Kiteworks

Manufacturing: 2023 Sensitive Content Communications Privacy and Compliance

Industry Findings and Takeaways

HIGHLIGHTS

Communication Tools in Use	**26%**	7+
	35%	6
	24%	5
	15%	Less than 4
Average Annual Budget for Communication Tools	**22.5%**	$500,000+
	16.5%	$350,000 – $499,999
	36.5%	$250,000 – $349,999
	21%	$150,000 – $249,999
	3%	$100,000 – $149,999
Number of Third Parties With Which They Exchange Sensitive Content	**21%**	5,000+
	38%	2,500 – 4,999
	36.5%	1,000 – 2,499
	4.5%	499 - 999
Attack Vector Weighted Score (based on ranking)	**100**	Phishing
	98	URL Manipulation
	93	Cross-site Scripting
	76	Rootkits
	73	Malware (ransomware, trojans, etc.)
	72	DNS Tunneling
	70	SQL Injection
	60	Man in the Middle
	59	Password/ Credential Attacks
	59	Session Hijacking
	42	Zero-day Exploits and Attacks
	39	Denial of Service
	17	Insider Threats
Exploits of Sensitive Content Communications in Past Year	**16.5%**	10+
	24%	7 – 9
	53%	4 – 6
	6%	2 – 3
Level of Satisfaction With 3rd-party Communication Risk Management	**8%**	Requires a New Approach
	38%	Significant Improvement Needed
	26%	Some Improvement Needed
	29%	Minor Improvement Needed

Cyber Incidents Show No Sign of Slowing Down in Manufacturing

The manufacturing industry continues to face a growing number of cyber threats, with no signs of slowing down. Indeed, manufacturing is still one of the most targeted industries for cyberattacks due to high-value intellectual property and sensitive data. This explains why the average cost of a data breach in manufacturing continues to rise—going from $4.24 million in 2021 to $4.47 million in 2022, an increase of 5.4%.[1] Personally identifiable information (PII) is the most targeted data type (60%). Denial of service (DoS) is the objective about two-thirds of the time.[2] Hacking, malware attacks, social attacks, and ransomware account for the majority of attack actions.

Disaggregated Tool Soup Drives Up Costs

Kiteworks' 2023 Sensitive Content Communications Privacy and Compliance Report found that 85% of manufacturing companies use five or more tools for sensitive content communications. Managing a disaggregated tool soup makes it difficult for organizations to demonstrate adherence to different compliance regulations and security standards. Needing to purchase and manage individual toolsets drives up both capital (CapEx) and operating expenses (OpEx). For example, over three-quarters of manufacturing respondents spend $250,000 or more, on average, on communication tools.

75.5% of manufacturing companies spend $250,000 or more, on average, on communication tools.

Ranking Third-party Content Communication Risk for Manufacturers

Manufacturers face significant risks associated with third-party content communication. Nearly two-thirds of manufacturers use six or more systems to track, control, and secure content communications with third parties. This heightens their risk exposure. Furthermore, manufacturing respondents in the study reveal file sharing and mobile application communication channels have the highest risk. 33.5% of the respondents ranked these two channels number one and two, respectively.

60.5% of manufacturing companies use six or more systems to track, control, and secure content communications with third parties.

Only 36.5% of manufacturers have a comprehensive system in place to track and control access to sensitive content folders for all content types and departments. Surprisingly, this ranks among the highest compared to other industries, such as energy and utilities at 20% and higher education at 19%. Respondents also indicated that a vast majority of manufacturers (71.5%) believe they need to improve their approach to mitigating the risks associated with third-party content communication. Of these respondents, over 7 in 10 called for a new approach (7.5%) or require significant or some improvements (63.5%). This assessment makes a lot of sense, considering 93.5% of manufacturers experienced four or more exploits of sensitive content communications in the past year.

Manufacturers Need to Improve Digital Risk Management

The study found that manufacturers need to take a closer look at their digital risk management practices, as the lack of robust measures can lead to information breaches. Nearly one-third of respondents indicated they have policies for tracking and controlling content collaboration and sharing on-premise but not in the cloud. Nearly one-quarter have the opposite: tracking and controls for sensitive content communications in the cloud but not on-premise. Meanwhile, 33.5% of manufacturers have sensitive content communications tracking and controls on-premise and in the cloud. These figures reveal a concerning gap in digital risk management practices across the manufacturing industry, highlighting the need for improvement to better protect sensitive content.

Kiteworks Private Content Network for Manufacturers

The Kiteworks Private Content Network enables manufacturers to share and send sensitive content such as product design and specifications, technical documentation, supply chain planning, manufacturing schedules, patents, and production and inventory data. Alignment of risk management strategies for the measurement and management of sensitive content communications is either in progress or planned for later this year by 75% of manufacturers. When it comes to digital rights management capabilities, manufacturers list ease of deployment and maintenance and rich individual control over sensitive content shared with partially trusted individuals and organizations at the top of their list of requirements. The Kiteworks platform supports adherence with these standards through a range of robust security features, including encryption, access controls, and audit logging. Additionally, manufacturers benefit from Kiteworks' user-friendly interface, which simplifies the process of sharing files and collaborating with colleagues.

[1] "Cost of a Data Breach Report 2022," IBM and Ponemon Institute, July 2022.

[2] "2023 Data Breach Investigations Report," Verizon, June 2023.

Get the Full Report

Kiteworks

Kiteworks 2023 Sensitive Content Communications Privacy and Compliance Report

Seeking to empower private and public sector organizations to manage their file and email data communication risks better, Kiteworks began publishing an annual Sensitive Content Communications Privacy and Compliance Report in 2022. Rogue nation-states and cybercriminals recognize the value of sensitive content and target the communication channels used to send, share, receive, and store it—email, file sharing, managed file transfer, web forms, APIs, and more.

The 2023 Sensitive Content Communications Privacy and Compliance Report surveyed 781 IT, security, risk, and compliance professionals across numerous industries and 15 different countries. The in-depth report, which is based on their survey responses, explores a range of issues related to file and email data communication risks—how organizations are addressing those today and plan to do so in the coming year. The analysis includes a look back to 2022 data and what changes were observed in 2023.