIGHTS

Communication Tools in Use	13%	7+
	12%	6
	25%	5
	21%	4
	18%	3
	8%	2
	3%	1
Exchange Sensitive Content With Third Parties	13%	Over 5,000
	27%	2,500 to 4,999
	23%	1,000 to 2,499
	14%	500 to 999
	23%	Less Than 499
Data Types Biggest Concern (Top 3)	53%	Financial Documents
	50%	IP
	46%	PII
	38%	GenAI LLMs
	38%	Legal Communications
	32%	PHI
	28%	CUI and FCI
	15%	M&A
Biggest Privacy and Compliance Focus (Top 2)	57%	GDPR
	29%	U.S. State Privacy Laws
	28%	CMMC
	27%	Country-specific Data Privacy Laws
	23%	HIPAA
	22%	SEC Requirements
	14%	PCI DSS
Most Important Security Validations (Top 2)	59%	ISO 27001, 27017, 27018
	42%	NIST 800-171/CMMC 2.0
	27%	SOC 2 Type II
	27%	IRAP (Australia)
	20%	NIS 2 Directive
Number of Times Experienced Sensitive Content Communications Hack	10%	10+
	17%	7 to 9
	21%	4 to 6
	26%	2 to 3
	17%	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 regions, including EMEA (Europe, Middle East, and Africa). This brief focuses on the key findings related to the EMEA 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

Half of EMEA organizations rely on five or more communication tools to send and share sensitive content, which is slightly less than the 53% that do so globally. Compared to global results where 39% of organizations cannot track and control more than half their sensitive content communications once it is sent, shared, or transferred, EMEA organizations admitted to a larger problem: 45% are unable to do so.

However, unifying and securing sensitive content communications is a growing objective for many organizations. The top priority EMEA organizations cited was prevention of data leaks of confidential IP and corporate secrets (62% identified as number one or two priority), followed by mitigation of lengthy/expensive litigation (51%) (e.g., class action lawsuits due to data privacy leakage). These data point trends underscore the necessity for organizations to consolidate sensitive content communication tools to mitigate risk and improve operational efficiency.

Assessing the Third-party Risk of Sensitive Content

Managing third-party risk is a critical concern for organizations in the EMEA region. 63% of EMEA organizations exchange sensitive content with over 1,000 third parties, which is slightly less than what was reported globally (66%). This is concerning since only 45% of EMEA 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

86% of EMEA organizations revealed their measurement and management of compliance for sensitive content communications requires some to significant improvement. This is slightly less than the global average of 88%.

Not surprisingly, EMEA organizations cited GDPR at the top of their list of focus areas over other data privacy and compliance regulations (57% ranked first or second). The next higher focus areas were U.S. state data privacy laws (29%) and CMMC 2.0 (28%). In the case of the latter, for EMEA organizations operating in the U.S., adherence with U.S. specific state laws and federal laws is important. When it comes to vetting and selecting security validations and certifications, EMEA respondents listed ISO 27001, 27017, and 27018 at a higher rate (59%) than both APAC (48%) and the Americas (46%). Surprisingly, the NIS 2 Directive only came up 20% of the time.

Assessing the Risk of Sensitive Content Security

88% of EMEA organizations indicate their measurement and management of security risk associated with sensitive content communications requires significant or some improvement. 48% of EMEA organizations revealed their sensitive content was breached four or more times (27% said seven times or more). Even more disturbingly, 9% of EMEA 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 EMEA organizations 43% of the time, with another 4% indicating advanced security is not used at all. 53% of EMEA organizations said they use advanced security all the time. Compared to global averages, EMEA is lagging behind here (59% globally).

Assessing the Cost of Security and Compliance

27% of EMEA respondents indicated they experienced over seven sensitive content communication data breaches over the past year. Another 21% said they had between four and six. This is slightly less than the global average of 32% with over seven data breaches. Just as concerning, 9% said they were not certain how many data breaches their organizations experienced.

When it comes to the financial impact of data breaches, 25% of EMEA organizations reported over $5 million in litigation costs—the same as the global average. Another 16% said they experienced between $3 million and $5 million—or 41% reported over $3 million in the past year. While these numbers are not as high as the Americas, they are substantial.

Knowledge and Categorization of Data Types

21% of EMEA organizations indicated they tag and classify less than 25% of unstructured data; another 33% admitted they tag and classify less than half. These percentages align with the global averages; 21% tag and classify less than one-quarter, while another 29% disclosed it is half or less.

These numbers take on larger significance with the answers EMEA respondents cited in response to the percentage of unstructured data that needs to be classified; 24% said they need to tag and classify 40% or less of unstructured data (and another 37% cited between 40% and 60%). This reveals a gap; unstructured data that is not tagged and classified but needs to be.

Imperative for Robust Sensitive Content Management in EMEA

The Kiteworks 2024 Sensitive Content Communications Report underscores the importance of managing risk and compliance in the realm of sensitive content communications. For organizations in the EMEA region, leveraging advanced communication tools, mitigating third-party risks, adhering to stringent compliance standards, and understanding the types of data handled are essential components of a robust cybersecurity strategy. Further, EMEA organizations will benefit by leveraging next-generation digital rights management (DRM) for advanced governance of sensitive content.

As the threat landscape continues to evolve, a proactive and comprehensive approach to managing sensitive content is imperative for maintaining data integrity and protecting organizational assets. EMEA organizations, with their slightly higher focus on certain aspects compared to global trends, are well-positioned to address these challenges effectively.

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.