

The State of Data Risk Management Report



Data Security

Governance



Table of Contents

EXECUTIVE SUMMARY	3
SURVEY METHODOLOGY	3
CURRENT LANDSCAPE OF DATA SECURITY AND GOVERNANCE	4
RISK MANAGEMENT CHALLENGES	5
IMPACT OF INDUSTRY ON DATA RISK MANAGEMENT	6
BREACH DATA ACROSS INDUSTRIES	7
DATA SECURITY CHALLENGES: COMPLIANCE, RISK MANAGEMENT, AND THREAT CONCERNS	9
DATA GOVERNANCE: INVESTIGATING THE ADOPTION OF TOOLS AND DATA PROTECTION	10
MANUAL PROCESSES VS. AUTOMATED APPROACHES	11
ADDRESSING THE GAPS IN ORGANIZATIONAL DATA SECURITY: THE NEED FOR STRATEGIC	12
SUMMARY OF DATA AND ANALYSIS	13
CONCLUSION	14

Executive Summary

Despite tightened standards from regulatory bodies like the FTC, HIPAA, and the SEC, many organizations overestimate their security measures. The “State of Data Risk Management” research is an effort to examine the gap between perceived data security confidence and actual effectiveness, set amid rising data breaches.

The findings of the research are stark, and they highlight the urgent need for organizations to adopt integrated and automated data security strategies. This gap is particularly evident in sectors like financial services and healthcare, where high confidence in existing data security posture is belied by the frequency of breaches.

The survey underscores that high confidence in data security does not correlate with lower breach rates. It is clear that many organizations are underestimating their vulnerabilities, relying on outdated, manual processes, and proving to be slow to adopt automated systems. Modern, proactive approaches—including regular audits, strategic use of technology, and external consulting—are essential.

Even in sectors where adoption of advanced capabilities has been strong—sectors like technology, finance, and healthcare—organizations still face significant threats. This discrepancy highlights the need for continuous improvement and vigilance. Organizations must foster a culture of transparency, collaboration, and ongoing enhancement to better align their security posture with reality and strengthen resilience against cyber threats.

This report highlights the importance of adopting integrated and automated data security strategies to navigate the complex and evolving landscape of data risk effectively.

SURVEY METHODOLOGY

Over 300 survey respondents from various sectors—including education, professional services, information technology, government, health and life sciences, and financial services—completed the survey. The participants’ job roles ranged from Infrastructure, Compliance, Security, and Operations to Development, Governance, Data and Analytics, and included the C-suite as well.

The respondents’ varied job functions added depth to the analysis, offering a multifaceted view of data security and governance challenges. This diversity ensures the findings reflect a broad spectrum of perspectives and experiences, enriching the report’s conclusions and recommendations.

CURRENT LANDSCAPE OF DATA SECURITY AND GOVERNANCE

Data security and governance efficacy can be viewed across a spectrum, from “Not Effective” to “Effective,” and these labels can be applied to both perception and reality. The State of Data Risk Management research discovered that larger organizations—particularly those in industries such as financial services and health and life sciences—tend to rate their data security and governance practices more positively. In contrast, sectors such as education and smaller organizations report more challenges, often resulting in lower ratings.

However, as we dig deeper, we discover that organizations across various industries exhibit diverse practices and performance levels. This discrepancy prompts a critical examination of the underlying factors and the actual effectiveness of these data security measures.

Analysis

Examination of How Data Risk Perceptions and Preparedness Vary Across Different Industries

To further understand the dynamics, there is value in moving beyond surface-level insights to correlation analysis. This scrutinizes how data risk perceptions and actual preparedness against breaches fluctuate across different industries. This analysis, juxtaposing survey responses with actual breach incidents from recent reports, uncovers the nuances of data security ratings and organizations’ tangible preparedness for cybersecurity threats.

In juxtaposing the data in this manner, we are able to evaluate the correlation—or lack of correlation—between perceived and actual security postures. It then becomes possible to explore the intricacies and shortcomings of data security ratings, and provide a comprehensive view of the prevailing data security challenges and the efficacy of governance strategies in the face of evolving cyber threats.

Data Security Ratings

Industries such as information technology, healthcare, financial services, and government give themselves relatively high “Effective” ratings in data security, suggesting a strong emphasis on—and confidence in—data security within these sectors.

