Kiteworks

Security and Defense: 2023 Sensitive Content Communications Privacy and Compliance

Industry Findings and Takeaways

HIGHLIGHTS

Communication Tools in Use	31%	7+
	28%	6
	32%	5
	9%	Less than 4
Average Annual Budget for Communication Tools	22%	$500,000+
	19%	$350,000 – $499,999
	37%	$250,000 – $349,999
	21%	$150,000 – $249,999
Number of Third Parties With Which They Exchange Sensitive Content	21%	5,000+
	35%	2,500 – 4,999
	31%	1,000 – 2,499
	7%	500 – 999
	6%	Less than 499
Attack Vector Weighted Score (based on ranking)	100	Password/Credential Attacks
	85	Denial of Service
	74	Man in the Middle
	62	DNS Tunneling
	60	SQL Injection
	58	Cross-site Scripting
	58	Rootkits
	54	URL Manipulation
	42	Zero-day Exploits and Attacks
	41	Phishing
	40	Session Hijacking
	37	Insider Threats
	35	Malware (ransomware, trojans, etc.)
Exploits of Sensitive Content Communications in Past Year	17%	10+
	23%	7 – 9
	55%	4 – 6
	5%	2 – 3
Level of Satisfaction With 3rd-party Communication Risk Management	4%	Requires a New Approach
	23%	Significant Improvement Needed
	41%	Some Improvement Needed
	32%	Minor Improvement Needed

Global Instability and the Threat of Cyber Armageddon

As the security and defense industry continues to confront evolving cyber threats, it must remain vigilant in fortifying its digital defenses, enhancing information security protocols, and fostering a culture of cybersecurity awareness. The storage, transmission, and exchange of vast volumes of classified data, proprietary technologies, and intellectual property within the security and defense sector contribute significantly to the heightened risk it faces. A report from ISACA earlier this year found that 87% of organizations in the Defense Industrial Base (DIB) do not meet basic cybersecurity regulations and have a Supplier Performance Risk System (SPRS) score below 70. Compliance with NIST 800-171—and therefore Cybersecurity Maturity Model Certification (CMMC 2.0)—is also a problem, with 71% of DIB suppliers indicating they comply via self-assessment while actual Department of Defense assessments of the same organizations reveal only 29% actually comply.[1]

Growing Impact of CMMC 2.0 Compliance in the DIB

Kiteworks' 2023 Sensitive Content Communications Privacy and Compliance Report finds that 93% of respondents said their businesses are directly related to their ability or inability to comply with cybersecurity frameworks and standards—particularly CMMC 2.0 Level 2. For the 7% that did not list CMMC 2.0 as a compliance regulation affecting their businesses, they either plan to shut down operations with the Department of Defense or need to initiate a process immediately to determine their readiness to comply with CMMC 2.0. The survey's results underscore the pressing need for businesses to prioritize cybersecurity measures and invest in the resources required to achieve compliance with CMMC 2.0.

Too Many Disaggregated Tools for Sensitive Content Communications

One of the takeaways in the report is that security and defense organizations rely on a lot of communication tools to send and share sensitive content: Nearly 6 out of 10 have six or more sensitive content communication systems in place. This disaggregated sensitive communications landscape complicates their ability to protect sensitive data that is sent and shared internally and with the DIB supply chain. It also creates compliance challenges, including their ability to achieve CMMC certification.

95% of defense and security firms' insurance providers consider their data privacy and compliance risk management for rating coverages. This is more than any other industry

Ranking Third-party Content Communications Risk

Risk management of third-party content communications is seen as a problem across industry sectors, and security and defense is not spared. 27% of respondents say they require a new approach, or their current approach requires significant improvement. Another 41% indicate some improvement is needed. And if the ISACA report is correct, survey respondents may be overconfident in their risk capabilities. The number of exploits they reported for the past 12 months is corroboration, with 95% of organizations in the sector experiencing four or more exploits of sensitive content communications.

Better Digital Risk Management Required

All the above translates into significant risk to the DoD supply chain and slows down the CMMC 2.0 certification process. Lack of robust digital rights management is a big part of the problem, though weaknesses across security and defense organizations are not the same. For example, 55% of respondents say they have administrative policies in place for tracking and controlling content collaboration and sharing on-premise but not in the cloud. However, at the same time, 24% expressed the opposite—namely, they have tracking and controls in place for the cloud but not on-premise. More alarmingly, only 13% of them have both the cloud and on-premise covered, which was among the lowest across industries.

When it comes to managing and restricting third-party access to folders and files with capabilities such as content permissions, expiration, locking, and versioning, more than 7 in 10 of security and defense firms indicate they fail to do so across all departments (36% say they do so for certain departments and 39% indicate they do so for only certain content types). Tracking and recording third-party access to files and folders is not much better: nearly 8 in 10 of security and defense firms fail to do so for all content across all departments.

Kiteworks and Security and Defense Organizations

Security and defense firms lack the appropriate governance and security for their file and email data communications. The Kiteworks Private Content Network provides a platform that breaks down silos between disparate communication channels and delivers zero-trust policy management. This delivers lower CapEx and OpEx while enabling dramatically improved risk management. With Kiteworks, security and defense firms can securely share classification in compliance with relevant regulations, collaborate on defense strategies, exchange mission-critical data, share intelligence reports, collaborate on threat assessments, and share nation-state secrets.

Security and defense firms can also accelerate their CMMC 2.0 certification process with Kiteworks, which supports nearly 90% of CMMC 2.0 Level 2 practice requirements. FedRAMP, SOC 2, and ISO 27001, 27017, and 27108 certified, Kiteworks uses a hardened virtual security approach that includes an embedded network firewall, WAF, and antivirus and integrates advanced security capabilities like CDR, DLP, and ATP.

Get the Full Report

[1] Kirsten Morales, "More than 87% of Pentagon Supply Chain Fails Basic Cybersecurity Minimums," Cybersheath, November 30, 2022

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.

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.