Kiteworks

2025 Forecast for Managing Private Content Exposure Risk

12 Predictions for Sensitive Content Communications Based on Cybercrime, Cybersecurity, and Compliance Trends

REPORT

Executive Summary

The cybersecurity landscape in 2025 is characterized by a rapid escalation in the complexity and frequency of threats, coupled with increasingly stringent regulatory requirements. Sophisticated attacks targeting supply chains, the widespread misuse of artificial intelligence, and the global surge in data privacy regulations are among the top concerns for organizations. 75% of the world's population will have their personal data protected under privacy laws in 2025,[1] underscoring the urgency for businesses to implement robust, compliant data management strategies to mitigate risks and safeguard operations.

This report identifies 12 pivotal cybersecurity and compliance trends shaping the year ahead, emphasizing the convergence of data privacy, compliance, and technology-driven security measures. From the transformative impact of AI in both offensive and defensive cyber tactics to the critical vulnerabilities inherent in third-party partnerships and supply chains, organizations must proactively address these developments to stay ahead of adversaries. Examples in 2024 include Change Healthcare and AT&T, where significant gaps in software supply chain security resulted in the compromise of millions of user records. Secure content collaboration, real-time threat detection, and the adoption of integrated frameworks emerge as critical components of a resilient cybersecurity strategy.

To thrive in this evolving landscape, organizations face several strategic imperatives:

Utilize predictive tools like the Risk Exposure Index: Identification and prioritization of high-risk areas to ensure security investments are both effective and efficient based on measuring data breaches based on an algorithmic Risk Exposure Index.[2]

Invest in advanced, automated security systems: Automation is no longer optional. It is a necessity for reducing operational complexities, minimizing response times, and optimizing security operations in the face of growing threats.

Adopt AI-driven threat detection and response: As cybercriminals increasingly exploit AI, organizations must leverage predictive analytics and machine-learning tools to detect and mitigate threats before they materialize.

Reinforce compliance and governance frameworks: With global privacy regulations becoming more intricate, aligning security initiatives with compliance requirements is paramount to avoiding penalties and maintaining trust.

Mitigate third-party risks: The supply chain remains one of the weakest links in organizational security. Strengthening third-party risk management frameworks and vetting partners for security maturity is essential to address vulnerabilities effectively.

Focus on secure content collaboration: As sensitive data moves across organizational boundaries, secure content sharing and communication platforms are integral to reducing exposure.

Kiteworks' 2025 forecast serves as a comprehensive roadmap for business leaders, IT professionals, and security teams. It provides actionable insights and practical guidance to help organizations navigate the fast-evolving cybersecurity environment. By aligning security priorities with business objectives, fostering a culture of compliance, and investing in adaptive technologies, organizations can enhance their resilience against a dynamic threat landscape while driving long-term operational success.

Introduction

As organizations move into 2025, they will encounter unique cybersecurity challenges shaped by regulatory pressures and new technological risks. Increased digital transformation has led to unprecedented data volumes and exchange across networks, intensifying both risks and compliance requirements. Kiteworks' 2025 forecast outlines the security trends and practices organizations need to secure sensitive information effectively.

This report synthesizes insights from industry studies, expert analysis, and trend forecasts to provide a strategic overview of changing cybersecurity priorities. It covers critical areas such as global data privacy laws, vulnerabilities in software supply chains, and the role of AI in security operations. Each trend is examined with a focus on its impact on organizational resilience, regulatory compliance, and data security strategies.

Organized into trend analysis, recommendations, and strategic planning, this report explores 12 trends that shape the cybersecurity landscape. Each section addresses specific risks, challenges, and potential solutions, equipping organizations with insights to manage complex security concerns while meeting compliance demands. By providing these perspectives, Kiteworks aims to empower security leaders and professionals to build robust, adaptable cybersecurity frameworks for 2025.

Sincerely,

Patrick Spencer

Patrick Spencer, Ph.D.
VP of Corporate Marketing and Research
Kiteworks

1. Global Data Privacy Evolution

The global landscape of data privacy continues to evolve, reshaping compliance requirements for organizations worldwide. By 2025, Gartner projects that 75% of the world's population will be covered under modern data privacy regulations, driving businesses to adopt stringent data management and security practices.[3] From Europe's GDPR to frameworks in Brazil, India, and China, these regulations emphasize transparency, consumer rights, and cross-border compliance.

The fragmented nature of privacy laws is becoming increasingly complex in the United States. While federal privacy legislation like the American Privacy Rights Act (APRA) remains uncertain, state-level regulations are expanding rapidly. In 2025, eight more states, in addition to the five with laws already in effect, will go live with data privacy laws, including Delaware, Iowa, Nebraska, New Hampshire, New Jersey, Maryland, Minnesota, and Tennessee.[4] These laws enhance consumer rights, mandate explicit consent for sensitive data, and introduce stricter rules for automated decision-making.

Internationally, privacy laws are tightening across Asia-Pacific countries such as Australia, India, and Japan. Thailand, for instance, plans to update its Personal Data Protection Act to regulate AI use, reflecting a growing global focus on AI governance. Meanwhile, the EU-U.S. Data Privacy Framework aims to streamline cross-border data transfers, replacing the invalidated Privacy Shield, though challenges remain.

Businesses must also address broader shifts in digital marketing and data handling. The phasing out of third-party cookies by late 2024 will push organizations to rely on first-party data strategies. Additionally, stricter enforcement of privacy laws is anticipated, with regulators levying heavier fines for noncompliance. To navigate these challenges, organizations are investing in automated privacy management tools, designating privacy officers, and implementing robust data governance strategies.