However, despite the high confidence levels reported in the survey, the [2024 Verizon Data Breach Report](#) tells a somewhat different story.



RISK MANAGEMENT CHALLENGES

The research sheds light on the perceived effectiveness of data security strategies:

 **Effective Data Security Strategies**
63% of responses

Most organizations view their data security strategy as “effective,” with 44% considering it “somewhat effective” and 19% rating it as “very effective.” This indicates a general confidence in the ability of organizations to mitigate security risks, though there is still room for improvement.

 **Uncertainty**
30% of responses

Many respondents need clarification about the effectiveness of their security measures, which could signal inconsistencies in risk assessment and mitigation.

 **Not Effective**
7% of responses

A small group acknowledges their strategies’ ineffectiveness, pointing to serious security vulnerabilities.

IMPACT OF INDUSTRY ON DATA RISK MANAGEMENT

Data security strategy effectiveness by industry:

Industry	 Effective	 Uncertain	 Not Effective
Information Technology	70.75%	24.52%	4.73%
Government (Local, State, or Federal)	53.34%	30.00%	16.66%
Financial Services	72.91%	20.83%	6.26%
Health & Life Sciences	63.15%	36.85%	Not specified

Observations

- Technology and financial services industries show confidence in their data security strategies, with the majority considering them effective.
- Government and healthcare have the least confidence in the effectiveness of their data security strategies, as indicated by the low percentage of responses that consider them effective. However, healthcare is the only industry where no respondent listed their data security strategy as “not effective.”

These insights suggest that while sectors like financial services feel more assured about their risk management strategies, others, particularly public sector bodies, face more challenges and exhibit less confidence in their data security measures. This data indicates a disparity in perceived security effectiveness within organizations where security teams are overconfident about their company’s security posture. In contrast, other departments outside of security lack similar confidence.

BREACH DATA ACROSS INDUSTRIES

Industry	Perceived Security Rating	Actual Breach Data		
		Verizon Data Report	Top Patterns	Threat Actors
Financial Services	72.91% High confidence, with 72.91% considering their data security strategy effective.	477 incidents	77% of breaches were: Basic Web Application Attacks, Miscellaneous Errors, and System Intrusions	66% External 34% Internal
Technology	70.75% High confidence, with 70.75% considering their data security strategy effective.	380 incidents	77% of breaches were: System Intrusion, Basic Web Application Attacks, and Social Engineering	80% External 20% Internal
Healthcare	63.15% Moderate confidence, with 63.15% considering their data security strategy effective.	433 incidents	68% of breaches were: System Intrusion, Basic Web Application Attacks, and Miscellaneous Errors	65% External 35% Internal
Government	53.34% Low confidence, with 53.34% considering their data security strategy effective.	582 incidents	76% of breaches were: System Intrusion, Lost and Stolen Assets, and Social Engineering	85% External 30% Internal

By implementing the actionable insights provided, organizations can better align their perceived security posture with reality, ultimately enhancing their resilience against cyber threats.

Observations

- **Financial Services:** The significant number of breaches contradicts high confidence in their security strategy, suggesting overconfidence in their security posture.
- **Healthcare:** While there is moderate confidence in their security measures, the high number of breaches indicates that regulatory compliance alone is insufficient to ensure security.
- **Technology:** Despite high confidence in their security strategies, frequent breaches highlight the need for continuous improvement and adaptation to evolving threats.
- **Government:** Lower confidence in security effectiveness aligns with the high number of breaches, indicating a need for substantial enhancements in security practices.

Key Findings

- **Financial Services Discrepancy:** Despite high confidence in security measures, the sector remains a prime target for cyberattacks due to valuable data, indicating a gap between perceived effectiveness and actual vulnerability.
- **Healthcare Discrepancy:** High regulatory requirements do not eliminate vulnerabilities, with significant breaches still occurring, highlighting areas for improvement in security measures.
- **Technology Discrepancy:** Despite advanced security capabilities, frequent incidents indicate the need for continued vigilance and improvement.
- **Government Discrepancy:** Despite moderate to high confidence ratings, there are many breaches, emphasizing the need for enhanced security measures and ongoing improvements.

The discrepancies between perceived data security confidence and actual breach data across various industries highlight the need for continuous improvement and proactive measures. By implementing the actionable insights provided, organizations can better align their perceived security posture with reality, ultimately enhancing their resilience against cyber threats.

