Kiteworks

Kiteworks' 2023 Sensitive Content Communications Privacy and Compliance Report

Executive Summary

HIGHLIGHTS

Complexity in Tools and Recipients

90% of organizations share sensitive content with 1,000+ third parties, and 44% share with over 2,500

50% of organizations use six or more channels to share sensitive content

Cybersecurity Challenges

85% of organizations use four or more systems to track, control, and secure sensitive content

Barely **one-quarter** of organizations consider their security measurement and management practices adequate

There is a high volume of exploits specifically around sensitive content communications, with **84%** of organizations experiencing four or more such incidents over the past year

Compliance Challenges

Compliance remains a significant challenge, with over **two-thirds** of organizations dedicating 300+ staff hours annually to ensure compliance for sensitive content communications

Governance

Gaps exist in implementing best practices, with only **22%** of organizations having comprehensive tracking and recording of third-party access

Organizations are slowly adopting digital rights management (DRM), with **93%** already classifying sensitive content but encountering challenges in deployment

Key Insights and Takeaways

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.

Complex Web of Recipients, Channels, and Tools

An increasing number of third parties with which organizations share content is exacerbating security concerns. Comparing survey data from 2022 and 2023, 90% of organizations in 2023 reported sharing content with more than 1,000 outside organizations, up from 63% in 2022. Notably, 44% now share with over 2,500 third parties. This rise is apparent across enterprises of all sizes and industry sectors. Moreover, organizations are using a growing number of communication channels to transmit sensitive content, making it more challenging to control access. With 50% of organizations using six or more tools for sensitive content communications, tracking and controlling secure content exchange is more complex. This complexity necessitates substantial resources, resulting in higher expenses and challenges in maintaining compliance.

Security Maturity: A Long Way Ahead

The report highlights a significant gap between organizations' security efforts and what is required for effective sensitive content communication. Only one-quarter of respondents consider their security measurement and management practices to be adequate. They also acknowledge the risk of various channels such as email, file sharing, mobile apps, and APIs.

The number of incidents targeting sensitive content communication is alarmingly high, with over 80% of organizations reporting four or more such exploits in the past year. The financial impact and compliance fines resulting from these attacks have been severe, affecting over 60% and 40% of organizations, respectively.

Challenges in Compliance Requirements

Compliance with regulations and standards, such as GDPR, PIPEDA, PCI DSS, HIPAA, and numerous others, remains a massive undertaking for organizations, with the majority investing substantial time and resources to ensure compliance. Businesses are grappling with increasing requirements, which puts a strain on their IT, security, and compliance teams.

While respondents demonstrate an understanding of best practices, there is a gap in their application. Only a fraction of organizations has been able to extend tracking, recording, and access control for sensitive content across all departments, content types, and infrastructure. Not surprisingly, only a quarter of respondents believe their compliance risk measurement and management is under control; the other three-quarters believe either a new approach is needed or significant to some improvement is necessitated.

Digital Rights Management "Do-over"

Despite the challenges, the report offers a beacon of hope with digital rights management (DRM) positioned as a solution. Classifying sensitive content, segmenting it based on risk, and controlling access according to roles and geographies are essential steps in DRM. Although its adoption is slow, most organizations understand its importance and are gradually aligning their strategies accordingly.

While there are significant gaps in sensitive content communication protection, these represent opportunities for organizations to improve their strategies in the coming year. By adopting a holistic approach, such as DRM, organizations can enhance compliance, protect against insider threats, and secure sensitive content, regardless of its origin or mode of sharing.

Only 28% of organizations indicate their sensitive content communications security efforts are already aligned with the corporate risk management strategy.

Only 22% of organizations track and control access to sensitive content at the admin level, on-premises and in the cloud.

A significant majority of organizations acknowledge the importance of DRM, with more than 90% already classifying their sensitive content. Despite challenges in deployment, such as the need for agent intervention for unencrypted files with third parties and customizable controls for different users and content types, DRM is steadily gaining ground as a preferred methodology.

Report findings also underscore the importance of adherence to industry standards such as the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF). Such frameworks aim to bridge the protection gaps and enable organizations to ensure the security of their sensitive content communications.

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.