Kiteworks

Technology (Hi-tech): 2023 Sensitive Content Communications Privacy and Compliance

Industry Findings and Takeaways

HIGHLIGHTS

Communication Tools in Use	**25%**	7+
	25%	6
	28.5%	5
	21.5%	Less than 4
Average Annual Budget for Communication Tools	**14.5%**	$500,000+
	21.5%	$350,000 – $499,999
	27%	$250,000 – $349,999
	30.5%	$150,000 – $249,999
	7%	$100,000 – $149,999
Number of Third Parties With Which They Exchange Sensitive Content	**18%**	5,000+
	25%	2,500 to 4,999
	41%	1,000 to 2,499
	10.5%	500 to 999
	5.5%	Less than 499
Attack Vector Weighted Score (based on ranking)	**100**	DNS Tunneling
	93	SQL Injection
	90	Cross-site Scripting
	77	Password/Credential Attacks
	76	Denial of Service
	74	URL Manipulation
	60	Zero-day Exploits and Attacks
	60	Rootkits
	52	Phishing
	41	Session Hijacking
	38	Malware (ransomware, trojans, etc.)
	32	Man in the Middle
	25	Insider Threats
Exploits of Sensitive Content Communications in Past Year	**7%**	10+
	16%	7 – 9
	57%	4 – 6
	19.5%	2 – 3
Level of Satisfaction With 3rd-party Communication Risk Management	**9%**	Requires a New Approach
	46%	Significant Improvement Needed
	38%	Some Improvement Needed
	7%	Minor Improvement Needed

Growing Cyber Threat Landscape in the Technology Sector

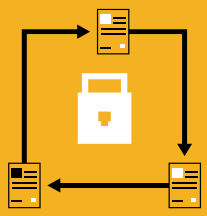
Technology companies are a primary target by adversaries conducting data theft and extortion campaigns. According to Crowdstrike's 2023 Global Threat Report, the technology sector was the most frequently targeted vertical with advanced interactive intrusion activity, reflecting an increase compared with the relative frequency of intrusions in the top 10 industry verticals from the prior 12 months.[1] These attacks targeted everything from highly confidential intellectual property (IP) to personally identifiable information (PII) and have led to a flurry of privacy regulations. A report by the World Economic Forum reveals that 73% of organizations believe cyber and privacy regulations are effective in reducing their cyber risks.[2] This is a significant shift from the year before, where more than half of respondents did not agree with the same statement.

When Too Many Communication Tools Spell Trouble for Sensitive Data

Kiteworks' 2023 Sensitive Content Communications Privacy and Compliance Report finds tech companies, along with most organizations across industry sectors, use multiple disaggregated communication tools. Half of tech companies use six or more systems for sensitive file and email content communications. The more communication tools an organization uses, the more difficult it becomes to manage and protect sensitive data. This leads to compliance violations, brand damage, lost revenue, and diminished efficiencies. The need to purchase and manage individual sensitive communication toolsets drives up both capital expenses (CapEx) and operating expenses (OpEx). For technology companies, 36% spend $350,000 or more per year for communication tools used to exchange sensitive content.

Evaluating Third-party Content Communication Risks

Tech companies are highly vulnerable to third-party content communication risks. The Kiteworks report shows that 85.5% of tech firms use four or more systems to manage content communications with third parties. Tech companies list email as the communication channel posing the biggest risk, with 1 in 3 respondents ranking it number one. Application programming interfaces (APIs) supporting sensitive content communications came in second, with about 1 in 5



36% of tech companies spend over $350,000 annually for communication tools used to send and share sensitive content.

4 out of 5 tech firms have experienced four or more exploits of sensitive content communications in the past year.

respondents ranking APIs as their top risk channel. When asked if they have a comprehensive system to track and control access to sensitive content folders for all content types and departments, only 23% of tech companies said they have such.

What's even more alarming is that 4 out of 5 tech firms have experienced four or more exploits of sensitive content communications in the past year. This is a serious concern, and it explains why 93% of tech firms believe they need to improve their approach to mitigating the risks associated with third-party content communication. Out of this number, more than three-quarters (84%) require significant or some improvements, while 9% call for a new approach.

Tech Companies Must Prioritize Digital Risk Management

One of the key reasons tech companies struggle to protect their file and email data communications is their difficulty in embracing digital rights management. Only 25% of tech companies track and record third-party access to sensitive files and folders across all departments, with 39.5% tracking only for certain departments and 21.5% tracking for specific content types. Top priorities tech companies list around digital rights management include providing easy, secure access to all content repositories without migration (61% gave it a rank of #1 to #4) and protecting content in motion from malicious threats (58% gave it a rank of #1 to #4).

Kiteworks and Tech Companies

It is crucial for tech firms to adopt a proactive approach to mitigate file and email communication privacy and compliance risks. They have numerous use cases, including sharing proprietary code internally and with third-party developers, collaborating on product development, distributing software updates, exchanging customer data, sharing product test data, sharing proprietary algorithms and research, and more. Kiteworks offers tech companies a comprehensive approach to secure their sensitive content communications and manage the associated risks. Comprehensive governance tracking and controls enable tech companies to restrict access to content, controlling who can view and edit it, to whom it can be shared and sent, and where it is sent and shared.

[1] "2023 Global Threat Report," Crowdstrike, February 2023.

[2] "Global Cybersecurity Outlook," World Economic Forum, January 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.