Kiteworks

2023 Forecast for Managing Private Content Exposure Risk

15 Predictions for Sensitive Content Communications Based on Cybercrime, Cybersecurity, and Compliance Insights

REPORT

Introduction: Understanding Private Content Exposure Risk

Organizations must manage the risk of data privacy exposure, carefully navigating a minefield ever-evolving cyber threats, legislation, and technology options. Our 2023 Forecast identifies 15 data privacy and compliance predictions that IT, security, risk, and compliance leaders need to know to proactively manage their risk postures in 2023. These predictions reflect forward-thinking analysis from Kiteworks thought leaders who possess decades of experience in cybersecurity, compliance, and technology.

Data sprawl, including private content, remains on a steep growth trajectory, as more organizations adopt data-driven business models. Virtually every departmental function, in every industry and sector (public and private), has witnessed explosive growth in data volume, with no signs of slowing. This includes private content, previously stored on-premises or generated and shared through manual processes, but now easily accessed and shared from any device or location. As private content that is more accessible is more susceptible to unauthorized access, having comprehensive tracking and controls in place for managing security and compliance risk is crucial.

This Forecast aims to help organizations to manage this risk by highlighting the latest cyber threats posed by malicious or careless employees, cybercriminals, both lone actors and organized crime syndicates, and rogue nation-states. The Forecast takes into consideration various cybersecurity technology and practices, as well as evolving compliance standards, all designed to protect private content.

Growth in Sensitive Content Communications

1. Sensitive Data-sharing, While Risky, Is a Business Requirement

Organizations will continue to leverage data-sharing to realize competitive advantages. Some of this data is sensitive content such as personally identifiable information (PII), protected health information (PHI), financial records, merger & acquisition details, research & development (R&D), and intellectual property (IP). The latter includes information on manufacturing schedules, product design, marketing and go-to-market strategies, and DNA sequences, among others. Digital exchange of this private data occurs intra-departmentally as well as with third parties like consultants, vendors, partners, and regulators.

All of this translates into rapid growth in file sharing and managed file transferring (MFT). The enterprise file synchronization and sharing marketing is forecasted to grow at a compound annual growth rate (CAGR) of 28.1% through 2027,[1] while the MFT market is expected to grow at a 28.3% CAGR over the same timeframe.[2]

Trust is a key element in data-sharing. Gartner indicates that through 2023, organizations that can instill trust with partners and customers will enable them to participate in 50% more customer and partner ecosystems that will lead to expanded revenue-generation opportunities.[3] As data, including sensitive content, is sent, shared, and received using various communication channels—email, file sharing, managed file transfer, web forms, and application programming interfaces (APIs)—organizations require a solution that consolidates governance tracking and control across each of them, ensuring the data is protected and processes are compliant with regulations.

2. Insecure Emailing of Sensitive Content Remains a Significant Risk

Even though adoption rates for communication channels such as chat and SMS continue to climb, email remains a mainstay for many organizations—especially for communications with third parties. Email volumes, as a result, continue to spike, with the total number of emails sent in 2023 expected to grow nearly 12% over 2020 (hitting 347.3 billion).[4] Higher email volumes inevitably translate to higher probability of interception. For outbound email alone, according to a recent study by Ponemon Institute, almost one-quarter (23%) of organizations report 30-plus security incidents involving employee use of email every month.[5] A significant number of these were related to misdelivery—namely, email sent to an unintended recipient—which Verizon attributed to around 15% of all data breaches in 2021.[6]

Trust is a key element in data-sharing. Gartner indicates that through 2023, organizations that can instill trust with partners and customers will enable them to participate in 50% more customer and partner ecosystems that will lead to expanded revenue-generation opportunities.

