Kiteworks

Financial Services: 2023 Sensitive Content Communications Privacy and Compliance

Industry Findings and Takeaways

HIGHLIGHTS

Communication Tools in Use	**35%**	7+
	34%	6
	26.5%	5
	4.5%	Less than 4
Average Annual Budget for Communication Tools	**19%**	$500,000+
	39.5%	$350,000 – $499,999
	26.5%	$250,000 – $349,999
	14.5%	$150,000 – $249,999
Number of Third Parties With Which They Exchange Sensitive Content	**28%**	5,000+
	34%	2,500 – 4,999
	32.5%	1,000 – 2,499
	3%	500 – 999
	3%	Less than 499
Attack Vector Weighted Score (based on ranking)	**100**	URL Manipulation
	83	Session Hijacking
	76	Password/Credential Attacks
	65	Malware (ransomware, trojans, etc.)
	67	Cross-site Scripting
	67	Denial of Service
	54	DNS Tunneling
	54	Rootkits
	52	Zero-day Exploits and Attacks
	50	SQL Injection
	30	Phishing
	26	Insider Threats
	17	Man in the Middle
Exploits of Sensitive Content Communications in Past Year	**20.5%**	10+
	41%	7 – 9
	34%	4 – 6
	4.5%	2 – 3
Level of Satisfaction With 3rd-party Communication Risk Management	**10%**	Requires a New Approach
	17.5%	Significant Improvement Needed
	34%	Some Improvement Needed
	38%	Minor Improvement Needed

The Financial Industry Continues to Be a Top Target for Cybercriminals

Financial services often is at the forefront of a sophisticated and evolving digital landscape, witnessing rapid technological advancements that deliver new services to customers and drive operational efficiencies. However, the movement of more confidential data into the digital space and is exchanged with first and third parties has not gone unnoticed. For example, according to CrowdStrike's 2023 Global Threat Report, the financial sector was the second most frequently targeted vertical after the technology vertical last year. [1] Verizon's 2023 Data Breach Investigations Report (DBIR) found that personally identifiable information (PII) is the top target of bad actors (74% of the time).[2]

Too Many Disaggregated Tools for Sensitive Content Communications

Kiteworks' 2023 Sensitive Content Communications Privacy and Compliance Report revealed that financial firms struggle to manage file and email data communication risks—both inside their organizations and with third parties. One of the reasons is the large number of systems financial organizations use to send and share private data. Nearly 7 out of 10 financial institutions have six or more sensitive content communication systems in place.

Ranking Third-party Content Communications Risk

Financial organizations rank among the highest when it comes to the number of different systems used to send and share content communications with third parties: 60% use six or more. Surprisingly, in terms of ranking, respondents pegged web forms at the top of the list, with 25% giving them a number one ranking. When ranks one and two are factored together, email caught up with web forms, with 41% giving each a number one and two ranking. One of the ways email poses risk relates to challenges with encryption; specifically, when recipients cannot decrypt an email due to it being encrypted in a format not supported by their organization. Application programming interfaces (APIs) came in second, with 29.5% of respondents ranking them at number one and two.

Governance plays an important causation role here: 31% only track and control access to sensitive content folders for certain content types, while another 37% only do so for certain departments.

Risk management of third-party content communications is seen as a problem across industry sectors, and financial services is one at the top of the list. 44% of respondents said they require a new approach or their current approach requires significant improvement. Another 38% indicated some improvement is needed. Survey responses corroborate concerns around risk: 95.5% of financial services organizations experienced four or more exploits of sensitive content communications in the past year.

Better Digital Risk Management Required

Lack of robust digital rights management is a big part of the problem, though weaknesses across financial services organizations are not the same. For example, 42.5% of respondents said they have administrative policies in place for tracking and controlling content collaboration and sharing on-premises but not in the cloud. However, at the same time, 20.5% said the opposite—namely, they have tracking and controls in place for the cloud but not on-premises. Only slightly more than one-third indicate they have digital risk management capabilities in place for both the cloud and on-premises.

Kiteworks and Financial Organizations

The Kiteworks Private Content Network employs a content-defined zero-trust approach that enables financial services organizations to unify, track, control, and secure all their sensitive content communications in one platform. Financial services organizations can track and control access to files and folders, who can edit and share them, and to whom and where they can be shared. Doing so enables financial firms to ensure private personally identifiable information, intellectual property, client financial records, insurance claims, and more remain private and in compliance with global regulations.

Web forms and email tied for highest risk of all communication channels, with 41% of financial firms listing them as either their number one or two risk.

69% of financial institutions use 6+ sensitive content communication tools and systems.

95.6% of financial services organizations experienced four or more exploits of sensitive content communications in the past year.

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

[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.

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.