Accordingly, artificial intelligence (AI) governance is emerging as a central focus for data privacy. Countries such as Thailand, Australia, and the European Union are incorporating specific AI regulations into their broader privacy frameworks. These rules emphasize transparency in AI algorithms, accountability for data use, and safeguards against bias and misuse. The European Union's AI Act, expected to be finalized in 2025, will introduce stringent requirements for high-risk AI applications, including clear documentation, data handling protocols, and human oversight.[5] Such regulations aim to balance innovation with ethical and privacy considerations, compelling organizations to rethink their AI strategies to align with compliance standards.

As of November 2024, the cumulative total of GDPR fines in 2024 is approaching $5.3 billion.[6]

2. Software Supply Chain Security

The increase in software supply chain attacks over recent years underscores the growing vulnerabilities within third-party software ecosystems. These attacks target interconnected systems to access sensitive data across various organizations. Notable incidents, such as the breaches involving MOVEit and GoAnywhere, expose the severe cascading impact a single compromised vendor can have on an entire industry, compromising the trust organizations place in their software suppliers. Cybercrime Magazine predicts that the global annual cost of software supply chain attacks will reach $60 billion in 2025 and will grow at a 15% year-over-year clip to $138 billion by 2031.[7]

To combat these evolving threats, organizations and governments are adopting more rigorous security measures, with an emphasis on building hardened security capabilities in the software that organizations use. A zero-trust security model is becoming the standard approach, requiring verification for every connection and data exchange across all networks and vendors. This minimizes the risk of malicious actors exploiting weak links in the supply chain to gain unauthorized access.

The Cybersecurity and Infrastructure Security Agency (CISA) has been instrumental in enhancing national cybersecurity through initiatives like real-time monitoring, threat intelligence sharing, and the promotion of software bills of materials (SBOMs). However, with the incoming Trump administration, there are indications of potential changes to CISA's structure and focus. Senator Rand Paul, who is expected to chair the Senate Homeland Security and Governmental Affairs Committee, has expressed intentions to significantly reduce CISA's powers, particularly concerning its efforts to counter disinformation.[8] Further, discussions within the administration suggest a shift toward a more business-friendly regulatory approach, which might lead to alterations in CISA's emphasis on certain cybersecurity measures.[9]

Given these potential changes, organizations should remain vigilant and adaptable. While CISA's current initiatives, such as SBOMs and cross-sector collaboration, have been pivotal in strengthening software supply chain security, it is crucial to monitor policy developments and adjust security strategies accordingly. Maintaining robust internal security practices and fostering private-sector collaborations will be essential to mitigate risks, especially if federal support undergoes significant modifications.

Best practices recommended by the National Institute of Security & Technology (NIST) and CISA include routine software updates, effective patch management, and in-depth risk assessments for all software suppliers. These steps contribute to a standardized, proactive approach to software supply chain security that strengthens resilience against an array of sophisticated cyber threats. Additionally, the continuous sharing of real-time threat intelligence is crucial in maintaining situational awareness and adapting security strategies quickly.

Verizon's Data Breach Investigations Report 2024 found that the software supply chain accounted for 15% of data breaches over the prior year, a 68% year-over-year increase.[10]

Potential Changes to CISA Under New Trump Administration

Positive Outcomes

If the new Trump administration rolls back CISA regulations, organizations may benefit from reduced compliance burdens and greater operational flexibility. For many businesses, particularly small and medium-sized enterprises, loosening federal mandates could lower the costs associated with meeting stringent regulatory requirements, such as detailed reporting and specific security frameworks like the SBOM. This deregulated environment may foster innovation, allowing companies to adopt cybersecurity practices tailored to their unique needs rather than adhering to prescriptive government standards. In addition, organizations could have more freedom to allocate resources toward proactive security measures or business priorities without being constrained by federal oversight.

Negative Repercussions

Scaling back CISA's role could expose organizations to heightened cybersecurity risks, particularly as federal initiatives like real-time threat intelligence sharing and coordinated responses to supply chain attacks diminish. Without strong federal leadership, businesses may find themselves more vulnerable to evolving threats such as ransomware and software supply chain breaches, which require collective action to effectively mitigate. Smaller organizations that rely on CISA's guidance and support might struggle to address complex cyber risks independently, leading to potential vulnerabilities across critical sectors. Moreover, the lack of consistent federal standards could create fragmented cybersecurity practices, making it harder for organizations to collaborate effectively and ensure the safety of interconnected systems.

3. Multilayered Security Architecture

Organizations must prioritize the protection of sensitive content at rest, in use, and in motion. A multilayered security architecture ensures robust defenses by implementing several overlapping protective measures. This approach not only safeguards sensitive content but also enhances organizational resilience against sophisticated threats.

A defense-in-depth strategy is the cornerstone of a multilayered architecture. By deploying multiple, complementary security measures, such as encryption, network firewalls, antivirus, and antispam solutions, organizations can ensure that if one layer fails, others will prevent unauthorized access or data compromise. For example, encryption technologies protect sensitive data in transit and at rest, ensuring that unauthorized parties cannot access or decipher the information.

Data loss prevention (DLP) systems monitor and control data transfers to prevent leaks of sensitive content. DLP tools enforce policies to detect and block unauthorized sharing of classified files or email attachments, significantly reducing the risk of accidental or intentional data exposure. Similarly, content disarm and reconstruction (CDR) technologies remove potentially malicious code from files while preserving their usability, ensuring secure content sharing without compromising productivity.

