Kiteworks

Professional Services: 2023 Sensitive Content Communications Privacy and Compliance

Industry Findings and Takeaways

HIGHLIGHTS

Communication Tools in Use	37.5%	7+
	21.5%	6
	29.5%	5
	12%	Less than 4

Average Annual Budget for Communication Tools	23.5%	$500,000+
	23.5%	$350,000 – $499,999
	27.5%	$250,000 – $349,999
	21.5%	$150,000 – $249,999
	4%	$100,000 – $149,999

Number of Third Parties With Which They Exchange Sensitive Content	27.5%	5,000+
	31.5%	2,500 – 4,499
	25.5%	1,000 – 2,499
	6%	500 – 999
	10%	Less than 499

Attack Vector Weighted Score (based on ranking)	100	DNS Tunneling
	100	Session Hijacking
	85	Password/Credential Attacks
	79	URL Manipulation
	73	Man in the Middle
	70	Cross-site Scripting
	67	Phishing
	64	Denial of Service
	64	Zero-day Exploits and Attacks
	61	Rootkits
	47	SQL Injection
	38	Malware (ransomware, trojans, etc.)
	15	Insider Threats

Exploits of Sensitive Content Communications in Past Year	27.5%	10+
	21.5%	7 – 9
	43%	4 – 6
	8%	2 – 3

Level of Satisfaction With 3rd-party Communication Risk Management	14%	Requires a New Approach
	35%	Significant Improvement Needed
	39%	Some Improvement Needed
	12%	Minor Improvement Needed

Professional Services Firms Remain a Prime Target for Cyberattacks

The professional services industry continues to face escalating cyber threats, with no signs of abating. The M-Trends 2023 Report by Mandiant puts business and professional services firms as the second most targeted industry by adversaries.[1] The industry remains an attractive target for both financially and espionage motivated actors, and sensitive data is in the crosshairs. As professional services firms exchange highly confidential data related to finances, supply chains, intellectual property (IP), and mergers and acquisitions, protecting this data from malicious cyberattacks and inadvertent exposure is critical. Verizon's 2023 Data Breach Investigations Report puts system intrusion (47%), basic web application attacks (25%), and social engineering (18%) as the three top threat patterns affecting professional services firms.[2] With the volume of third-party content communications continuing to expand exponentially, sensitive content communications privacy and compliance have never been more important.

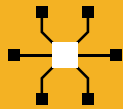## More Communication Tools Than Any Industry Sector

A key factor in risk behind file and email data communications with third parties is related to the number of tools used to send, share, receive, and store it. Kiteworks' 2023 Sensitive Content Communications Privacy and Compliance Report found that 37.5% of professional firms use seven or more tools for sensitive content communications. This is the highest among all industries surveyed. This "tool soup" is one explanation why professional services firms have long been a favored target for cybercriminals, in addition to the high-value client data they hold. The report further finds that these disaggregated tools have led to high CapEx for professional services firms, with 45% using $350,000 or more, annually.

Assessing Third-party Content Communication Risk in the Professional Services

When it comes to third-party content communications risk, Kiteworks' 2023 Sensitive Content Communications Privacy and Compliance Report found that 27.5% of professional services firms share sensitive content with over 5,000 third parties. This only compares with the financial services industry, with all other industries having lower figures. 92% of the professional services firms share and manage sensitive content with these third parties using four or more systems, which increases their risk exposure. The respondents in this industry went further to list email as the channel with the highest risk, with 39% of them giving it a rank of one and two.

37.5% of professional services firms use seven or more communication tools, more than any other industry.

88% of professional services firms believe they need to improve their approach to mitigating the risks associated with third-party content communication.

The volume of file and email data communications with third parties necessitates the use of tight governance tracking and controls. The study found an overwhelming majority of professional services firms (88%) believe they need to improve their approach to mitigating the risks associated with third-party content communication. Of these respondents, 14% called for a new approach, while 74% felt that some or significant improvements were necessary.

The report also reveals that in the past year, 92% of professional services firms experienced four or more exploits of sensitive content communications. This was lower than other industries such as healthcare at 98% but higher than energy and utilities firms at 80%. This demonstrates a clear need for professional services firms to prioritize and strengthen their content communication strategies to better safeguard sensitive information and reduce their risk exposure. By implementing a comprehensive system that tracks and controls access to sensitive content and improving their overall approach to mitigating third-party content communication risks, professional services firms can better protect themselves and their clients.

Professional Services Firms Lag in Digital Risk Management Practices

One critical outtake from the data is the need for professional services firms to embrace digital risk management. Only 27.5% track and record third-party access to sensitive files and folders across all departments, 41% track only for certain departments, and 19.5% track but only for certain content types. When it comes to digital rights management, professional services firms list content tracking permissions, expiration, locking, and versioning as their top priority (35.5% ranked it one or two), followed by automating encryption, file sharing, reporting, and other processes as number two (31.5% ranked this either number one or two).

Kiteworks Private Content Network for Professional Services Firms

The Kiteworks Private Content Network enables professional services firms to embrace digital rights management by unifying, tracking, controlling, and securing their sensitive content communications with first and third parties from one platform. It includes comprehensive digital rights management tracking and controls that enable professional services organizations to manage access and collaboration, expiration, versioning, to whom content is sent or shared, and to where it is sent and shared. Its hardened virtual appliance, security layering, end-to-end encryption, and AI-enabled anomaly detection is industry leading and certified—from FedRAMP Authorization, to FIPS 140-2, to ISO 27001, 27017, and 27108, to SOC 2, to many others.

[1] "M-2023 Trends Report," Mandiant, April 2023.

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

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.