Kiteworks

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

HIGHLIGHTS

Communication Tools in Place	17%	7+
	8%	6
	27%	5
	20%	4
	17%	3
	11%	2
	2%	1
Exchange Sensitive Content With Third Parties	11%	Over 5,000
	23%	2,500 to 4,999
	32%	1,000 to 2,499
	20%	500 to 999
	15%	Less Than 499
Data Types Biggest Concern (Top 3)	79%	Financial Documents
	46%	IP
	46%	Legal Communications
	44%	GenAI LLMs
	35%	PII
	23%	M&A
	15%	CUI and FCI
	13%	PHI
Biggest Privacy and Compliance Focus (Top 2)	52%	U.S. State Privacy Laws
	36%	GDPR
	33%	SEC Requirements
	29%	CMMC
	21%	HIPAA
	18%	Country-specific Data Privacy Laws
	11%	PCI DSS
Most Important Security Validations (Top 2)	58%	ISO 27001, 27017, 27018
	37%	IRAP (Australia)
	33%	SOC 2 Type II
	29%	NIST 800-171/CMMC 2.0
	29%	FedRAMP Moderate
	9%	NIS 2 Directive
Number of Times Experienced Sensitive Content Communications Hack	14%	10+
	12%	7 to 9
	23%	4 to 6
	29%	2 to 3
	23%	1
	0%	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 manufacturing. This brief focuses on the key findings related to manufacturing, 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 manufacturers 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, 52% of manufacturing 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.

When it comes to sensitive content communications privacy and compliance priorities, preventing leakage of confidential IP and corporate secrets (61%) and avoiding operational outages and lost revenue (44%) were the two top priorities for manufacturers. This contrasts across all respondents who cited preventing leakage of confidential IP and corporate secrets (56%) and mitigating lengthy and expensive litigation (51%). The lowest priority checked by manufacturing 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 manufacturers, with 34% reporting they exchange sensitive content with over 2,500 third parties. Two-thirds of manufacturers exchange sensitive content with 1,000-plus third parties. There was good news when it comes to tracking and controlling sensitive content communications in manufacturing; a higher percentage (79%) than any other industry said they can track and control more than three-quarters of sensitive content once it leaves an app.

Assessing the State of Sensitive Content Compliance

94% of manufacturers revealed their measurement and management of compliance for sensitive content communications requires some to significant improvement. This is significantly higher than what all respondents reported: 88%. The only industry that reported a higher gap than manufacturing was professional services (96%).

Manufacturers cited U.S. state data privacy laws as their biggest focus area over other data privacy and compliance regulations (52% ranked it first or second). With 18 individual state laws now passed, this is not a huge surprise. GDPR received the second-highest listing with 36% of organizations listing it as one of their top two. PCI DSS came in last for manufacturing with 11% checking it first or second.

When it comes to vetting and selecting security validations or certifications, 58% of manufacturers listed ISO 27001, 27017, and 27018 as one of their top two. The Information Security Registered Assessors Program (IRAP), overseen by the Australian government to independently assess their cybersecurity posture, identify risks, and suggest mitigation measures, surprisingly was listed most often by 37% of manufacturers—higher than SOC 2 Type II (33%).

Assessing the Risk of Sensitive Content Security

98% of manufacturers indicated their measurement and management of security risk associated with sensitive content communications requires significant or some improvement (compared to 88% of all respondents). This is a significant difference and security gap.

Advanced security capabilities and practices such as encryption, multi-factor authentication, and governance tracking and control are only used for some sensitive content by manufacturers 42% of the time (compared to 39% across industries). This reveals a security risk that needs to be addressed.

Assessing the Cost of Security and Compliance

Like most industry sectors, survey data revealed manufacturers have a serious risk when it comes to data breaches, though better than aggregate data across industries. Specifically, 49% of manufacturers revealed their sensitive content was breached five or more times (24% said seven times or more). This is better than all survey respondents: 32% experienced seven or more and 55% experienced four or more.

When it comes to litigation costs, the survey found manufacturers are doing better than most other industry segments: 18% indicated they spend over $5 million annually. This compares to all survey respondents where 25% admitted their litigation costs were over $5 million.

Knowledge and Categorization of Data Types

Almost half (49%) of manufacturers said they tag and classify over three-quarters of unstructured data; another 30% 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. 18% of manufacturing respondents said 80% or more of unstructured data should be classified. 58% said less than 60% of unstructured data should be tagged and classified.

Imperative for Robust Sensitive Content Management in Manufacturing

The Kiteworks 2024 Sensitive Content Communications Report highlights the critical need for robust management of risk and compliance in sensitive content communications in manufacturing. Financial documents were cited by far as the data type posing the greatest risk by manufacturing respondents (79%)—the highest of any industry.

Operationally, manufacturers spend a lot of time managing logs generated by the numerous communication tools they use to share and send sensitive content. Half of respondents must reconcile over 11. This compiles into a huge report logjam; 11% spend 2,500 hours or more annually and another 21% spend over 2,000 hours.

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.