Cloud security posture management (CSPM) and zero-trust architecture (ZTA) play critical roles in modern security frameworks. CSPM provides visibility into cloud environments, identifying misconfigurations and monitoring compliance with security policies. ZTA enforces continuous validation of user identities, devices, and applications before granting access, minimizing implicit trust and protecting sensitive communications from lateral attacks within the network.

The integration of security tools is also vital to eliminate gaps in defenses. Centralized platforms, such as security information and event management (SIEM) or extended detection and response (XDR) systems, streamline monitoring, threat detection, and incident response. These platforms provide a unified view of security events across email, file sharing, and managed file transfer (MFT) systems, enabling faster and more coordinated responses to threats.

Organizations with a zero-trust security approach can save more than $1 million during a data breach.[11]

4. Secure Content Collaboration

Dynamic collaboration with third parties has become a cornerstone of modern business operations, enabling organizations to accelerate workflows and foster innovation. However, these interactions inherently increase exposure to data breaches and compliance violations. The exchange of sensitive content with external stakeholders—such as contractors, vendors, and partners—demands more granular controls and robust governance mechanisms to mitigate risks effectively.

To address these challenges, organizations are turning to secure content collaboration platforms that integrate dynamic access management and advanced tracking capabilities. These platforms enforce granular user permissions, ensuring that only authorized individuals can access specific files, folders, or data sets. This level of control is critical for minimizing the likelihood of accidental or malicious data exposure during third-party exchanges.

Granular governance also extends to activity monitoring and audit logs. Real-time tracking of content access and sharing activities enables organizations to detect and respond to potential security incidents swiftly. Comprehensive audit logs ensure compliance with regulatory requirements and provide a defensible position in the event of a security breach or data misuse allegation.

Further, technologies such as DLP tools and end-to-end encryption (E2EE) enhance the security of third-party collaboration. DLP systems enforce security policies by monitoring and blocking unauthorized data transfers, while E2EE ensures that data remains encrypted throughout its life cycle—from creation to transmission and storage.

The increased reliance on third-party collaborations highlights the necessity for organizations to adopt a zero-trust approach to secure content collaboration. This model assumes no implicit trust, continuously verifying user identities and device integrity before granting access to sensitive content. Coupled with automated compliance checks and advanced risk analytics, zero-trust principles provide the foundation for safeguarding data in a dynamic, interconnected environment.

83% of organizations use content collaboration platforms to share files externally with clients, partners, and other third parties.[12]

Next-gen Digital Rights Management

Legacy digital rights management (DRM) systems often hinder productivity and collaboration with their restrictive features, such as static, view-only access, limited file format support, and deployment complexities. They frequently require heavy client software installations, introduce security vulnerabilities during file transfers, and create version control chaos. These limitations prevent seamless external collaboration and fail to provide comprehensive oversight of sensitive content.

Enter Kiteworks SafeEDIT, a next-generation DRM solution designed to revolutionize how organizations collaborate externally. By streaming an editable rendition of files instead of transferring them, Kiteworks SafeEDIT ensures that original files remain securely protected within the owner's environment. This innovative approach enables external users to edit and co-author documents in a native application-like experience, without compromising security or data custody. With robust DRM governance, including detailed audit logs, access revocation, and universal file format support, Kiteworks SafeEDIT delivers secure, productive, and flexible collaboration without trade-offs.

5. Consolidated Communications Security

Organizations today rely on a multitude of systems for sensitive content communications, including email, file sharing, SFTP, MFT, and web forms. While these tools serve critical purposes, managing disparate platforms creates significant challenges. The complexity of maintaining and securing multiple systems not only drives up costs but also heightens security and compliance risks. Organizations with higher numbers of communication tools experience a higher ratio of data breaches. For example, 32% of organizations with 10 or more data breaches have more than seven communication tools, and 42% of those with six communication tools experienced seven to nine data breaches. These numbers are dramatically higher than the average number of data breaches across all respondents: only 9% reported 10 data breaches.[13]

The lack of integration across these tools makes it difficult for organizations to enforce consistent security policies, leaving them vulnerable to data breaches and compliance violations. Each additional platform introduces potential gaps in security and adds to administrative overhead, such as managing separate licenses, performing multiple audits, and training employees on various systems.

Consolidation into a single, secure platform addresses these inefficiencies by streamlining operations and reducing redundancies. By eliminating the silos between communication tools, organizations can achieve better visibility and control over sensitive content. A unified audit log provides a comprehensive record of all communications, enabling more proactive threat detection and faster incident response while simplifying compliance reporting. This not only supports regulatory requirements but also strengthens overall security posture.

Consolidation also reduces the total cost of ownership by minimizing expenses related to software licensing, maintenance, and staff training. IT teams can allocate resources more effectively, focusing on strategic initiatives rather than troubleshooting disconnected systems.

Almost one-third of organizations with over seven sensitive content communications experienced more than 10 data breaches.[14]

38% of North American organizations indicate they use 6+ communication tools to send and share sensitive content.[15]

6. API Security and Automation of Secure Content Communications

APIs are critical for automating the secure sharing and transfer of sensitive data across systems, applications, and external parties. While they streamline operations and enhance efficiency, APIs also introduce risks, necessitating robust security and governance to safeguard sensitive information and ensure regulatory compliance.