Cyberattacks Expose Private Data

3. Multitenant Cloud Hosting Provides Cyberattackers With Fertile Ground

Cyberattackers are increasingly targeting multitenant solutions in the cloud where they can create sandboxes to pinpoint vulnerabilities and develop corresponding sophisticated exploits. For a few thousand dollars, bad actors can acquire a cloud instance for Microsoft or other software providers, pinpoint vulnerabilities, and develop complex exploits used to intercept sensitive content moving across the software supply chain. In addition, because the data of different tenants sits side by side in a multitenant cloud environment, a security failure with one tenant can expose systems, applications, and content of other tenants residing in the same instance.[7]

Organizations need to opt for single-tenant hosting solutions with a dedicated server that is isolated from other tenants. But that is just the start. They must decide who is going to manage the server and take full responsibility for securing the content the server contains. When businesses and their cloud access security broker (CASB) providers share responsibilities, assumptions are made about "who does what" that can lead to security gaps and misconfigurations. This allows anyone with an internet connection to access the private content on these servers. Organizations need to therefore ensure the data on these single-tenant cloud solutions is encrypted, both in storage and when transferred, with sole encryption key ownership and in compliance with requirements such as the National Institute of Standards & Technology (NIST) Cybersecurity Framework (CSF), International Organizational for Standardization (ISO), and SOC 2.

4. Third Parties in the Supply Chain Ratchet Up Risk

Third-party suppliers, contractors, legal counsel, and other external entities will continue to grow in scope as a target. Private information that is shared with third parties across the different communication channels can be exploited for ransomware, IP theft, and extortion (public shaming, brand degradation). In a survey published earlier this year, PwC found that more than half of enterprises either just started or are still planning to implement third-party risk management practices.[8] Not surprisingly, Verizon in its latest Data Breach Investigations Report found that the supply chain was responsible for 62% of system intrusions and 39% of data breaches were the result of breached business partners.[9] These statistics should remind organizations that their cybersecurity policies, practices, and technology investments are only as defensible as their weakest supply chain partner.

Bad actors can acquire a cloud instance for Microsoft or other software providers, pinpoint vulnerabilities, and develop complex exploits used to intercept sensitive content moving across the software supply chain.

5. The Axis of Rogue Nation-states Continues to Expand

Cyber-espionage attacks by rogue nation-states rose dramatically in 2022. Attacks on critical infrastructure in fact jumped from 20% of nation-state attacks to 40% over the past year.[10] Rogue nation-states—comprised of North Korea, China, Russia, and Iran[11]—will continue to attack high-value targets such as supply chains that offer access to hundreds or thousands of organizations. Organizations must remain diligent in securing their sensitive content communications against these four nation-states and their increasing prowess to develop sophisticated exploits.

6. Cyberattackers Get More Sophisticated—and More Dangerous

While lone malicious actors still exist, cyber-hacking has become a multibillion-dollar enterprise with R&D budgets and organizational hierarchies, and private data—both at rest and in transit—is a prime target for most. These well-funded criminal organizations employ advanced technologies such as artificial intelligence (AI) to conduct reconnaissance, infiltrate applications and networks, navigate across them to locate sensitive content while avoiding detection, and to intercept that sensitive content when it is sent, shared, received, and/or stored. Their use of advanced persistent threats enables AI, machine learning, and automation that obfuscate their presence within the network or applications and remain undetected for months, pilfering terabytes of private content for extortion and/or sale on the dark web.

Well-funded criminal organizations employ advanced technologies such as artificial intelligence (AI) to conduct reconnaissance, infiltrate applications and networks, navigate across them to locate sensitive content while avoiding detection, and to intercept that sensitive content when it is sent, shared, received, and or stored.

Cybersecurity Strategies and Technology Evolve to Address Risk Inherent in Sensitive Content Communications

7. Content-defined Zero Trust and a Private Content Network for Sensitive Content Communications

Most organizations either are in the process of adopting or have already adopted a zero-trust security strategy in response to the deficiencies of perimeter security and an evolution in the sophistication of cyberattacks. Zero trust assumes that users, applications, and infrastructure cannot be trusted and employ least-privilege access policies across each of them to safeguard their most private content.

