Kiteworks

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

HIGHLIGHTS

Communication Tools in Place	8%	7+
	14%	6
	25%	5
	22%	4
	17%	3
	6%	2
	2%	1
Exchange Sensitive Content With Third Parties	7%	Over 5,000
	31%	2,500 to 4,999
	39%	1,000 to 2,499
	14%	500 to 999
	10%	Less Than 499
Data Types Biggest Concern (Top 3)	61%	Legal Communications
	48%	Financial Documents
	39%	PII
	37%	CUI and FCI
	36%	IP
	34%	PHI
	31%	GenAI LLMs
	15%	M&A
Biggest Privacy and Compliance Focus (Top 2)	43%	HIPAA
	42%	SEC Requirements
	32%	CMMC
	31%	U.S. State Privacy Laws
	25%	GDPR
	18%	Country-specific Data Privacy Laws
	11%	PCI DSS
Most Important Security Validations (Top 2)	48%	ISO 27001, 27017, 27018
	47%	NIST 800-171/CMMC 2.0
	45%	IRAP (Australia)
	38%	FedRAMP Moderate
	20%	SOC 2 Type II
	4%	NIS 2 Directive
Number of Times Experienced Sensitive Content Communications Hack	3%	10+
	40%	7 to 9
	29%	4 to 6
	17%	2 to 3
	7%	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 regions, including APAC (Asia-Pacific). This brief focuses on the key findings related to the APAC 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

52% of APAC organizations rely on five or more communication tools to send and share sensitive content, which is only slightly less than the 53% that do so globally. When it comes to tracking and controlling sensitive content, APAC organizations are the same as the global average; 61% claimed they track and control more than three-quarters. While right on the global average, APAC is substantially behind their Americas counterparts (70%).

Not surprisingly, unifying and securing sensitive content communications is a growing objective for many organizations. But the reasons for APAC are different than the Americas and EMEA; 79% ranked avoidance of detrimental brand impact as their first or second reason—compared to preventing leakage of confidential IP and corporate secrets as the top reason for EMEA (61%) and avoidance of operational outages and lost revenue for the Americas (57%). Mitigation of lengthy and expensive litigation (e.g., class action lawsuits due to data privacy leakage) was the second-highest reason cited by APAC organizations (61%).

Assessing the Third-party Risk of Sensitive Content

Managing third-party risk is a critical concern for organizations in APAC that exchange data at a higher volume per organization than those in EMEA and the Americas: 77% share, send, or transfer data with over 1,000 third parties (compared to 63% in the

Americas and EMEA). This is concerning since 39% of APAC organizations indicated they can track and control sensitive data once it leaves an application less than half the time.

Assessing the State of Sensitive Content Compliance

83% of APAC organizations revealed their measurement and management of compliance for sensitive content communications requires some to significant improvement. This is slightly below the global average of 88%. However, 32% indicated significant improvement is needed—the same as the Americas and higher than EMEA (25%).

When it comes to vetting and selecting security validations and certifications, APAC organizations listed ISO 27001, 27017, and 27018 as the most important (53% ranked it either first or second). NIST 800-171/CMMC 2.0 was cited second most often by APAC respondents, followed by IRAP (33%). The latter, considering many APAC respondents were from Australia, was not surprising.

Assessing the Risk of Sensitive Content Security

82% of APAC organizations indicated their measurement and management of security risk associated with sensitive content communications requires significant or some improvement. This makes sense when you look at the breach data, where 72% of APAC organizations revealed their sensitive content was breached four or more times (43% said seven times or more), This is significantly higher than EMEA and the Americas, 48% and 53%, respectively. And like EMEA and the Americas, a shocking number of APAC organizations do not even know how many times their sensitive content was breached (5%).

Advanced security capabilities and practices such as encryption, multi-factor authentication, and governance tracking and control are only used for some sensitive content by APAC organizations 43% of the time (57% employ them all the time, which is significantly less than the 67% in the Americas).

Assessing the Risk of Security and Compliance

Survey data reveals APAC has serious risk when it comes to data breaches, with 42% indicating their organizations experienced over seven data breaches in the past year. This is substantially higher than the global average of 32% that reported over seven data breaches. Another 28% reported four to six data breaches. 6% said they did not know.

When it comes to litigation costs, the survey found 22% of APAC organizations spent over $5 million last year. This is less than the global average of 25% that cited litigation costs over $5 million. Another 26% of APAC respondents said their litigation costs were between $3 million and $5 million.

Knowledge and Categorization of Data Types

24% of APAC organizations indicated they tag and classify less than 50% of unstructured data. This is slightly more than the global average; 22% tag and classify less than one-quarter; another 30% said they tag and classify less than 50%.

These numbers take on larger significance with the answers APAC respondents cited in response to the percentage of unstructured data that needs to be classified; 20% said they tag and classify 25% or less of unstructured data (and another 45% cited between 40% and 60%). When compared to global averages, APAC respondents lag—40% tag and classify 60% or more of their sensitive data globally versus 33% for APAC.

Imperative for Robust Sensitive Content Management in APAC

The Kiteworks 2024 Sensitive Content Communications Report highlights the unique challenges faced by organizations in APAC in managing sensitive content communications. With 52% of APAC organizations relying on five or more communication tools, the complexity of tracking and controlling sensitive content is evident. Interestingly, the primary motivation for unifying and securing sensitive content communications in APAC is the avoidance of detrimental brand impact, followed by the mitigation of costly litigation risks.

An overwhelming majority of APAC organizations acknowledge the need for improvement in measuring and managing compliance and security risks associated with sensitive content communications. The high frequency of data breaches experienced by APAC organizations, coupled with the limited adoption of advanced security practices, underscores the urgency of addressing these vulnerabilities. Enhancing data classification and tagging practices, along with implementing robust security measures, will be crucial for APAC organizations to safeguard their sensitive content and maintain compliance in an increasingly complex digital landscape.

Get the Full Report