# High Stakes of DRM Revealed in Kiteworks 2023 Sensitive Content Communications Privacy & Compliance Report

*While third-party file and email data communications spike, inadequate tracking, controls, and security ratchet up risk.*

SAN MATEO, CA, USA, July 11, 2023 /EINPresswire.com/ -- Kiteworks, which delivers data privacy and compliance for sensitive content communications through its Private Content Network, revealed today serious gaps in digital rights management that expose private and public sector organizations to serious security and compliance risks. Kiteworks' 2023 Sensitive Content Communications Privacy and Compliance Report found many organizations lack unified tracking, control, and security of private data that is sent, shared, and transferred with third parties, which creates significant risk of unauthorized access—malicious and accidental.

> "This year's report accentuates the need for DRM that applies content-defined zero trust across all departments and all sensitive data that is accessed, sent, shared, and transferred to 3rd parties."
>
> *Frank Balonis*

Increased Risk From Siloed Communication Tools and Expanded Third-party Supply Chain

Part of the problem is the number of systems and tools organizations use for tracking, controlling, and securing third-party content communication: 85% of survey respondents said their organizations rely on four or more. The result is that nearly three-quarters admit significant to some improvement is needed in how they measure and manage security and compliance risk as it relates to sensitive content access. It is not surprising, as a result, that fewer than one-quarter of respondents said they manage or restrict all third-party access to sensitive content. Three-quarters of organizations admit their risk management of third-party sensitive data communications requires a completely new approach or significant to some improvement.

Digital Rights Management "Do-over" Needed

According to the report, many organizations need a "do-over" for digital rights management: 42% indicated either they need a completely new approach or significant improvement for third-party sensitive content communication risk management. This digital rights management gap, as a

result, creates substantial risk, with nearly 85% of respondents disclosing they experienced four or more sensitive content communication exploits in the past year. More than 55% ranked the ability to employ compliance and security policies to the level of users, roles, and content classes rather than individual users classifying each asset manually as their first or second top digital rights management priority.

Areas of Biggest Risk and Concern

Respondents listed personally identifiable information (PII) as the sensitive content type that poses the greatest security and compliance risk—over intellectual property (IP), legal documents, merger and acquisition information, financial documents, and other data types. This concern directly correlates with the need to adhere to data privacy laws. For example, 37% of respondents said they must adhere to the General Data Protection Regulation (GDPR).

Of file and email data communication channels, email and web forms were identified as posing the highest risk (40% ranked it number one or two). File sharing services were seen as an especially big risk in energy and utilities (32% ranked it number 1), while web forms were higher in financial services (25%). Email was seen as an even bigger risk in technology and security and defense companies, with 32% in both industries ranking it as number 1. One area that respondents overwhelmingly cited as a concern is the use of multitenant cloud hosting of tools. The highest concern here was bad actors exploiting one application or dataset, moving laterally across the instance, and then gaining access to application or data for other tenants (48%).

Standards and Compliance Play an Important Role

In line with what other recent studies reveal, respondents indicated cybersecurity frameworks are critical in helping them to maintain revenue and perform their organizational mission. Those specific to certain industries or regions have a higher representation in organizations in those segments. ISO 27001 appeared the most often followed by NIST CSF. At the same time, Cybersecurity Maturity Model Certification (CMMC) 2.0 compliance was listed by nearly every contractor in the defense/security sector. The importance of compliance with data privacy regulations is accentuated by nearly 4 in 10 respondents being hit with regulatory fines and penalties due to noncompliance.

“This year’s report accentuates the need for digital rights management that applies content-defined zero trust across all departments and all sensitive data that is accessed, sent, shared, and transferred to third parties,” said Frank Balonis, CISO and Senior Vice President of Operations at Kiteworks. “This cannot be done piecemeal but rather requires unified tracking and control to the level of individual users. The report also highlights how organizations are using cybersecurity frameworks such as NIST CSF to manage their security and compliance risk. This corroborates the direction Kiteworks has taken to align our Private Content Network with NIST CSF, which creates more comprehensive digital rights management governance.”

For a copy of the report and analysis around it, see the below links.

2023 Sensitive Content Communications Privacy and Compliance (report): Click here

Navigating the High Stakes of Digital Rights Management: Key Takeaways From Kiteworks' 2023 Sensitive Content Communications Privacy and Compliance Report (webinar roundtable): Watch replay now

About Kiteworks
Kiteworks' mission is to empower organizations to effectively manage risk in every send, share, receive, and save of sensitive content. The Kiteworks platform provides customers with a Private Content Network that delivers content governance, compliance, and protection. The platform unifies, tracks, controls, and secures sensitive content moving within, into, and out of their organization, significantly improving risk management and ensuring regulatory compliance on all sensitive content communications. Headquartered in Silicon Valley, Kiteworks protects over 35 million end users for thousands of global enterprises and government agencies.

The 2023 Sensitive Content Communications Privacy and Compliance Report is based on responses from 781 IT, security, risk, and compliance management professionals located in 15 countries around the globe. The survey was conducted during the months of February and March 2023.

Patrick Spencer
Kiteworks
press@kiteworks.com
Visit us on social media:
Facebook
Twitter
LinkedIn
YouTube

---