The push for zero trust at the federal level, in the form of Executive Order 14028 and subsequent memorandums, will translate into expanded zero-trust standards in the private sector.[12] Additionally, with sensitive content the ultimate target of cybercriminals, there is growing recognition for content-defined zero trust. Currently, unstructured data that is sent or shared without appropriate tracking and controls in place presents significant risk. This gives rise to the Private Content Network, a dedicated system that secures digital communications of highly sensitive information—both sent and shared internally and externally—using content-policy zero trust to govern content assets, users, and actions.[13]

8. Least-privilege Access and Authentication Become Non-negotiable

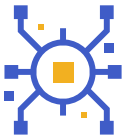
Least-privilege access and authentication are foundational requirements of zero trust. In its latest M-Trends Report, Mandiant found that stolen credentials comprise 11% of the initial infection vectors.[14] Using stolen credentials, which can be obtained in any number of ways (dark web, phishing, etc.), cybercriminals and rogue nation-states gain access to your network, applications, and content. Organizations cite numerous potential impacts due to stolen credentials, with loss of sensitive data at the top of the list (35%).[15]

To counter identity access and authentication risk and credential theft, organizations require a zero-trust approach that applies least-privilege policies using multifactor authentication (MFA) to mitigate the threat of credential theft. MFA is now the de facto method for network and application access. And regardless of where your private content resides (on-premises, in a private cloud, or in the public cloud), MFA—including SAML 2.0 and Kerberos SSO—is critical for tracking and controlling access.

With sensitive content the ultimate target of cybercriminals, there is growing recognition for content-defined zero trust. Currently, unstructured data that is sent or shared without appropriate tracking and controls in place presents significant risk.

9. More Businesses Will Choose Sole Ownership of Their Encryption Keys

Key encryption and key management will become a bigger concern for cloud providers and their end customers. Many end-customers only co-manage their encryption keys and thus law enforcement and security agencies, lawyers, and other entities can "bypass" the end-customer and subpoena cloud providers for their encryption keys and they must oblige, providing access to a customer's private content. The European Union and individual European countries have responded, enacting the French Blocking Statute and Standard Contractual Clauses in the General Data Protection Regulation (GDPR) to protect their citizens' privacy. The U.S. federal government, looking to prevent a security concern from becoming a diplomatic concern, recently issued an Executive Order dubbed "Privacy Shield 2.0" that promises safeguards to protect the private information of EU residents.[16]



10. Mitigating Vulnerabilities in Third-party Libraries and Software Becomes Even More Critical

The number of Common Vulnerabilities and Exposures (CVE) published in 2022 is 35% higher than the number published in 2021.[17] As a significant percentage of software code is open sourced, organizations must continuously assess their software supply chain. To mitigate the risk posed by CVEs and thereby reduce vulnerability exploit and impact severity, organizations are proactively—and more aggressively—hardening and adding multiple security layers to their software solutions.[18] And as part of their risk management approach, they may even rescore a CVE based on those mitigating security factors. (CVEs are scored on a scale of 1 to 10 based on the severity of the risk they pose.)

11. AI Is Becoming More Widely Adopted to Detect Anomalies in Data Shares and Transfers

AI holds almost limitless potential across the cybersecurity landscape, including advanced threat detection and protection of sensitive content. Specifically, AI technology can detect anomalous data shares and transfers. By integrating AI capabilities with sensitive content communications and security operations center (SOC) tools, such as security information and event management (SIEM) and security orchestration, automation, and response (SOAR), security personnel and incident response teams can receive real-time alerts so they can take immediate action to lessen the impact of malicious activity.

12. Organizations Will Focus More Resources on Security Hardening and Integrating Security Investments

Integration and consolidation of cybersecurity technology investments remains a key focus for many organizations, and this is certainly true when it comes to sensitive content communications. IT, security, risk, and compliance teams operate more efficiently and effectively when they can consolidate threat intelligence and compliance data into a single dashboard.[19] Embedding antivirus capabilities to check for malware and other viruses contained within emails, file sharing, managed file transfer, and APIs is an important starting point. Integrating network and web application firewall and intrusion prevention system (IPS) capabilities creates layers of security that protects sensitive content behind tiers of services using least-privilege access controls.