This combined section compares breach data with the perceived effectiveness of data security strategies, highlighting discrepancies and providing insights and recommendations for improvement.

DATA SECURITY CHALLENGES: COMPLIANCE, RISK MANAGEMENT, AND THREAT CONCERNS

Data security challenges include compliance, risk management, and specific threats. Effective risk management helps organizations navigate complexities and enhance security against threats such as those listed below.

Threat Concerns

The survey indicates that the respondents chose these threats as the primary concerns facing their organizations.



Data Breaches (26.45%) are a significant concern, highlighting the fear of unauthorized access to or theft of corporate data.



Ransomware (23.04%) is nearly as prevalent, indicating the increasing worry about malicious software attacks that encrypt data and demand ransom.



Insider Threats (21.16%) underscore the need for robust internal security measures and monitoring to prevent internal risks.



Misconfigurations (19.80%) Concerns about misconfigurations reveal the importance of proper system setup to prevent security vulnerabilities.

Compliance Challenges

An impressive 72% of organizations are addressing compliance challenges by leveraging various methods such as regular audits, in-house legal teams, compliance software, and external consultants. This proactive approach is crucial for adhering to regulations like HIPAA, PCI DSS, GDPR, and CCPA:



Regular Audits (31% of responses): Many organizations rely on regular audits to ensure compliance, emphasizing the need for ongoing monitoring.



In-House Legal Team (23% of responses): This reflects the complexity of navigating data protection laws, requiring specialized legal expertise.



Compliance Software (12% of responses) and External Consultants (6% of responses): Organizations use these methods to support their compliance efforts.



Uncertain (28% of responses): Some respondents needed clarification about their compliance mechanisms, suggesting a potential gap in effective compliance strategy implementation.

DATA GOVERNANCE: INVESTIGATING THE ADOPTION OF TOOLS AND DATA PROTECTION

Adopting data governance tools and strategies is critical in strengthening organizational defenses against cyber incidents. This analysis reveals how integrating various data governance practices, including data hosting, storage types, monitoring, classification, tagging, and implementation of security principles, correlates with an organization's preparedness against data breaches.

Data Cataloging Tools

Approximately 27% of organizations have implemented data cataloging tools reflecting proactive data management and security measures, while 22% contemplate their adoption, demonstrating a recognition of these tools' significance in data governance. However, 21% still need to embrace these tools, and 30% still need clarification, suggesting a potential gap in data governance frameworks.

Data Hosting and Storage

- **40% of organizations use a hybrid approach for data hosting**, while 30% rely on multi-cloud environments, indicating a preference for diverse and flexible data storage solutions.
- **About 50% of data stores are cloud data platforms**, signifying a substantial adoption of cloud services for data management.

Monitoring and Access Control

- **28% of organizations employ automated monitoring tools to oversee data-in-use**, with 25% conducting regular audits, highlighting the importance of continuous monitoring in data governance.
- **60% of respondents have implemented a role-based access control system**, suggesting a widespread acknowledgment of the need for structured access management.