Secure APIs facilitate seamless data sharing between platforms, such as file sharing services, ERP systems, and cloud-based applications. Enforcing stringent authentication, authorization, and encryption protocols is essential to prevent unauthorized access and data breaches. Incorporating defense-in-depth principles ensures sensitive content remains protected throughout its life cycle, both in transit and at rest.

By automating routine tasks like file transfers, user provisioning, and policy enforcement, APIs reduce manual errors, save time, and improve operational efficiency. Automated workflows consistently apply security controls, enabling organizations to scale their processes while maintaining compliance with regulations such as GDPR, HIPAA, and CCPA. At the same time, centralized API management enhances governance by providing real-time visibility into data flows and user activities through detailed audit logs. Granular access controls restrict sensitive data to authorized users and systems, further reducing the risk of exposure.

Advanced API security tools leverage real-time monitoring and machine learning to detect anomalies in traffic, mitigating potential threats before they escalate. Regular updates and automated vulnerability scanning ensure APIs remain resilient against evolving risks.

Flexible deployment models, including on-premises systems, private clouds, and hybrid environments, allow APIs to adapt to diverse operational requirements while aligning with privacy and compliance mandates. Scalable and secure API frameworks help organizations maintain performance without compromising sensitive content protections.

Nearly three-quarters of organizations reported at least three API-related data breaches over the past two years.[16]

7. Regulatory Compliance Evolution

The regulatory landscape in 2025 reflects significant advancements in compliance and cybersecurity, driven by developments in 2024. Key frameworks, such as the full implementation of Cybersecurity Maturity Model Certification (CMMC) 2.0, the enforcement of the EU AI Act, the U.S. White House Executive Order on AI (Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence), updated NSA security guidelines, and international standards, are transforming how organizations safeguard sensitive data, address third-party risks, and ensure compliance.

The full enforcement of CMMC 2.0 requires businesses within the Defense Industrial Base (DIB) to meet specific compliance benchmarks or risk disqualification from federal contracts. This enforcement, underpinned by CFR 32 and CFR 48, will extend beyond DIB contractors, influencing a broader range of businesses to adopt similar cybersecurity frameworks to remain competitive in the market. Organizations are urged to proactively conduct readiness assessments and implement robust cybersecurity controls to secure their operations and supply chains. In addition, with two-thirds of organizations exchanging sensitive content with 1,000-plus third parties, enhanced focus on third-party risk management requires businesses to ensure that their partners and vendors meet stringent cybersecurity standards.[17]

The enforcement of the EU AI Act in 2025 introduces strict regulatory requirements for AI systems. Organizations must now comply with risk-specific criteria, which include implementing transparent AI models, addressing bias proactively, and strengthening data governance practices. These measures aim to ensure ethical AI development and usage, prioritizing privacy, accountability, and fairness. Companies deploying AI-driven solutions must align with both U.S. and international AI regulations to avoid financial penalties and reputational harm, marking a pivotal shift in how AI technologies are governed globally.

The NSA's updated security guidelines, released in 2024, continue to shape cybersecurity strategies in 2025. Organizations are placing greater emphasis on automation and zero-trust ecosystems, leveraging predictive and adaptive defense mechanisms to counter increasingly sophisticated cyber threats. These measures align closely with the principles of CMMC 2.0 and reinforce the importance of proactive security measures to protect critical infrastructure and sensitive data.

International standards, such as ISO/IEC 27001, 27017, and 27108, are expected to see increased adoption as multinational enterprises seek to streamline compliance across jurisdictions. By aligning with these standards, organizations can ensure consistent security practices, enhance operational resilience, and navigate complex regulatory landscapes effectively.

The regulatory shifts of 2024 have paved the way for a more secure and compliance-driven environment in 2025. Organizations are encouraged to approach these changes as an opportunity to strengthen their cybersecurity postures, mitigate risks, and build trust with stakeholders. By prioritizing readiness and embracing proactive measures, businesses can not only meet evolving regulatory demands but also position themselves as leaders in a rapidly transforming digital landscape.

Why CMMC 2.0 Compliance Is Critical for Defense Contractors

In 2025, the full enforcement of CMMC 2.0 Level 2 will take center stage for defense contractors in the DIB. Under CFR 32 and CFR 48, contractors must implement rigorous cybersecurity practices to protect controlled unclassified information (CUI) and federal contract information (FCI). Noncompliance will result in disqualification from Department of Defense (DoD) contracts, placing immense pressure on contractors to meet certification requirements. As audits become more stringent, contractors will need to adopt robust controls like end-to-end encryption, access management, and detailed audit logging to secure sensitive data and maintain their eligibility for government contracts.

Kiteworks is poised to be a key enabler for organizations navigating these challenges. Its FedRAMP Moderate Authorized Private Content Network supports nearly 90% of CMMC 2.0 Level 2 requirements, providing contractors with a significant head start on compliance.[18] By unifying secure email, file sharing, managed file transfer, and other secure communication tools into a single platform, Kiteworks simplifies compliance and reduces audit complexity. In 2025, DIB contractors leveraging Kiteworks will benefit from enhanced operational efficiency, seamless audit preparation, and comprehensive protection for their sensitive content, positioning them for continued success in the evolving regulatory landscape.

