Kiteworks

# Europe: 2023 Sensitive Content Communications Privacy and Compliance

## Regional Findings and Takeaways

### HIGHLIGHTS

| | | |
|---|---|---|
| **Communication Tools in Use** | **22%** | 7+ |
| | **27%** | 6 |
| | **35.5%** | 5 |
| | **15.5%** | Less than 4 |
| **Average Annual Budget for Communication Tools** | **16%** | $500,000+ |
| | **17%** | $350,000 – $499,999 |
| | **34%** | $250,000 – $349,999 |
| | **24.5%** | $150,000 – $249,999 |
| | **9%** | $100,000 – $149,999 |
| **Number of Third Parties With Which They Exchange Sensitive Content** | **15%** | 5,000+ |
| | **25%** | 2,500 – 4,999 |
| | **49%** | 1,000 – 2,499 |
| | **5%** | 500 – 999 |
| | **6%** | Less than 499 |
| **Attack Vector Weighted Score (based on ranking)** | **100** | Password/Credential Attacks |
| | **93** | Cross-site Scripting |
| | **81** | Session Hijacking |
| | **71** | Denial of Service |
| | **70** | SQL Injection |
| | **70** | DNS Tunneling |
| | **65** | Rootkits |
| | **61** | Phishing |
| | **59** | Zero-day Exploits and Attacks |
| | **57** | URL Manipulation |
| | **55** | Malware (ransomware, trojans, etc.) |
| | **52** | Man in the Middle |
| | **19** | Insider Threats |
| **Exploits of Sensitive Content Communications in Past Year** | **11%** | 10+ |
| | **25%** | 7 – 9 |
| | **46%** | 4 – 6 |
| | **16%** | 2 – 3 |
| | **2%** | 1 |
| **Level of Satisfaction With 3rd-party Communication Risk Management** | **15%** | Requires a New Approach |
| | **37%** | Significant Improvement Needed |
| | **29%** | Some Improvement Needed |
| | **19%** | Minor Improvement Needed |

## Surge of Cyberattacks in Europe

Europe is grappling with an alarming surge in cyberattacks, highlighting the pressing need for enhanced security measures. Check Point Research's 2022 Cyber Security Report found Europe experienced a 26% increase in cyberattacks over the previous year.[1] The United Kingdom, Italy, and Germany emerged as the primary targets, while the manufacturing sector (25%) and finance and insurance industry (18%) bore the brunt of these malicious activities.[2] Ransomware attacks (26%) and unauthorized server access (12%) stood out as the most prevalent attack types during this period. With confidential data at stake, European organizations must prioritize privacy and compliance to combat these mounting cyber threats effectively.

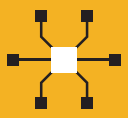
## Disaggregated Sensitive Content Communication Tools

European organizations face a growing challenge in safeguarding their sensitive content communications due to the use of multiple and scattered tools. Kiteworks' 2023 Sensitive Content Communications Privacy and Compliance Report reveals that 84.5% of European respondents rely on five or more communication tools for sending and sharing sensitive content. The disaggregated tools issue significantly complicates data security, making European organizations vulnerable to cyber threats as well as regulatory compliance challenges. The "tool soup"also results in substantial capital expenditure, with one-third of European organizations investing $350,000 or more annually—and this does not include the related OpEx costs to manage all the toolsets.

**84.5% of European organizations use five or more communication tools.**

## Third-party Content Communication Risk in Europe

Disaggregation of file and email communication tools makes it difficult to create governance tracking and controls. The communication channel cited most often by respondents as having the highest risk was email (ranked 1, 2, or 3 by 51% of respondents), followed by application programming interfaces (APIs) and web forms (both ranked 1, 2, or 3 by 45% of respondents).



**81% of European organizations believe they need to improve their approach to mitigating the risks associated with third-party content communication.**

Given the substantial volume of file and email data communications with third parties, heightened governance tracking and controls are imperative. The report underscores a unanimous sentiment among organizations that improvement is needed, with 81% recognizing the need to enhance their approach to mitigating third-party content communication risks. Of this group, 15% call for a new approach, while 66% emphasize the need for some or significant improvement.

Their concerns are well-founded. 82% experienced four or more sensitive content communication exploits in the past year. Although lower than North America at 96%, this statistic exceeds that of the Asia Pacific region (at 80%).

## The Need for Digital Risk Management

European organizations are grappling with the adoption of digital risk management practices, according to survey responses. For example, only 24% track and record third-party access to sensitive files and folders across all departments today. Another 35% track such only for certain departments, while 27% track only for specific content types.

When it comes to digital rights management priorities, European organizations consider protecting content in motion from malicious threats as their top priority (29% ranked it one or two), which was followed by fulfilling eDiscovery requests by demonstrating full audit logging quickly and easily (27% ranked this either number one or two).

## Kiteworks Private Content Network for European Organizations

Kiteworks Private Content Network enables European governmental agencies and public sector businesses to protect their sensitive content communications while enabling them to demonstrate compliance with regional and international regulations. With Kiteworks, European organizations can centrally manage file and email data policies using comprehensive access controls. For those concerned about data sovereignty requirements, Kiteworks can be configured to store data in specific geographic locations, allowing European organizations to comply with data residency requirements found in GDPR and other regulations. Audit logging details all user activities, including file access, file shares, and file transfers, enabling European organizations to demonstrate compliance with data privacy regulations like GDPR, PCI DSS, and others.

[1] "2022 Cyber Security Report," Check Point Research, January 2023.

[2] "The IBM Security X-Force Threat Intelligence Index," IBM, February 2023.

**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.