Data Usage Tracking and Classification

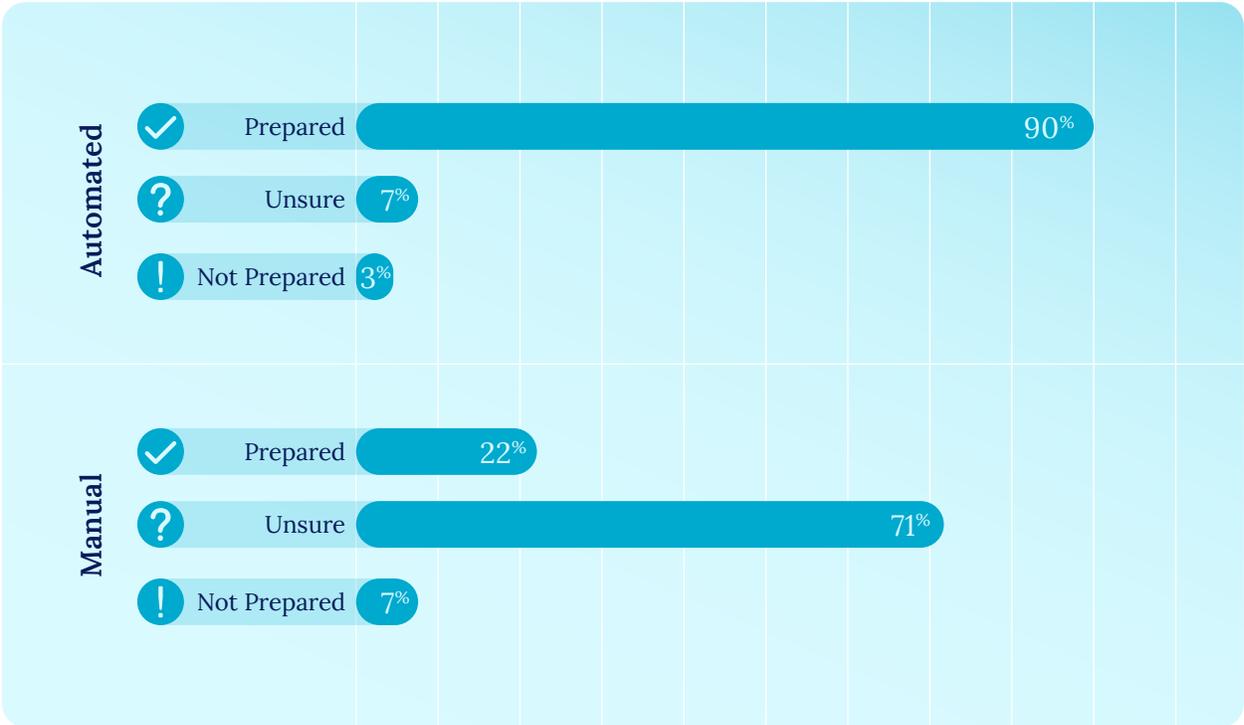
- **30% of organizations use either automated tools or a combination of manual and automated methods** for tracking data usage to identify suspicious activities, emphasizing the adoption of proactive security measures.
- **38% of organizations utilize manual and automated processes to classify sensitive data**, demonstrating the complexity and significance of accurate data categorization in enhancing security.

Data Tagging and Security Principles

- Regarding implementing the principle of least privilege (PoLP), **58% describe their approach as effective**. While most find their efforts successful, there are still considerable challenges in enforcing minimal access rights to secure sensitive data.

MANUAL PROCESSES VS. AUTOMATED APPROACHES

When classifying sensitive data, monitoring data-in-use, and tracking data usage, the following levels of preparedness are vital in preventing data breaches.



Correlation with Data Protection Effectiveness

While manual processes remain prevalent, implementing automated technology-driven solutions can significantly bolster an organization’s defenses against cyber threats, thus improving preparedness and resilience in the face of potential data breaches.

The analysis reveals a clear correlation: Adopting data governance tools and strategies, particularly those that automate and streamline processes, is crucial in building a more secure and prepared organizational environment against cyber incidents.

ADDRESSING THE GAPS IN ORGANIZATIONAL DATA SECURITY: THE NEED FOR STRATEGIC ALIGNMENT AND AUTOMATION

Examining organizations' data security posture reveals significant challenges due to manual, homegrown, and often undefined processes. This situation is exacerbated by a lack of awareness and understanding among executives and other departments about key security processes within their organizations.

Securing On-Premises Data Stores

Third-Party Solutions: 34.01% of respondents rely on third-party solutions, indicating a trend toward externalizing data security responsibility.

- **Uncertainty:** 29.29% of respondents are unclear about their on-premises data security measures, highlighting a critical gap in organizational knowledge and strategic oversight.
- **Manual Processes:** 7.74% of respondents still use manual processes, while 6.40% have no specific process, signaling a pressing need for streamlined and automated security strategies.

Shadow Data Sprawl Management

- **Uncertainty and Neglect:** 37.58% of respondents are unsure of their management approach, and 11.74% do not use tools, indicating prevalent uncertainty and potential neglect in addressing shadow data risks.
- **Manual Monitoring:** 12.42% of respondents rely on manual monitoring, reflecting outdated and inefficient methods exacerbating the challenge of managing dispersed and unstructured data.

Cloud and On-Premises Security Management

- **Divided Landscape:** 38.05% of respondents use separate solutions for cloud and on-premises environments, and 28.96% are unsure of their strategy. This division reflects siloed security practices, leading to disjointed and potentially ineffective security measures.
- **Need for Integration:** The lack of integrated approaches suggests the need for holistic solutions that provide seamless security across all environments.