8. Data Classification Strategies

The strategic importance of data classification has never been more pronounced. In an era where data is both an asset and a liability, classification provides the foundation for robust data governance, compliance, and operational efficiency. Effective data classification enables organizations to reduce risks, enhance data visibility, and unlock the potential of their information assets while safeguarding sensitive information against breaches and noncompliance penalties. Only 10% of organizations have tagged and classified all of their unstructured data, whereas 52% admit they have tagged and classified less than half of their unstructured data.[19]

Automated classification tools are becoming increasingly sophisticated, leveraging AI and machine learning to process vast data sets with precision. These tools can identify patterns, apply contextual tagging, and classify information with minimal human intervention. This reduces errors and ensures that sensitive information is correctly identified and protected. AI-driven classification also allows for real-time updates, helping organizations adapt to rapidly changing data environments and regulatory requirements.

Data discovery and mapping are essential for organizations to gain a comprehensive understanding of their data landscape. Moving beyond merely identifying the locations of sensitive data, these processes now incorporate risk profiling and value analysis. With data spread across multi-cloud and hybrid infrastructures, advanced discovery tools provide real-time visibility into data flows and highlight vulnerabilities. This allows organizations to apply targeted safeguards, ensuring compliance and mitigating risks in complex environments.

Metadata management has evolved to provide dynamic, real-time insights into data attributes such as origin, ownership, and regulatory impact. This enriched context enables organizations to enforce stricter governance policies and streamline compliance processes. As regulations like GDPR, CCPA, and the EU AI Act continue to evolve, metadata-driven insights will play a pivotal role in ensuring organizations remain compliant with global standards.

Heightened regulatory scrutiny is another driver making data classification a critical focus area in 2025. As governments worldwide enact stricter data privacy laws, organizations face increasing pressure to implement proactive classification governance. Aligning with frameworks such as GDPR, the AI Act, and the CCPA, classification policies must now embed compliance requirements at their core. This ensures consistent handling of sensitive information across diverse business units and geographical regions, reducing the risk of fines and reputational damage.

The emphasis on data classification in 2025 extends beyond compliance and risk management. Organizations are recognizing its potential to enable better decision-making and operational efficiency. By categorizing and securing data appropriately, businesses can optimize access controls, streamline workflows, and foster innovation, particularly in data-driven initiatives. Moreover, robust classification frameworks empower organizations to confidently adopt advanced technologies, such as AI and machine learning, without compromising security or compliance.

NIST's Data Classification

The National Institute of Standards and Technology (NIST) underscores the importance of robust data classification as a cornerstone for effective data collection and management. Data classification involves organizing information into predefined categories based on its sensitivity, value, and compliance requirements. This structured approach not only enhances data integrity and accessibility but also aligns data collection practices with organizational security policies and regulatory mandates. By categorizing data according to its importance and risk level, organizations can ensure that sensitive data receives appropriate protections, mitigating risks such as unauthorized access, data breaches, and regulatory noncompliance.

Implementing NIST's data classification guidelines helps organizations optimize their data collection processes. Classification enables better decision-making by ensuring data is collected with clear purpose and context, avoiding redundant or irrelevant information. For instance, applying classification tiers—such as public, internal use, and restricted—allows organizations to tailor collection methods to the specific needs of each category, safeguarding sensitive information while streamlining data management. With a strong foundation in classification, organizations can improve data governance, enhance operational efficiency, and foster trust with stakeholders by demonstrating a commitment to data security and regulatory adherence.

9. Multidimensional Risk Assessment

Multidimensional risk assessment will emerge as a critical strategy for organizations navigating increasingly sophisticated cyber threats. Future models will expand their focus, leveraging AI-driven analytics and integrated threat intelligence to evaluate risks across dynamic parameters, such as real-time attack patterns, geopolitical shifts, user behavior, and data sensitivity. These advancements will enable security teams to prioritize vulnerabilities with unparalleled precision, allocating resources to areas of greatest risk and ensuring comprehensive threat mitigation. Algorithmic scoring of risk across industry segments, such as Kiteworks' Industry Risk Score Index, also provides organizations with useful benchmarks and the means to address potential risks proactively.[20]

Context-aware security is expected to evolve significantly, becoming a fundamental pillar of multidimensional risk assessment frameworks. Emerging systems will incorporate predictive AI to detect anomalies in user behavior, including access location, device usage, and timing, offering unprecedented insight into potential threats. The integration of predictive capabilities will empower organizations to preemptively address risks, shifting from reactive responses to proactive threat management. This innovation will not only reduce response times but also bolster defenses against increasingly targeted cyberattacks.

Continuous monitoring and adaptive defenses will become standard as organizations face rapidly evolving threat landscapes. In 2025, security platforms will dynamically adjust protocols in real time, driven by live global threat intelligence and behavioral data. This adaptability will ensure resilience against persistent and emerging threats, enabling organizations to maintain robust protection in an ever-changing environment.

Moreover, 2025 will see a heightened focus on integrating multidimensional assessments across compliance, cybersecurity, and operational risk domains. This unified approach will provide a holistic view of interconnected risks, allowing organizations to design agile security strategies that adapt to shifting regulatory and threat landscapes. The year will mark a turning point, where multidimensional risk assessments are not just tools but essential frameworks for navigating the complexities of modern cybersecurity.

Healthcare: Elevated Regulatory Risks and Ransomware Resilience

The healthcare sector demands urgent attention in 2025 due to its unique combination of high-value targets, critical operations, and regulatory oversight. As the primary custodian of sensitive patient information, healthcare organizations face significant risks from ransomware, with attack rates and breach costs continuing to rise. In 2024, the average healthcare data breach cost surpassed $6 million, and ransomware attacks frequently disrupted patient care.[21] These incidents demonstrate how attackers exploit both the sensitive nature of protected health information (PHI) and healthcare's reliance on legacy systems.

