Kiteworks

Local Government: 2023 Sensitive Content Communications Privacy and Compliance

Industry Findings and Takeaways

HIGHLIGHTS

Communication Tools in Use	**4.5%**	7+
	13%	6
	56.5%	5
	26%	Less than 4
Average Annual Budget for Communication Tools	**4.5%**	$500,000+
	4.5%	$350,000 – $499,999
	39%	$250,000 – $349,999
	35%	$150,000 – $249,999
	17.5%	$100,000 – $149,999
Number of Third Parties With Which They Exchange Sensitive Content	**13%**	2,500 – 4,999
	74%	1,000 – 2,499
	8.5%	500 – 999
	4.5%	Less than 499
Attack Vector Weighted Score (based on ranking)	**100**	Denial of Service
	98	Man in the Middle
	98	Rootkits
	88	Zero-day Exploits and Attacks
	85	URL Manipulation
	83	SQL Injection
	80	Password/Credential Attacks
	73	Session Hijacking
	70	Phishing
	60	Cross-site Scripting
	50	Insider Threats
	48	DNS Tunneling
	20	Malware (ransomware, trojans, etc.)
Exploits of Sensitive Content Communications in Past Year	**9%**	7 – 9
	52%	4 – 6
	35%	2 – 3
	4%	1
Level of Satisfaction With 3rd-party Communication Risk Management	**13%**	Requires a New Approach
	26%	Significant Improvement Needed
	48%	Some Improvement Needed
	13%	Minor Improvement Needed

Local Governments Continue to Face a Never-ending Wave of Cyberattacks

Local governments face a never-ending wave of cyberattacks. According to the Verizon 2023 Data Breach Investigations Report (DBIR), the public sector had the most cyber incidents and attacks this past year.[1] Rogue nation-states and cybercriminals recognize local governments are resource constrained and send and share high volumes of personally identifiable information (PII), protected health information (PHI), and other types of sensitive content, both within their organizations and often with thousands of third parties. Breached data is held for ransom, sold on the dark web, and used for other nefarious purposes. Sensitive content targeted by cyberattacks include public safety information, budgets and financial data, collaboration on urban planning projects, data on infrastructure and planning projects, social services program data, criminal background information, personally identifiable information (PII), and more. Further, in the compliance era, local governments must protect file and email data communications while demonstrating compliance with various data privacy regulations.

Too Many Communication Systems Compromising Sensitive Content Communications

Kiteworks' 2023 Sensitive Content Communications Privacy and Compliance Report finds that local governments rely on a variety of different communication tools to exchange sensitive content. Approximately 7 out of 10 local government agencies use five or more. These pose significant hurdles for local governments, making it difficult to safeguard private information. For local governments, which are local resource and budget constrained, nearly half spend $250,000 or more annually on communication tools.

Evaluating Third-party Content Communications Risks

For local governments, email is listed as the communication channel with the highest risk, with one in five respondents ranking it as the top risk. File sharing comes in second with 35% of respondents ranking it number 1 or number 2.

Local governments lack governance tracking and controls around sensitive content communications. Only 4% of local governments—by far the lowest of every industry segment—indicate they have a comprehensive system in place to effectively track and control access to sensitive content folders across

Approximately 7 out of 10 local government agencies use five or more communication tools for exchanging sensitive content.

Over half of local governments rely on four or more systems to manage sensitive content communications with third parties.

all departments. The same percentage of local government respondents admitted they do not track and record third-party access to sensitive files and folders—activity such as who viewed a document and when, who edited a document and when, who downloaded a document, and who shared a document and when.

Due to porous gaps in governance, local governments have significant risks. Approximately three out of five local government agencies experienced four or more breaches in sensitive content communications in the past year. It is not surprising that 87% of local government agencies recognize the need to enhance their sensitive content communication risk mitigation strategies. Of these, 74% require significant or some improvements, while 13% require a new approach to third-party communication risk management.

Challenges in Digital Risk Management for Local Governments

When it comes to prioritizing digital rights management (DRM), local government agencies list automating encryption, file sharing, reporting, and other processes (61% ranked it as a top three priority) and unifying management, tracking, policies, and reporting (48% ranked it as a top three priority) as their top two DRM priorities. Respondents indicated that the biggest hurdle facing them on the DRM front is agents or specific software in clients to open an unencrypted file with external third parties. Often, when third-party recipients cannot open an encrypted file, they revert to workarounds that create risk.

Kiteworks and Local Governments

There are varying types of sensitive content that local governments send and share with first and third parties. The Kiteworks Private Content Network enables local governments to apply DRM-based tracking and controls based on the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF). Comprehensive audit logs can be integrated into SIEM and SOAR systems or viewed separately in the CISO Dashboard. Kiteworks uses a hardened virtual appliance that includes an embedded network firewall, WAF, and antivirus and employs an advanced security approach that integrates DLP, CDR, and ATP and includes AI-enabled anomaly detection. This ensures that private content sent and shared by local government agencies is secure.

Get the Full Report

[1] "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.