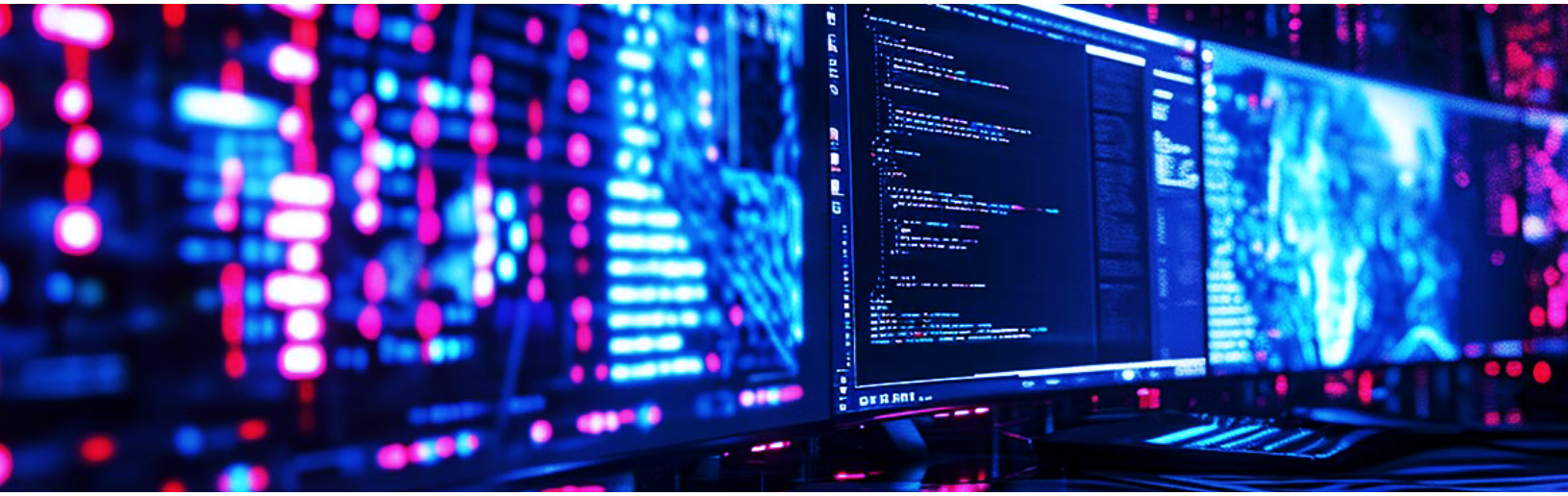
Kiteworks

# Kiteworks 2024 Sensitive Content Communications Privacy and Compliance Report

## Protecting Sensitive Content Communications

EXECUTIVE SUMMARY



**The 2024 Kiteworks Sensitive Content Communications Privacy and Compliance Report provides a detailed examination of current data security and privacy practices worldwide. With contributions from 572 IT, cybersecurity, and compliance leaders, the report highlights the importance of protecting sensitive information, including personally identifiable information (PII), protected health information (PHI), financial data, and intellectual property. The report underscores the devastating impact of breaches, which can result in financial loss, reputational damage, regulatory penalties, and operational disruptions.**

## Methodology Used in the Report

The report is based on a comprehensive survey conducted by Centiment between February and March 2024, encompassing 33 questions on data security, privacy, and compliance. Responses were gathered from professionals across eight countries in North America, Europe, the Middle East, Africa (EMEA), and the Asia-Pacific regions, representing various industries such as security and defense, manufacturing, healthcare, financial services, government, and education. The diverse pool of respondents ensures a broad perspective on the challenges and priorities in sensitive content protection.

# Key Findings From Kiteworks Survey Report

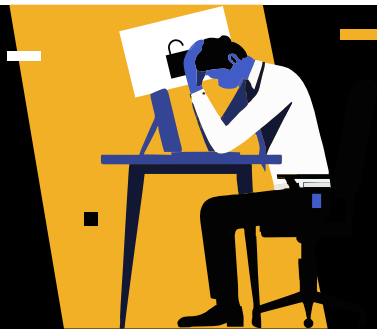
## 1. Security Risks Associated With Sensitive Content

Sensitive content is increasingly targeted by cybercriminals. The report found that nearly one-third of respondents experienced seven or more external malicious hacks in the past year. Some of the more salient findings included:

**32%**
of respondents reported seven or more breaches

**68%**
Higher education, security and defense, and oil and gas sectors had over 68% of respondents experiencing multiple breaches

**28%**
Pharmaceuticals and life sciences companies had only 28% of respondents reporting four or more breaches



## 2. AI Cyber Risks and Sensitive Content Communications

AI technologies, particularly Generative AI (GenAI) and large language models (LLMs), present significant security challenges. Nearly half of cybersecurity leaders are concerned about third-party access to sensitive data through AI tools, with fears of data breaches and erroneous decision-making by AI systems. Other pertinent findings included:

