Kiteworks

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

HIGHLIGHTS

Communication Tools in Place	16%	7+
	27%	6
	14%	5
	15%	4
	20%	3
	6%	2
	1%	1
	1%	Don't Know
Exchange Sensitive Content With Third Parties	7%	Over 5,000
	26%	2,500 to 4,999
	39%	1,000 to 2,499
	18%	500 to 999
	10%	Less Than 499
Data Types Biggest Concern (Top 3)	53%	Financial Documents
	50%	GenAI LLMs
	50%	IP
	41%	Legal Communications
	36%	PII
	34%	PHI
	26%	CUI and FCI
	12%	M&A
Biggest Privacy and Compliance Focus (Top 2)	41%	HIPAA
	38%	U.S. State Privacy Laws
	38%	CMMC
	32%	GDPR
	28%	SEC Requirements
	18%	PCI DSS
	6%	Country-specific Data Privacy Laws
Most Important Security Validations (Top 2)	50%	ISO 27001, 27017, 27018
	44%	NIST 800-171/CMMC 2.0
	38%	FedRAMP Moderate
	35%	IRAP (Australia)
	22%	SOC 2 Type II
	11%	NIS 2 Directive
Number of Times Experienced Sensitive Content Communications Hack	3%	10+
	39%	7 to 9
	26%	4 to 6
	20%	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 industry sectors, including security and defense. This brief focuses on the key findings related to security and defense, 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

57% of security and defense firms rely on five or more communication tools to send and share sensitive content, which is slightly less than the 53% of respondents that do so globally. When it comes to tracking and controlling sensitive content, 41% of security and defense firms said they can track and control sensitive data sent and shared internally, whereas only 39% indicated they can do so when it is exchanged externally. This is measurably worse than the cross-industry global cohort that reported 51% and 43% respectively (and a cause for concern for DoD agencies).

When it comes to sensitive content communications privacy and compliance priorities, mitigating lengthy/expensive litigation due to data privacy leakage (57%) and prevention of leakage of confidential IP and corporate secrets (50%) were the two priorities for security and defense firms. The former is slightly higher than the cross-industry cohort (51%) while the latter is lower (compared to 56%).

Assessing the Third-party Risk of Sensitive Content

Managing third-party risk is a critical challenge for nearly all organizations. Compared to other industry sectors, security and defense firms have about the same number of third parties with which they exchange sensitive data (33% do so with over 2,500) as other industry sectors. And like most other industry segments, they struggle when it comes to tracking and controlling sensitive information when it leaves an application. Only 10% claim they can do so 100% of the time while 37% said they can do so 50% or less of the time.

Assessing the State of Sensitive Content Compliance

83% of security and defense firms said they need significant (22%) or some (60%) improvement when it comes to compliance for sensitive content communications. Purportedly, this is slightly better than the global cross-industry cohort where only 11% said they need no improvement.

Surprisingly, security and defense firms cited HIPAA as the data privacy law comprising the biggest concern for them (41%). CMMC 2.0 compliance was tied for second place with 38% (with U.S. state data privacy laws). Country-specific data privacy laws compliance was listed the least often (6%). With CMMC full implementation not far off, the percentage is low and perhaps a concern. Based on data from other studies, most security and defense providers are unprepared for CMMC; thus, the fact CMMC compliance was not cited in higher numbers is a red flag.

When it comes to vetting and selecting security validations or certifications, 50% of security and defense firms listed ISO 27001, 27017, and 27018 as one of their top two. 44% said NIST 800-171/CMMC was their most important security certification/validation standard. FedRAMP Moderate came in third (38%). The NIS 2 directive was cited least often (11%).

Assessing the Risk of Sensitive Content Security

As with the question of compliance, slightly more security and defense firms revealed their sensitive content communications security requires significant or some improvement. Advanced security capabilities and practices such as encryption, multi-factor authentication, and governance tracking and control for internal content communications are used by only 55% of security and defense firms (compared to 59% of all respondents). The same is true for external content communications; only 51% do so as compared to 59% of all respondents. These two data points reveal a security risk that needs to be addressed.

Assessing the Cost of Security and Compliance

With cybercriminals and rogue nation-states targeting security and defense firms due to the sensitive and secret content they send and share, the number of reported data breaches in the past year is concerning: 42% said they experienced seven or more (compared to 32% of all respondents).

When it comes to litigation costs, the survey found security and defense firms have a serious risk. More than half (53%) admitted to annual litigation costs for data breaches of $3 million or more (compared to 45% of all respondents).

Knowledge and Categorization of Data Types

Almost half (48%) of security and defense firms said they tag and classify over three-quarters of unstructured data; another 28% admitted they tag and classify over half. These percentages are about the same as global numbers, where 48% said they tag and classify three-quarters or more of their unstructured data.

But not all unstructured data needs to be classified, at least that is what respondents told us. 27% of security and defense respondents said 60% or more of unstructured data should be classified. Another 47% of security and defense firms believe 40% to 60% only needs to be tagged and classified.

Imperative for Robust Sensitive Content Management in Security and Defense

The Kiteworks 2024 Sensitive Content Communications Report highlights the critical need for robust management of risk and compliance in sensitive content communications in security and defense. Financial documents were cited as the data type posing the greatest risk (53%) followed by Generative AI LLMs and IP (both at 50%). On the GenAI LLM front, security and defense was tied with energy and utilities for the highest industry percentage.

Operationally, security and defense firms spend a lot of time managing logs generated by the numerous communication tools they use to share and send sensitive content. Nearly 3 out of 10 said they spend 2,000 or more hours doing so. Another 38% spend 1,500 to 1,999 hours.

Get Full Report