Kiteworks

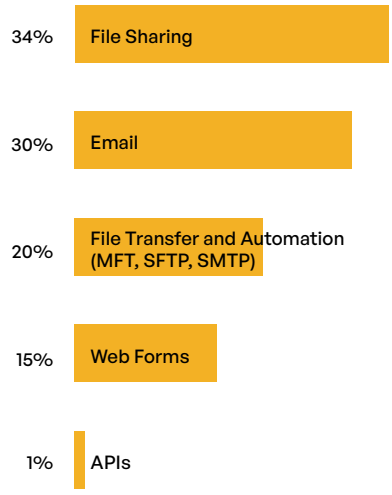
Sensitive Content Communications Privacy and Compliance in Financial Services

"2022 Sensitive Content Communications Privacy and Compliance" Report

FINANCIAL SERVICES BRIEF

Data is at the heart of virtually every financial services institution. Financial firms are literally built on data. New business opportunities and growth are possible because of artificial intelligence (AI) and data analytics. How all this data is captured, shared, transferred, and stored plays a crucial role in both the day-to-day operations as well as the long-term innovation of a financial services organization.

What Sensitive Content Communications Channel Poses the Greatest Risk?



Security and Compliance Governance

These activities must be strictly governed by security and compliance standards. Privacy regulations, such as the EU's General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), and the California Consumer Privacy Act (CCPA), control how personally identifiable information (PII) and protected health information (PHI) are captured, shared, used, and stored.

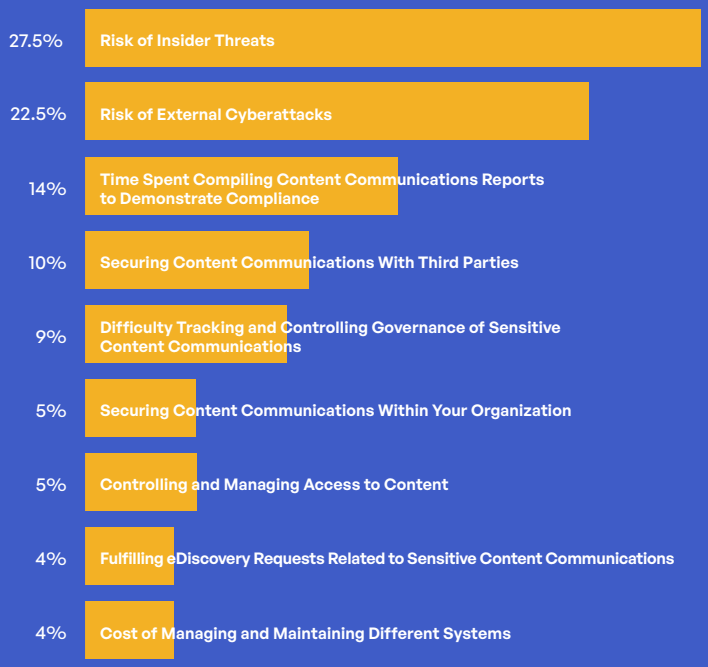
Compliance also comes into play when customer information is shared with other financial institutions to syndicate large commercial loans and other financial transactions. Much of the information shared between financial firms can be done so using automated sharing and transfer, such as the generation of customer statements and regulator fraud and AML reports, loan processing, credit card transactions, among others.