**48%**
of respondents find it challenging to apply zero-trust principles across both on-premises and cloud environments

**45%**
of organizations have not yet achieved zero trust with content security

Only **35%** of U.K. respondents & **39%** of respondents from the Middle East and Asia-Pacific regions have implemented zero-trust measures


## 3. Compliance Risks and Sensitive Content Communications

Navigating data privacy regulations is increasingly complex, with laws like the GDPR and CCPA requiring constant adaptation. The report reveals that 93% of organizations have had to rethink their cybersecurity strategies in response to evolving regulations.[1] Some of the more relevant findings included:

**93%**
of organizations had to rethink cybersecurity strategies due to new regulations[1]

Only **11%**
of respondents claimed no improvement was needed in managing compliance risk

**43%**
of organizations admitted being unable to track, control, and report on all external content exchanges

## 4. Role of Human Error in Data Breaches

Human error is a significant risk factor, accounting for 68% of breaches. To mitigate this, organizations should implement regular training, multi-factor authentication (MFA), strict access controls, comprehensive data encryption, and robust incident response plans. Key findings included:

**End-users account for 68% of errors leading to data breaches**

**Industries like healthcare and finance are particularly vulnerable to user-related breaches**

## 5. Data Privacy and Compliance and Sensitive Content Communications

The report highlights the high cost of data breaches, with legal fees often exceeding $2 million annually and even $7 million depending on the circumstances. Proper data classification is essential, yet many organizations struggle with this. A few of the findings included:

**60%**

of respondents reported spending more than $2 million annually on legal costs related to data breaches

**49%**

of organizations claimed that 75% or more of their unstructured data is tagged or classified

**41%**

of respondents said the GDPR and U.S. state privacy laws are their top two areas of focus when it comes to privacy and compliance

## 6. Compliance and Risk Management and Sensitive Content Communications

Compliance reporting remains a challenge, with many organizations unable to track and report all external content exchanges. The report suggests investing in advanced tools and processes to reduce the burden of compliance reporting and enhance security practices. Some of the findings included:

**53%**

of respondents prioritize ISO standards

**42%**

focus on NIST 800-171

**62%**

of organizations spend over 1,500 staff hours annually on compliance reporting

## 7. Cybersecurity and Risk Management and Sensitive Content Communications

Achieving zero trust for content security is crucial yet challenging. The report emphasizes the importance of advanced security measures, including encryption, threat detection, and security awareness training. Effective tracking and control of sensitive content access are also critical.

**45%**
of organizations have not yet achieved zero trust for content security

Only **16%**
of organizations can track and control access to content consistently

**56%**
of respondents indicated some improvement is necessary in their sensitive content communications security

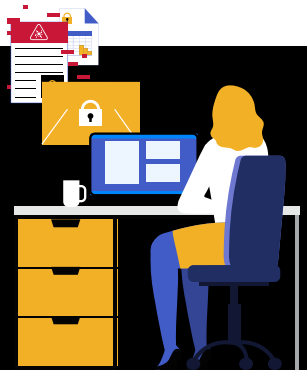
## 8. Operational Processes and Sensitive Content Communications

Managing third-party risks, consolidating communication tools, and addressing log reconciliation challenges are essential for securing sensitive content. The report recommends reducing tool sprawl, implementing robust tracking mechanisms, and ensuring compliance with data privacy regulations. Key findings included:

**2/3**
of respondents exchange sensitive content with over 1,000 third parties

**7+**
Organizations using more than seven communication tools experienced higher frequencies of data breaches

**48%**
of organizations must reconcile over 11 logs, with 14% needing to consolidate more than 20 logs



## Effective Strategies for Securing Sensitive Content Communications

**In light of the eight above takeaways, organizations should prioritize:**

**1. Consolidating Communication Tools:**
Reducing the number of tools can lower breach risks and improve efficiency

**2. Implementing Content-defined Zero Trust:**
Strict access controls and continuous monitoring are essential using zero-trust principles

**3. Developing Private Content Networks:**
Isolating sensitive communications enhances security

**4. Enhancing Security Measures:**
Investing in encryption, MFA, and threat detection

**5. Improving Compliance Reporting:**
Automating processes and ensuring robust tracking

**6. Prioritizing Data Classification:**
Implementing systems to categorize and protect high-risk data

## Conclusion

The 2024 Kiteworks Report underscores the critical need for robust data security and compliance strategies. By addressing the identified challenges and adopting the recommended strategies, organizations can better protect their sensitive content, ensure compliance, and mitigate risks in today's complex digital landscape.

For further insights, access the 2024 Report webpage featuring regional and industry briefs, infographics, and a Kitecast podcast episode.

[1] "Despite increased budgets, organizations struggle with compliance," Help Net Security, May 24, 2024.