Increased regulatory scrutiny compounds these challenges. Enhanced HIPAA provisions and international frameworks such as GDPR will intensify compliance requirements, especially for organizations unable to adequately track and secure sensitive data exchanges. Reports show a direct link between unmanaged communications and breach severity, with organizations using 10 or more communication tools experiencing 3.5 times more data breaches.[22]

Healthcare is uniquely vulnerable due to its critical role in society. A breach not only risks patient trust and compliance penalties but also endangers lives when operations are disrupted. To mitigate these risks, IT and compliance leaders must prioritize zero-trust architectures, advanced threat detection, and robust data governance to align with the increasingly complex regulatory landscape.

10. AI Data Security Risks

AI data security risks will escalate in 2025, with malicious actors leveraging AI to orchestrate more complex and large-scale cyberattacks. Threat actors will use AI to automate vulnerability scanning, generate deceptive content for phishing campaigns, and evolve malware in real time to bypass traditional defenses. These developments will place AI systems themselves at the center of the cybersecurity battlefield, making them prime targets for attacks aimed at corrupting training data, hijacking models, or disrupting operations. Organizations will need to adopt proactive measures, including fortified security protocols and AI-specific threat detection tools, to counteract these sophisticated threats. In a recent study, 90% of organizations indicated they are actively implementing or planning to explore LLM use cases; however, only 5% are highly confident in their AI security preparedness.[23]

Organizations ingesting sensitive data into AI systems will also face heightened scrutiny over privacy and compliance risks. In 2025, stricter global regulations will demand greater accountability for how AI models process and protect sensitive information. Improper handling of proprietary data or personal information could lead to severe penalties as regulators impose stricter standards for transparency, ethical AI use, and data minimization. Privacy-preserving technologies, such as federated learning and differential privacy, will become essential for organizations seeking to balance innovation with compliance, ensuring that AI systems can learn from data without exposing sensitive details.

The rise of adversarial attacks will further challenge AI security frameworks. Attackers will increasingly exploit vulnerabilities in AI systems by manipulating input data to influence model outputs, introducing biases, or causing outright failure. To mitigate these risks, 2025 will see a surge in the adoption of adversarial testing, secure model development practices, and automated auditing tools. These advancements will be critical in ensuring AI models are robust and trustworthy under real-world conditions.

As AI technology becomes further entrenched in business processes, organizations in 2025 will be tasked with building comprehensive AI governance frameworks. These frameworks will address the dual challenge of defending against AI-enabled cyber threats while ensuring regulatory compliance and ethical data usage. With evolving threats and stricter oversight, organizations will need to prioritize continuous monitoring, real-time threat mitigation, and transparency in AI operations to maintain trust and security in the rapidly advancing AI landscape.

96% of organizations indicate they are using GenAI applications and that over one-third of sensitive data being ingested is regulated data.[24]

Manufacturing: Protecting Supply Chains Amid Digital Transformation

Manufacturing stands out as a sector requiring heightened focus in 2025 due to its rapid digital transformation and critical role in global supply chains. The adoption of Industry 4.0 technologies has exponentially increased the attack surface, making manufacturing one of the fastest-rising sectors in terms of cybersecurity risks. In 2024, the industry's Risk Score surged to 8.6, highlighting the significant exposure to threats.[25]

Unlike other sectors, manufacturing operates at the intersection of IT and operational technology (OT) environments. This hybrid setup is a prime target for attackers seeking to disrupt production or steal intellectual property. In addition, the reliance on third-party vendors amplifies vulnerabilities, with supply chain breaches having the potential to impact multiple organizations downstream.

Regulatory changes further heighten the importance of securing this sector. As governments expand frameworks like CMMC 2.0 to include non-defense contractors, manufacturers will need to align their operations with stricter data security and compliance mandates. Failure to do so could lead to hefty fines, reputational damage, and loss of contracts.

Manufacturing's pivotal role in the global economy and its interdependence with other sectors make it a strategic target for adversaries. Leaders must enhance endpoint security, enforce IT/OT network segmentation, and invest in predictive analytics to protect operations and ensure compliance with emerging regulations. Without proactive measures, manufacturers risk production disruptions and regulatory backlash, jeopardizing their market competitiveness.

11. Compliance-driven Security

Compliance-driven security will become increasingly dynamic as organizations face expanding regulatory mandates and heightened enforcement. The shift will be driven by evolving global standards requiring greater transparency, accountability, and demonstrable adherence to data protection laws. Organizations will prioritize embedding compliance at the core of their security strategies to avoid penalties and protect stakeholder trust. Compliance-driven security will move beyond simply meeting standards to actively shaping how organizations manage and secure sensitive data in a more complex regulatory environment.

The year will see significant advancements in automated compliance technologies. AI-powered tools are expected to enable real-time monitoring, flagging potential violations as they occur, and automating remediation processes to close gaps swiftly. These systems will integrate seamlessly with security frameworks to align compliance efforts with broader risk management goals. Dynamic compliance reporting will also gain traction, giving organizations actionable insights and ensuring they stay ahead of regulatory updates. The combination of automation and predictive compliance tools will empower organizations to proactively adapt to emerging requirements.

Risk management frameworks like the NIST RMF will evolve to address the need for agility in compliance-driven security. Organizations will increasingly adopt customizable frameworks tailored to specific industries and geographies, balancing security requirements with local and international compliance standards. These frameworks will also incorporate real-time threat intelligence, enabling a unified approach to mitigating risks while maintaining regulatory alignment.