Automating cybersecurity processes is just as crucial. Content disarm and reconstruction (CDR) automatically detects and removes executable content within incoming email, file sharing, MFT, and APIs while delivering the content to the recipient. Data loss prevention (DLP) checks outbound email, file sharing, MFT, and APIs to prevent both accidental and intentional data leakage. Building API connections with SOC monitoring and incident response tools, such as SIEM and SOAR, enables SOC teams to monitor sensitive content communications and receive real-time alerts when attacks or anomalies occur.

AI technology can detect anomalous data shares and transfers. By integrating AI capabilities with sensitive content communications and SOC tools, security personnel and incident response teams can receive real-time alerts so they can take immediate action to lesson the impact of malicious activity.

Manage the Risk by Tracking and Controlling the Digital Exchange of Private Data

13. Keeping Pace With New and Expanded Data Privacy Regulations

Virtually every country in the world has enacted some form of a data privacy law that regulates how information is collected, how data subjects are informed of that collection, and how the data will be used. Businesses that fail to follow these myriad laws are subject to fines and penalties, lawsuits, and even prohibition of doing business in a certain jurisdiction. The negative publicity surrounding a business's violation of a data privacy law can also have a detrimental impact on its brand.

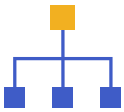
The data privacy landscape is currently broad and will continue to expand. HIPAA (Health Insurance Portability and Accountability Act) regulates data privacy as it relates to protected health information (PHI). FISMA, GLBA, PCI DSS (Payment Card Industry Data Security Standard), among others, stipulate the protection of financial information and personally identifiable information (PII). The EU's GDPR (General Data Protection Regulation) was one of the first attempts to regulate data privacy across multiple regions. In the absence of a national data privacy regulation in the U.S., various states have recently implemented data privacy laws. California was the first with the passage of CCPA (California Consumer Privacy Act). Four other states have passed similar data privacy legislation that will be enacted in 2023:[20] Virginia (Consumer Data Protection Act, January 1, 2023), Colorado (Privacy Act, July 1, 2023), Utah (Consumer Protection Act, December 31, 2023), and Connecticut (Data Protection Act, July 1, 2023).

In response to the enactment of these four new state laws as well as continued global focus on data privacy, there will be a growing focus in 2023 on governance tracking and controls around data privacy as well as how that data is protected when it is sent, shared, received, and stored. Noncompliance with permutations in existing data privacy laws and new ones is not optional.

14. Geofencing of Private Data Exchange Will Increase

Security and data privacy concerns between countries are a growing requirement for global businesses. The need to protect and govern private data shared within specific jurisdictions and between jurisdictions has grown exponentially in recent years—both in terms of compliance regulations as well as security capabilities. To prevent unauthorized sends and shares of private data with specific geographical jurisdictions—both internally within an organization and externally with third parties—organizations must employ geofencing controls that block sends, shares, and receives of individual files and folders stamped with those jurisdictions. Data sovereignty controls constrain individual files to storage only in the data owner's home country. In addition to using block-lists and watch-lists, organizations will need to employ content-policy zero-trust tracking and controls.

The data privacy landscape is currently broad and will continue to expand with the addition of four new state data privacy laws in 2023 alone.



15. Adoption of Best Practice Cybersecurity Controls and Frameworks Becomes More Widespread

The influence of cybersecurity frameworks such as ISO 27001, NIST CSF, and SOC 2 will continue to expand in scope and adoption for both the public and private sectors. Adherence to the best practice standards contained in these frameworks enable organizations to manage their risk more effectively. Accordingly, as organizations assess the risk of sensitive content exposure, they will increasingly turn to cybersecurity frameworks to do so.

