Kiteworks

Energy and Utilities: 2023 Sensitive Content Communications Privacy and Compliance

Industry Findings and Takeaways

HIGHLIGHTS

Communication Tools in Use	**24%**	7+
	24%	6
	48%	5
	4%	Less than 4
Average Annual Budget for Communication Tools	**12%**	$500,000+
	24%	$350,000 – $499,999
	36%	$250,000 – $349,999
	20%	$150,000 – $249,999
	8%	$100,000 – $149,999
Number of Third Parties With Which They Exchange Sensitive Content	**16%**	5,000+
	24%	2,500 – 4,999
	52%	1,000 – 2,499
	4%	500 – 999
	4%	Less than 499
Attack Vector Weighted Score (based on ranking)	**100**	Session Hijacking
	95	Password/ Credential Attacks
	75	Zero-day Exploits and Attacks
	75	Denial of Service
	65	DNS Tunneling
	65	Rootkits
	65	URL Manipulation
	60	Cross-site Scripting
	40	SQL Injection
	30	Insider Threats
	25	Phishing
	25	Man in the Middle
	15	Malware (ransomware, trojans, etc.)
Exploits of Sensitive Content Communications in Past Year	**12%**	10+
	16%	7 – 9
	52%	4 – 6
	20%	2 – 3
Level of Satisfaction With 3rd-party Communication Risk Management	**20%**	Requires a New Approach
	24%	Significant Improvement Needed
	24%	Some Improvement Needed
	32%	Minor Improvement Needed

Rising Cyber Threats Put Energy and Utilities Companies at Risk

The growing reliance on digital technology and interconnectedness systems makes the energy and utilities sector an attractive target for cybercriminals. These rising cyber threats put energy and utilities companies at risk, not just in terms of financial and reputational damage but also in terms of the security and safety of critical infrastructure and services. At the same time, confidential information exchanged via file sharing and transfer and email by energy and utilities companies poses a significant target for cyberattacks.

Too Many Disaggregated Tools for Sensitive Content Communications

Kiteworks' 2023 Sensitive Content Communications Privacy and Compliance Report found that energy and utilities companies struggle to manage file and email data communication risks—both inside their organizations and with third parties. Like other industry sectors, the majority of energy and utilities companies rely on a silo of different communication tools for sending, sharing, and transferring sensitive content: 96% use five or more systems. These increase CapEx and OpEx for energy and utilities companies, with 72% spending more than $250,000 on them annually.

96% of energy and utilities companies use five or more sensitive content communication systems.

Ranking Third-party Content Communications Risk for Energy and Utilities Companies

40% of energy and utilities companies send and share sensitive content to 2,500-plus third parties on a regular basis. 92% do so with 1,000-plus third parties. This creates significant privacy and compliance risk. The disaggregation of file and email communication tools makes it difficult to create governance tracking and controls that minimize risk. The communication channel with the highest risk was file sharing, according to survey respondents (68% ranked it number 1, 2, or 3), which was followed by email (ranked 1, 2, or 3 by 56% of respondents).

One in every three energy and utilities companies rank file sharing as the most risky channel for third-party content communications.

Alarmingly, the industry ranked among the lowest in terms of having a comprehensive system in place to track and control access to sensitive content folders for all content types and departments, with only 20% indicating they have these in place today. It is not surprising that 68% of industry respondents believe they need to improve their approach to mitigating these risks. Their assessment is illustrative of the fact that four out of five energy and utilities companies experienced four or more instances of sensitive content communication exploits in the past year.

Need to Improve Digital Risk Management

There is cause for serious concern when it comes to protecting sensitive content communications from privacy and compliance exposure. Only 24% of respondents admit they track and record third-party access to sensitive files and folders across all departments. Another 12% track only for certain departments, while 44% track such—though only for certain content types. Lack of digital rights management poses a problem. More respondents in energy and utilities say their risk management of third-party content communications needs a completely new approach—the highest of every industry sector—and another 24% saying significant improvement is needed.

Kiteworks Private Content Network for Energy and Utilities Companies

The Kiteworks Private Content Network provides energy and utilities companies a secure environment for exchanging sensitive content between users, organizations, and systems. Using the Kiteworks platform, energy and utilities companies can demonstrate compliance with data privacy regulations and cybersecurity standards. Zero-trust policy management provides risk and compliance professionals with unified visibility and the ability to set policies that adhere with regulations such as GDPR, HIPAA, Cyber Essentials Plus, among others. Advanced security capabilities in Kiteworks, which seamlessly integrates third-party security investments in ATP, CDR, and DLP, protect sensitive data, such as employee and customer PII, financial documents, merger and acquisition information, and legal documents, that energy and utilities companies send and share internally and with third parties. Kiteworks support for security best practices is confirmed by certifications that include FedRAMP Authorized, SOC 2, and ISO 27001, 27017, and 27018.

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.