Kiteworks

State and Provincial Governments: 2023 Sensitive Content Communications Privacy and Compliance

Industry Findings and Takeaways

HIGHLIGHTS

Communication Tools in Use	**21.5%**	6
	53.5%	5
	25%	Less than 4
Average Annual Budget for Communication Tools	**3.6%**	$350,000 – $499,999
	53.6%	$250,000 – $349,999
	35.7%	$150,000 – $249,999
	7.1%	$100,000 – $149,999
Number of Third Parties With Which They Exchange Sensitive Content	**14.3%**	2,500 – 4,999
	67.9%	1,000 – 2,499
	3.6%	Less than 999
Attack Vector Weighted Score (based on ranking)	**100**	DNS Tunneling
	89	SQL Injection
	87	Session Hijacking
	87	Denial of Service
	72	Password/Credential Attacks
	70	Zero-day Exploits and Attacks
	69	Cross-site Scripting
	60	Phishing
	53	Malware (ransomware, trojans, etc.)
	50	Man in the Middle
	50	URL Manipulation
	36	Rootkits
	11	Insider Threats
Exploits of Sensitive Content Communications in Past Year	**14.3%**	7 – 9
	71.4%	4 – 6
	14.3%	2 – 3
Level of Satisfaction With 3rd-party Communication Risk Management	**7%**	Requires a New Approach
	29%	Significant Improvement Needed
	39%	Some Improvement Needed
	25%	Minor Improvement Needed

Persistent Cyber Incidents in State Government

State and provincial governments send, share, receive, and store huge volumes of sensitive data. This data encompasses everything from personal data, such as personally identifiable information (PII), protected health information, and criminal records, to public safety information, to tax documents, to budget and financial data. Rogue nation-states and cybercriminals recognize the value of the data, and they are targeting state and provincial sensitive content communications with a variety of different attack methods. Kiteworks' 2023 Sensitive Content Communications Privacy and Compliance Report finds that 86% of state and provincial government agencies dealt with four to nine sensitive content communication exploits in the past year.

Scattered Tool Ecosystem Increases Risk and Cost for State and Provincial Governments

One of the reasons for this targeted concentration of cyberattacks and exploits is the use of numerous, siloed communication tools. Three-quarters of state and provincial governments in the survey reported that they utilize five or more communication tools. The dispersion of these tools poses a formidable challenge, making it increasingly complex to establish standard governance policies and security standards. In addition to ratcheting up security risk, this communication "tool soup" makes it difficult for state and provincial governments to demonstrate adherence with varying compliance regulations such as HIPAA, PIPEDA, GDPR, and many others. Utilizing siloed toolsets also increases CapEx and OpEx costs. For example, Kiteworks' report found that 54% of state and provincial governments spend between $250,000 and $349,000 annually on the communication tools themselves.

Evaluating Third-party Content Communication Risks

State and provincial government entities face considerable risks when it comes to third-party content communications. Over 21% of these entities use six or more systems to track, manage, and secure content communications with third parties. Respondents indicate that file sharing and mobile application communication channels are the highest risk areas. More than two-thirds exchange sensitive

Over 7 out of 10 state and provincial government agencies experienced between four to six exploits of sensitive content communications in the past year.

Over two-thirds of state and provincial government entities handle sensitive content communications with 1,000 to 2,499 third parties.

content with 1,000 to 2,499 third parties, which elevates the intricacy and risk of safeguarding content communication.

In light of the above, it is not surprising that only 21.5% of state and provincial government agencies have a comprehensive system to track and control access to sensitive content folders across all types of content and departments. As a consequence, most respondents acknowledge the need to change how they manage sensitive content communication risk.

State Government Agencies Must Strengthen Digital Risk Management

As with other industry sectors, state and provincial governments would do well to heed greater attention to digital rights management. Tracking and controlling content communications on-premises and in the cloud requires attention. Only 54% indicate they have established tracking and control measures for both on-premises and cloud environments. The one upside is state and provincial governments seem to recognize their gaps here, with 77% indicating they either are in the progress of implementing or have plans to align risk management strategies with their sensitive content communication approaches.

Kiteworks Private Content Network for State Government Agencies

State and provincial governments exchange large volumes of sensitive content, both within their organizations and with third parties. The use cases vary and include activities such as collaboration on state-wide policy development, transferring grant applications, sharing budget and financial information, exchanging information on social service programs, and sharing PII and PHI records. The Kiteworks Private Content Network enables state and provincial governments to establish zero-trust policy management—tracking and controls on who can access sensitive content, who can edit it, who can send and share it, to whom it can be sent and shared, and to where it can be sent and shared. This dramatically reduces privacy and compliance risk exposure. Further, to demonstrate compliance with various data privacy regulations, state and provincial governments can tap comprehensive audit logs in Kiteworks. Plus, because Kiteworks employs advanced security capabilities, including a hardened virtual appliance, an embedded network firewall, WAF, and antivirus, AI-enabled anomaly detection, end-to-end encryption, and integrated ATP, CDR, and DLP capabilities, file and email data communications by state and provincial governments are protected from malicious cyberattacks.

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.