Third-party Sensitive Content Communications

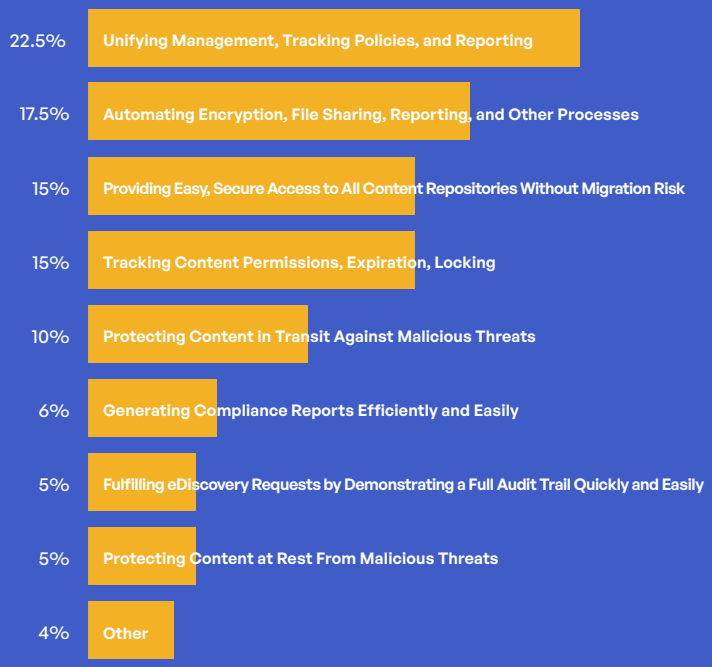
Management of third-party risk as it relates to privacy, compliance, and security is a critical requirement for financial institutions—from bank and investment firms to insurance companies and real estate firms. Many of the data-related regulations and standards specify certain requirements around data sovereignty and supervision.

Getting the right governance tracking and controls in place to ensure compliance and security of data is still a challenge for many financial firms based on a survey of global IT, security, privacy, and compliance professionals. One of the biggest challenges involves the sharing and transfer of data with third parties. The following data findings were derived from a survey of IT, security, privacy, and compliance leaders conducted in early 2022. The below analysis examines only findings from those in the financial services industry sector.

What Are Your Top Concerns in Managing Sensitive Content Communications?



What Are Your Top Priorities Around Third-party Sensitive Content Communications?



Governance, Risk, and Compliance Survey Findings

Based on findings from a survey conducted by Kiteworks and Survey Pacific in early 2022, financial services organizations are dissatisfied with their governance technologies and processes surrounding sensitive content communications.[1] Almost one-third indicate that either a new approach or significant improvements are required. One reason may be related to the fact that many lack technologies and processes for measuring risk.

Third-party risk management of sensitive content communications is seen by a large number (41%) as an area of concern. Half believe their organizations are inadequately prepared to address these risks. One of the gaps involves the cloud, where 43% either do not or only manage and monitor some of their content communications in the cloud.

The survey also found that financial institutions spend significant time and resources demonstrating compliance through audits and reports. And despite their focus on compliance findings, only 20% feel their compliance reports are fully accurate.

Governance

7 out of 10

indicate they use 4 or more systems for tracking, controlling, and securing sensitive data communications with third parties

32.5%

believe their governance and protection of third-party content communications either requires a new approach or requires significant improvement (another 35% say some improvement is needed)

35%

have technologies and processes in place to measure risk associated with third-party content communications (64% plan to do so)

Risk Management

52.5%

use antivirus and antispam technologies to verify incoming data communications from third parties (highest of all industry sectors)

60%

use DLP for file sharing and file transfer with third parties (33% higher than all-industry average)

51%

encrypt 75% or more of their content communications with third parties

41%

indicate their risk management and security of third-party content communications requires a new approach or significant improvement

50%

believe their organization is not well-protected against third-party content communication risks

43%

either do not or only manage and monitor some content communications in the cloud

Compliance

62.5%

must generate over 7 compliance reports annually

51%

spend over 40 hours generating each compliance report

20%

only 20% feel their compliance reports are fully accurate, with 18.5% indicating they are only somewhat accurate or inaccurate in various places

Kiteworks Private Content Network Provides Governance, Compliance, and Security

Kiteworks enables financial services organizations to create a dedicated Private Content Network (PCN) of internal and external digital communications that ensures privacy protection and compliance for sensitive information. When cybercriminals or nation-states access customer and financial data, the impact on a financial firm can be dramatic. According to IBM and the Ponemon Institute, individual data breaches of PII, PHI, and other sensitive content in financial services cost an average of $5.72 million.[2]

Kiteworks helps commercial and wholesale financial institutions to safeguard processing of business payrolls, credit card transactions, and wealth manager moves. For retail financial firms, they can protect and audit content transfers when delivering statements and client application documents. Unifying, tracking, controlling, and securing PII and financial data from the Kiteworks platform provides a single pane of glass for sharing and transferring sensitive information that is fully secure and compliant with regulations.

For these and other highlights from Kiteworks' "2022 Sensitive Content Communications Privacy and Compliance" report, download a copy.

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, 2021.

Kiteworks