Kiteworks

Middle Eastern Region: 2023 Sensitive Content Communications Privacy and Compliance

Regional Findings and Takeaways

HIGHLIGHTS

Communication Tools in Use	**24%**	7+
	29%	6
	30%	5
	17%	Less than 4
Average Annual Budget for Communication Tools	**17%**	$500,000+
	20.5%	$350,000 – $499,999
	37.5%	$250,000 – $349,999
	21.5%	$150,000 – $249,999
	3.5%	$100,000 – $149,999
Number of Third Parties With Which They Exchange Sensitive Content	**18%**	5,000+
	27%	2,500 – 4,999
	42%	1,000 – 2,499
	4%	500 – 999
	10%	Less than 499
Attack Vector Weighted Score (based on ranking)	**100**	URL Manipulation
	93	Rootkits
	65	Man in the Middle
	59	Password/Credential Attacks
	58	Phishing
	58	SQL Injection
	58	DNS Tunneling
	57	Cross-site Scripting
	51	Denial of Service
	46	Session Hijacking
	37	Insider Threats
	36	Zero-day Exploits and Attacks
	34	Malware (ransomware, trojans, etc.)
Exploits of Sensitive Content Communications in Past Year	**16%**	10+
	16%	7 – 9
	58%	4 – 6
	11%	2 – 3
Level of Satisfaction With 3rd-party Communication Risk Management	**10%**	Requires a New Approach
	33%	Significant Improvement Needed
	30%	Some Improvement Needed
	28%	Minor Improvement Needed

Cyber Threat Landscape in the Middle East

The Middle East faces the same cyber threats as the rest of the world. Energy and utilities, telecommunications, and government sectors top the list of industries that are targeted most frequently. Cybercriminals are employing more sophisticated tactics like double extortion and deepfake technology, and the Middle East has been affected by these more than other industries. The average cost of a data breach in the middle east hit $6.93 million last year, substantially higher than the $4.24 million global average.[1] Middle Eastern organizations face various types of cyberattacks targeting personally identifiable information (PII), protected health information (PHI), intellectual property (IP), financial documents, merger and acquisition activity, and criminal information, among others.

Too Many Communication Tools Compromise Sensitive Content Communications

Kiteworks' 2023 Sensitive Content Communications Privacy and Compliance Report shows many companies in the Middle East use multiple disaggregated communication tools, which pose risks to data privacy and compliance. Over half of Middle East companies use six or more systems for sensitive file and email content communications. This leads to difficulties in managing and protecting sensitive data as well as demonstrating compliance with various data privacy regulations. Emergence of new regulations in the region and expansion in countries outside of the Middle East ratchet up the importance of compliance governance and reporting. Managing multiple toolsets also adds to capital and operating expenses at the same time, with 37.5% of Middle Eastern companies spending $350,000 or more annually on communication tools.

Evaluating Third-party Content Communication Risks in the Middle East

Nearly half of the respondents in the Middle East report using six or more systems to manage content communications with third parties. Email was listed as the communication channel with the highest risk, with two out of five respondents giving it a number one rank. File sharing was the second highest, with approximately one in three participants rating it as their top risk channel.

37.5% of companies in the Middle East spend $350,000 or more annually on communication tools.

Two out of five respondents rank email as their communication channel with the highest risk.

There is good cause for organizations in the Middle East to be concerned about managing third-party content communication risks. Only one in five have a comprehensive system to track and control access to sensitive content folders for all content types and departments. Not surprisingly, almost 90% experienced four or more breaches of sensitive content communications in the past year. As a result, 72% believe they must improve their approach to mitigating the risks associated with third-party content communications, with 62% indicating significant or some improvement is needed, while the remaining 10% require a new approach.

Digital Risk Management in the Middle East

Only 22% of respondents track and record third-party access to sensitive files and folders across all departments, with 48% tracking only for certain departments and 23% tracking for specific content types. 34% rank protecting content in motion from malicious threats as their top priority (with a rank one or two), while 27.5% prioritize automating encryption, file sharing, reporting, and other processes and/or tracking content permissions, expiration, locking, and versioning.

Kiteworks for Organizations in the Middle East

Middle Eastern organizations seeking to mitigate their privacy and compliance risk can look to Kiteworks. The Kiteworks Private Content Network unifies, tracks, controls, and secures sensitive content communications in one platform. This unlocks zero-trust policy management across each communication channel—email, file sharing, managed file transfer, web forms, and APIs—and delivers comprehensive audit logs for tracking and reporting on governance-related issues. This unlocks the ability for organizations to demonstrate compliance with data privacy regulations like GDPR, HIPAA, PIPEDA, and others. Kiteworks also offers advanced security capabilities, including a hardened virtual appliance, an embedded network firewall, WAF, and antivirus engine, end-to-end encryption, AI-enabled anomaly detection, and integrated security capabilities like CDR, DLP, and ATP. Kiteworks also offers multiple deployment options. With several secure deployment options, including on-premises, private cloud, and hosted, Kiteworks is an excellent solution for sensitive content communication in the Middle East.

[1] "2022 Cost of a Data Breach Report," IBM and Ponemon Institute, July 2022.

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.