As compliance becomes a more strategic driver of security, organizations will invest heavily in integrating compliance-driven practices into their broader cybersecurity programs. This approach will enable businesses to anticipate regulatory shifts, build resilience against emerging risks, and reinforce their commitment to safeguarding data and maintaining trust in an increasingly complex regulatory landscape.

Data Privacy Frameworks for Managing Cybersecurity

The increasing complexity of global privacy laws underscores the critical importance of robust data security, privacy, and compliance strategies for enterprises. To navigate this landscape, 78% of surveyed organizations rely on frameworks or regulations such as GDPR, the NIST Privacy Framework, ISO/IEC 27002, and COBIT to manage privacy effectively. Regional preferences further shape these practices; GDPR is widely used by 78% of European respondents, while 61% in North America rely on the NIST Privacy Framework.[26] Collaboration between technical privacy professionals and legal teams is essential for ensuring compliance, but inconsistent engagement can expose enterprises to enforcement actions and operational risks, emphasizing the need for regular cross-functional meetings to align on privacy controls and compliance objectives.

Beyond meeting legal requirements, many adopt proactive controls like identity and access management (74%), encryption (73%), and data security measures (72%), demonstrating a commitment to building resilient privacy frameworks.[27] Confidence in achieving compliance remains mixed, with 43% of respondents expressing strong confidence, but 13% reporting low confidence in their teams' ability to address evolving regulations. The rise in data subject requests, reported by 31% of organizations, further underscores the need for integrated privacy and compliance strategies. Ensuring proper handling of these requests and maintaining robust back-end systems is crucial for addressing regulatory demands while preserving trust in data security and privacy practices.

12. Quantum Computing Increases Risk Over Time

The advent of quantum computing poses a paradigm shift for data security, challenging the foundations of current cryptographic protocols. While quantum computers promise breakthroughs in fields such as materials science and machine learning, they also threaten to break widely used encryption methods like RSA and ECC, which underpin global data security and compliance frameworks. Organizations need to begin preparing for the "quantum threat" by adopting post-quantum cryptography (PQC) standards currently being developed by NIST. Ensuring compliance with emerging quantum-safe standards will become a vital part of future-proofing data security strategies.

Incorporating quantum-resistant algorithms into enterprise security architectures requires a coordinated effort across IT, compliance, and risk management teams. Transitioning to these algorithms will involve assessing cryptographic dependencies in existing systems, upgrading protocols, and collaborating with vendors to ensure compatibility. Simultaneously, organizations must ensure regulatory adherence as new laws and standards related to quantum security, such as GDPR and the AI Act, evolve to account for quantum-resilient data protection.

Beyond technical readiness, businesses will also face compliance challenges associated with cross-border data transfers and data sovereignty in a post-quantum world. As encryption keys are rendered obsolete by quantum decryption capabilities, the integrity of sensitive communications and regulatory frameworks governing data privacy will face unprecedented challenges. Global collaboration between governments, regulatory bodies, and industry leaders will be critical to establishing cohesive policies that address quantum threats without stifling innovation.

The integration of quantum-resilient strategies into compliance frameworks will be an ongoing process, with early adopters likely gaining a competitive advantage. Organizations that proactively adopt post-quantum standards and implement hybrid cryptographic solutions will not only mitigate long-term risks but also enhance trust among stakeholders. By prioritizing quantum readiness today, businesses can safeguard their sensitive data while ensuring compliance with the next generation of data security standards.

Quantum Computing and Malicious Actors

Quantum computing is emerging as a game-changing technology, capable of solving complex problems exponentially faster than classical computers.
While it holds promise for advancements in fields like healthcare and logistics, malicious actors are leveraging its potential to plan future cyberattacks, particularly targeting encrypted data.
By stockpiling encrypted information today, these actors aim to decrypt it once quantum computers become sufficiently advanced, rendering current encryption methods like RSA and ECC obsolete. This approach, known as "harvest now, decrypt later," poses a significant threat to sensitive information, including trade secrets, classified intelligence, and personal data.

To counteract this looming risk, organizations and governments must act swiftly to adopt quantum-resistant cryptographic algorithms, as outlined by NIST. However, the race to achieve quantum supremacy has created a cybersecurity arms race, with malicious actors and rogue states investing heavily in quantum research. Their goal is to exploit the technology for cyber espionage and breaches before defenses are widely implemented. This underscores the urgency for global collaboration in developing post-quantum security standards, strengthening data governance practices, and staying ahead of adversaries planning to weaponize quantum computing capabilities.

