Kiteworks

Executive Summary

2022 Sensitive Content Communications Privacy and Compliance Report

Kiteworks' 2022 Sensitive Content Communications Privacy and Compliance Report is based on findings from a detailed survey of IT, security, privacy, and compliance leaders representing 15 different countries.[1] The objective of the survey was to identify key challenges and trends when it comes to how organizations govern and secure sensitive content communications.

The report comes at a time when the average cost of a data breach now exceeds $4 million, according to IBM and Ponemon Institute.[2] Regulatory bodies and government entities recognize the risk breached data poses to organizations, and we have seen significant growth in compliance standards in recent years. Depending on their industry and the geographical scope of operations, organizations must demonstrate their technology tools are compliant with those standards as well as produce audit trails that demonstrate adherence to governance tracking and controls around who accesses sensitive content, with whom it is shared, when was it updated and shared, on what devices it was shared, and where it is stored.

One of the foremost takeaways from the report is that a majority of organizations are inadequately protected against third-party security and compliance risks related to sensitive content communications. There are numerous reasons behind this issue.

Complexity, Silos, and Inefficiencies

Most organizations share sensitive content with a long list of third-party entities. Two-thirds of organizations do so with more than 1,000 third parties, while one-third have over 2,500. The complexity of governing and securing these sensitive content communications is heightened due to all organizations in the survey admitting to using numerous communication channels, including email, file sharing, web forms, file transfer and automation protocols, and application programming interfaces (APIs). Email and file sharing are most used, though other communication protocols were frequently cited as well.

67%

use 4+ different systems to track, control, and secure content communications

60%

ask the sender to send an unencrypted file to a shared drive link if an email cannot be decrypted

30+

Almost half spend 30+ staff hours monthly dealing with incoming emails that cannot be decrypted

Security Gaps

Secure content communications requires numerous governance and security protocols. Encryption of private data in transit and at rest should be a requisite. But a majority of organizations admit that they do not encrypt all their sensitive content communications. Insider threats remain a key concern—and rightfully so (more respondents ranked it their number one security concern than any other security concern)—for many organizations. But over half in the survey indicate they do not perform data loss prevention (DLP) scans on all outgoing emails. Comparable findings exist for incoming email, with many failing to utilize antivirus, advanced threat prevention, and other security technologies.

53%

do not encrypt all sensitive content communications with third parties

54%

do not perform DLP scans on all outgoing email

88%

do not encrypt all communications with third parties

Less than 50%

apply zero-trust security principles to file transfer and automation, web forms, and APIs

Risk Management

Both security and compliance risks can be a serious challenge for organizations. Disaggregated and siloed content communications protocols and technologies and the lack of metadata that provides a centralized pane of glass and management platform create substantial risk. This is the likely reason over half of the respondents said their organizations are not adequately protected against third-party risk when it comes to sensitive content communications. Many believe existing systems and processes require significant improvement or should be thrown out and rebuilt anew.

51%

believe their organizations are inadequately protected from sensitive content communications with third parties

41%

admit that their sensitive content communication systems and processes either require significant improvement or need to be replaced altogether

Nearly 2/3

have a formal risk management program in place for vetting and auditing third-party vendors and suppliers

Compliance

All organizations must comply with varying regulations and standards. These compliance requirements are related to risk management and the aim of maintaining an acceptable level of risk based on cyber insurance and other factors. The majority of respondents must compile compliance reports for more than seven regulations or standards annually. These typically take a significant amount of time and resources to compile. Yet, 89% of respondents reveal that their compliance reporting is not fully accurate.

89%

say their compliance reports are not fully accurate

52%

indicate they do not manage and monitor all content communications in the cloud

50%+

list HIPAA, PCI DSS, CCPA, GDPR, and DPA (France) as compliance regulations/standards with which they must comply

Takeaways

Data remains a key focus area for cybercriminals and nation-states. Gaining access to sensitive content pay can result in a significant impact—both on individuals and organizations. Beyond the financial impact of losing confidential IP and data exposing mission-critical corporate strategies and secrets, the latter can suffer severe brand reputation damage that has long-lasting implications. Noncompliance penalties and fines with regulatory standards also incur a significant cost—not to mention the brand degradation that often comes with them as well.

The 2022 Sensitive Content Communications Privacy and Compliance Report confirms that sensitive content communication security and compliance risks are a real challenge for many organizations. Disparate toolsets and the lack of governance tracking and controls—including centralized metadata—make it difficult for organizations to manage these security and compliance risks. For more insights, download the full report today.

References

[1] "2022 Sensitive Content Communications Privacy and Compliance Report," Kiteworks, April 13, 2022.

[2] "Cost of a Data Breach Report 2021," IBM and Ponemon Institute, July 2021.

Kiteworks