Some of the focus will be generated at the government level. For example, the zero-trust principles spelled out in U.S. EO 14028, and subsequent memorandums, include a keen focus on private data exposure. The same is true of the Cybersecurity Maturity Model Certification (CMMC) that uses NIST 800-171 and 800-172 as the basis for its practice controls pertaining to the exchange and storage of sensitive content within the U.S. Department of Defense (DoD) supply chain. At the same time, the private sector sees direct benefits from using cybersecurity frameworks, and their use to manage risk of private content exposure will continue to expand in 2023.[21]

Takeaways From Our Data Privacy Exposure Risk Forecast

The rapid maturation in the sophistication of cyberattacks by cybercriminals and rogue nation-states has pushed cybersecurity to the top of the priority list for most organizations. And with private data the target of many cyberattacks, organizations have been forced to rethink how they protect their sensitive content. The business value of data-sharing and the expanded supply chain landscape concurrently amplifies the risk of private data exposure. This requires organizations to have the appropriate security controls and practices in place to protect the digital exchange of sensitive content inside and outside their organizations.

Additionally, as different geographical jurisdictions expand existing data privacy regulations and pass new ones, the complexity of managing data privacy—and proving it to regulators—increases further. Organizations must institute more governance controls and tracking capabilities to demonstrate their sending, sharing, and use of private data complies with data privacy regulations in all the jurisdictions in which they operate.

Organizations will have a lot to keep in mind for 2023. Managing private data and mitigating its exposure must be a top priority. This requires a strategic compliance, governance, and security approach to your digital exchange of private data.

To prevent unauthorized sends and shares of private data with specific geographical jurisdictions—both internally within an organization and externally with third parties—organizations must employ geofencing controls.

References

[1] "Enterprise File Synchronization and Sharing (EFSS) Market: Growth, Trends, COVID-19 Impact, and Forecasts (2022-2027)," Mordor Intelligence, accessed November 9, 2022.

[2] "Managed File Transfer Market: Growth, Trends, COVID-19 Impact, and Forecasts (2022-2027)," Mordor Intelligence, accessed November 9, 2022.

[3] Laurence Goasduff, "Data Sharing Is a Business Necessity to Accelerate Digital Business," Gartner, May 20, 2021.

[4] "Number of sent and received e-mails per day worldwide from 2017 to 2025," Statista, February 2021.

[5] "Email Data Loss Prevention: The Rising Need for Behavioral Intelligence," Ponemon Insitute, May 18, 2022.

[6] "2022 Data Breach Investigations Report," Verizon, June 2022.

[7] Wayne Brown, Vince Anderson, and Qing Tan, "Multitenancy: Security Risks and Countermeasures," Network-Based Information Systems, September 2012.

[8] "2022 Global Digital Trust Insights," PwC, October 2021.

[9] "2022 Data Breach Investigations Report," Verizon, June 2022.

[10] "Microsoft Digital Defense Report 2022," Microsoft, accessed November 9, 2022.

[11] "Mandiant Cyber Security Forecast 2023," Mandiant, November 2, 2022.

[12] "How Federal Agencies Can Comply With the Data Requirement in Executive Order 14028," Kiteworks, February 2022.

[13] "Kiteworks Launches the Private Content Network," Kiteworks Press Release, August 11, 2022.

[14] "M-Trends 2022," Mandiant Special Report, February 2022.

[15] "Benchmarking Security Gaps & Privileged Access: Global survey of cybersecurity leaders," Delinea, September 2022.

[16] "FACT SHEET: President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework," The White House, October 7, 2022.

[17] Jason Villaluna, "2022 Trustwave SpiderLabs Telemetry Report," Trustwave, August 25, 2022.

[18] "Kiteworks Hardened Virtual Appliance Provides Multiple Security Layers to Dramatically Reduce Vulnerability Exploit and Impact Severity," Kiteworks, November 2022.

[19] Jim Boehm, et al., "Cybersecurity trends: Looking over the horizon," McKinsey, March 10, 2022.

[20] Thorin Klosowski, "The State of Consumer Data Privacy Laws in the US (And Why It Matters)," Wirecutter, September 6, 2021.

[21] Adamu A. Garba and Aliyu M. Bade, "An Investigation on Recent Cyber Security Frameworks as Guidelines for Organizations to Adopt," International Journal of Innovative Science and Research Technology, Volume 6, Issue 2, February 2021.

Kiteworks