Takeaways and Recommendations

1. **Focus on Strategic Cybersecurity Investments:** Organizations must align their cybersecurity budgets with long-term strategic goals, prioritizing investments in scalable technologies such as predictive threat intelligence systems, real-time compliance monitoring, and zero-trust architectures to future-proof their defenses.
2. **Build Resilience to Policy Shifts:** Anticipate regulatory changes and potential rollbacks in government cybersecurity initiatives, such as shifts in the U.S. Cybersecurity and Infrastructure Security Agency (CISA). Develop adaptive internal policies and foster private-sector collaboration to mitigate risks from a less coordinated regulatory environment.
3. **Prepare for Cross-border Data Privacy Challenges:** Strengthen governance frameworks to address the evolving complexity of international data privacy laws, particularly in regions with fragmented regulations. This includes proactive adaptation to stricter enforcement actions, such as GDPR fines and new frameworks like the EU-U.S. Data Privacy Framework.
4. **Adopt a Unified Risk Management Approach:** Integrate cybersecurity, compliance, and operational risks into a unified framework. This approach will ensure a holistic view of threats, enabling organizations to align mitigation efforts more effectively and reduce gaps between departments.
5. **Innovate in Third-party Risk Management:** Establish more robust oversight of third-party vendors by leveraging AI tools for automated risk assessments and real-time monitoring of third-party security practices. Ensure that your organization can respond quickly to supplier-related vulnerabilities.
6. **Enhance Employee-centric Security Practices:** While technology investments are critical, prioritize human-centric approaches like continuous security training, gamified phishing simulations, and clear accountability structures to mitigate insider threats.
7. **Prioritize Data Discovery and Classification:** Develop a comprehensive strategy for real-time data discovery and classification across all systems, including hybrid and multi-cloud environments. This will help organizations identify sensitive data, enforce access controls, and improve compliance with regulatory standards.
8. **Harness AI Responsibly for Cybersecurity:** Use AI to bolster security operations, such as real-time threat detection and adaptive risk assessments. However, ensure that AI tools are governed by robust policies to prevent unintended risks, such as adversarial attacks or bias in decision-making. Use AI anomaly detection to identify potential anomalous activity such as spikes in access, edits, sends, and shares of sensitive content.

Conclusion

As organizations navigate the complexities of 2025, a proactive and integrated approach to cybersecurity is paramount. This report underscores the need for multilayered security architectures, robust compliance integration, and advanced threat management powered by AI. Emphasizing secure content collaboration, API security, and automated compliance monitoring will enable organizations to address regulatory demands effectively while maintaining operational agility and resilience.

Looking ahead, cybersecurity will continue to evolve alongside technological advancements and regulatory shifts. By investing in adaptive security solutions and fostering a culture of continuous improvement, organizations can safeguard sensitive data, enhance trust, and drive innovation. Kiteworks encourages adopting the strategic recommendations in this report to build a resilient, future-ready defense framework, ensuring success in the dynamic cybersecurity landscape of 2025 and beyond.

References

[1] "Gartner Forecasts Global Security and Risk Management Spending to Grow 14% in 2024," Gartner, September 28, 2023.

[2] "Top 11 Data Breaches: Actionable Insights and Recommendations Using Kiteworks Risk Exposure Index," Kiteworks, October 2024.

[3] "Gartner Forecasts Global Security and Risk Management Spending to Grow 14% in 2024," Gartner, September 28, 2023.

[4] Morgan Sullivan, "Navigating the Expanding Patchwork of U.S. State Privacy Laws: What's Coming in 2025," Transcend, November 7, 2024.

[5] Heather Domin, "AI governance trends: How regulation, collaboration and skills demand are shaping the industry," World Economic Forum, September 5, 2024.

[6] "20 biggest GDPR fines so far [2024]," Data Privacy Manager, September 9, 2024.

[7] Steve Morgan, "Software Supply Chain Attacks To Cost the World $60 Billion by 2025," Cybercrime Magazine, October 3, 2023.

[8] Maggie Miller, "Rand Paul has plans to kneecap the nation's cyber agency," Politico, November 14, 2024.

[9] Catherine Stupp and James Rundle, "Trump's Second Term Is Expected to Bring Big Change to Top U.S. Cyber Agency," Wall Street Journal, November 13, 2024.

[10] "2024 Data Breach Investigations Report," Verizon, May 2024.

[11] Jennifer Gregory, "Companies without zero trust could lose $1M more during a data breach," Security Intelligence, September 21, 2022.

[12] "2 Ways to Tell If Your Communication to a Website Is Secure," UW-Madison Information Technology, February 10, 2022.

[13] "Sensitive Content Communications Privacy and Compliance Report 2024," Kiteworks, June 2024.

[14] Ibid.

[15] Ibid.

[16] "2023 State of API Security: A Global Study on the Reality of API Risk," Traceable and Ponemon Institute, September 6, 2023.

[17] "Sensitive Content Communications Privacy and Compliance Report 2024," Kiteworks, June 2024.

[18] "CMMC 2.0 Compliance Mapping for Sensitive Content Communications," Kiteworks, October 2024.

[19] "Sensitive Content Communications Privacy and Compliance Report 2024," Kiteworks, June 2024.

[20] "2024 Industry Risk Score Report: Insights and Analysis of Risk Scores Across Industries—2018 to 1H 2024," Kiteworks, October 2024.

[21] "Cost of a Data Breach Report 2024," IBM, July 2024.

[22] "Sensitive Content Communications Privacy and Compliance Report 2024," Kiteworks, June 2024.

[23] Haziqa Sajid, "AI Security Trends 2025: Market Overview & Statistics," Lakera, September 2, 2024.

[24] James Coker, "Sensitive Data Sharing Risks Heightened as GenAI Surges," InfoSecurity Magazine, July 17, 2024.

[25] "2024 Industry Risk Score Report: Insights and Analysis of Risk Scores Across Industries—2018 to 1H 2024," Kiteworks, October 2024.

[26] "Privacy in Practice 2024," ISACA, January 18, 2024.

[27] Ibid.

This report presents findings and insights developed with the assistance of AI technologies. While AI played a key role in generating the content, the methods used are experimental and may include inaccuracies or biases, making independent verification essential for critical decisions. The findings are not professional advice and should not be relied upon solely. Despite human review, errors or limitations in AI-driven processes remain, and the technologies used are subject to ongoing development. We disclaim liability for any consequences arising from the use of this information.