Kiteworks

Asia Pacific: 2023 Sensitive Content Communications Privacy and Compliance

Regional Findings and Takeaways

HIGHLIGHTS

Communication Tools in Use	**25%**	7+
	22.5%	6
	32%	5
	16%	Less than 4
Average Annual Budget for Communication Tools	**16%**	$500,000+
	20.5%	$350,000 – $499,999
	32.5%	$250,000 – $349,999
	26%	$150,000 – $249,999
	4.5%	$100,000 – $149,999
Number of Third Parties With Which They Exchange Sensitive Content	**15%**	5,000+
	30%	2,500 – 4,999
	50%	1,000 – 2,499
	2%	500 – 999
	4%	Less than 499
Attack Vector Weighted Score (based on ranking)	**100**	DNS Tunneling
	90	URL Manipulation
	85	Malware (ransomware, trojans, etc.)
	74	Man in the Middle
	74	Phishing
	74	Password/Credential Attacks
	74	Rootkits
	72	Zero-day Exploits and Attacks
	70	Session Hijacking
	69	SQL Injection
	65	Cross-site Scripting
	62	Denial of Service
	36	Insider Threats
Exploits of Sensitive Content Communications in Past Year	**11%**	10+
	26%	7 – 9
	43%	4 – 6
	19%	2 – 3
Level of Satisfaction With 3rd-party Communication Risk Management	**5%**	Requires a New Approach
	35%	Significant Improvement Needed
	35%	Some Improvement Needed
	26%	Minor Improvement Needed

Cyberattacks on the Rise in Asia Pacific Region

IBM's Security X-Force Threat Intelligence Index 2023 found that the Asia Pacific (APAC) region has maintained its position as the most cyberattacked region, accounting for 31% of all incidents worldwide in 2022, increasing 5% from 2021 (more than Europe at 28% and North America at 25% of attacks).[1] The APAC region has increasingly continued to play a greater role in the global supply chain, and organizations in the region are becoming a more attractive target for attackers seeking to exploit vulnerabilities to gain access to sensitive data. Rogue nation-states and cybercriminals target the manufacturing, finance, insurance, and other industries, with Japan, Philippines, Australia, India, and Vietnam the top countries being targeted.

Too Many Communication Tools Compromise Sensitive Content Communications

Kiteworks' 2023 Sensitive Content Communications Privacy and Compliance Report shows many organizations in the Asia Pacific region rely on numerous, disaggregated communication tools for sending and sharing sensitive content. Nearly four out of five respondents indicate their organizations use five or more tools. This leads to increased capital and operating expenses for the organizations. For example, 69% of the organizations spend $250,000 or more annually on communication tools. This is second only to the Middle East region.

Third-party Content Communication Risks in APAC Region

When asked which communication channels pose the greatest risk to third-party content communications, 36% of respondents gave email a rank one and two, while 35% of the respondents ranked web forms number one or two. Email encryption is a key concern. Content governance is another key issue. Only 27% of APAC respondents track and control access to sensitive content folders for all third parties across all departments. Another 32% track only for certain departments while 38% track only for certain content types.

Risk management of third-party content communications is a concern in APAC, with 75% of respondents stating that a new approach for managing risk is needed or significant improvement is required. This is probably driven by the number of exploits to sensitive content communications observed in this region. Four out of five respondents reported to experience four or more exploits in the past year.

Four out of five respondents experienced four or more sensitive content communications exploits in the past year.

69% of APAC companies spend $250,000 or more annually on communication tools.

Need for Better Digital Risk Management in the APAC Region

The Kiteworks report identifies a pressing need for better digital risk management. A significant percentage of respondents indicate their organizations lack robust policies for tracking and controlling content collaboration and sharing. Specifically, only 38% of respondents say they have administrative policies in place for on-premises but not in the cloud, while only 25% have policies in place for the cloud but not on-premises. Only about one-quarter of organizations have both the cloud and on-premises covered, suggesting the need for more comprehensive digital risk management practices in the region.

Kiteworks Private Content Network for APAC

The Kiteworks Private Content Network enables APAC governmental agencies and public-sector businesses to unify and secure their sensitive content communications while applying comprehensive governance tracking and controls. Kiteworks centralizes zero-trust policy management for all communication channels into one platform. Kiteworks content-defined zero trust allows only privileged access to secured content, tracking and controlling who can view and edit it, to whom it can be sent and shared, and where it can be sent (geofencing). Kiteworks uses an advanced security approach that includes a hardened virtual appliance, security layering, end-to-end encryption, embedded antivirus, network firewall, WAF, and AI-enabled anomaly detection. Kiteworks is IRAP assessed against PROTECTED level controls, SOC 2 and ISO 27001, 27017, and 27018 certified, and FedRAMP Authorized, among others. In addition, Kiteworks comprehensive audit logs enable APAC organizations to demonstrate compliance with various data privacy regulations.

[1] "The IBM Security X-Force Threat Intelligence Index 2023," IBM Security, February 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.