Misconfigured Data Stores Management

- **Uncertainty:** 40.40% of respondents are unclear about using tools to manage misconfigurations, revealing a substantial gap in proactive risk management.
- **Manual and Toolless Approaches:** 16.84% of respondents do not use any tools, and 16.16% manage manually, indicating a reliance on reactive or labor-intensive strategies that may not adequately address modern data complexities.

Database Security Across Types

Lack of Clear Strategy: 35.02% of respondents are unclear about their strategy, and 11.11% have no specific process, highlighting the challenges in maintaining robust security across diverse database systems.

Manual Processes: 12.46% of respondents rely on manual processes, emphasizing the need for automated and cohesive security frameworks.

The overarching theme of this analysis points to a critical need for enhanced clarity, alignment, and automation in data security practices. Information silos and the lack of shared understanding within organizations can hinder the development of a coherent and effective security posture. To mitigate these risks, organizations must foster a culture of transparency, collaboration, and continuous improvement in data security. Ensuring that executives and all departments are aligned and informed about the security processes is essential for safeguarding their data assets.



Organizations must prioritize modern, proactive approaches, including regular audits, strategic use of technology, and external consulting, to effectively navigate the evolving landscape of data risk.

SUMMARY OF DATA AND ANALYSIS

The survey data indicates high confidence in data security doesn't correlate with lower breach rates.

For instance, the technology, financial, and healthcare sectors still encounter substantial threats despite their advanced security capabilities.

This discrepancy suggests a false sense of security and underscores the need for continuous improvement and vigilance. The financial services sector, although highly confident, remains a prime target due to the valuable nature of its data. Similarly, the healthcare sector's stringent regulatory requirements do not fully mitigate its vulnerabilities, highlighting areas for improvement.

The survey underscores the importance of adopting integrated and automated data security strategies to address these challenges. Reliance on outdated, manual processes and slow adoption of automated systems contribute to current vulnerabilities. Organizations must prioritize modern, proactive approaches, including regular audits, strategic use of technology, and external consulting, to effectively navigate the evolving landscape of data risk.

By fostering a culture of transparency, collaboration, and continuous improvement, businesses can better align their perceived security posture with reality, enhancing their resilience against cyber threats.

DETAILED ADVICE ON SECURING DATA POSTURES

To enhance their data security postures, organizations should consider the following detailed advice:

Implement Comprehensive Discovery and Classification

Use platforms like Netskope to discover and classify data across all environments automatically. This step ensures that all data, including shadow data, is identified and categorized according to sensitivity and regulatory requirements, facilitating better data management and protection.

Adopt a Holistic Data Governance Framework and Educate and Train Staff

Establish a governance framework that integrates data security, compliance, and management practices, including clear policies on data access, usage, and retention, ensuring that data is handled securely throughout its life cycle.

Invest in ongoing cybersecurity training for all employees to build awareness of potential threats and the importance of data security. A well-informed workforce can act as the first defense against cyber threats. Keep organizational stakeholders out of the dark about data security strategies.

Leverage Advanced Monitoring and Analysis Tools That Embrace a Zero Trust Security Model

Use data-in-use monitoring to track how data is accessed and used across the organization. This approach helps detect anomalies, prevent unauthorized access, and ensure compliance with privacy standards.

Assume that internal and external networks are potentially hostile, and implement strict access controls and verification processes. This model minimizes the attack surface and reduces the risk of data breaches.

Prioritize Risk Management and Compliance

Regularly assess and update security measures to address emerging threats and comply with evolving regulations. Regular risk assessments and audits are incorporated into the security strategy to identify vulnerabilities and ensure continuous improvement.

Conclusion

By integrating these practices, organizations can truly secure their data security postures, reducing the risk of breaches and ensuring compliance with regulatory standards. Adopting a proactive, informed, and comprehensive data security and governance approach is vital.

There's a significant gap between perceived security strength and the reality of breaches. What is your next step? Assess your current data risk management strategy, then [request a demo](#) with Netskope to see how it can close these gaps. Let's move beyond assumptions and build a data security approach that withstands today's threats.

Interested in learning more?

Request a demo

Netskope, a global SASE leader, helps organizations apply zero trust principles and AI/ML innovations to protect data and defend against cyber threats. Fast and easy to use, the Netskope One platform and its patented Zero Trust Engine provide optimized access and real-time security for people, devices, and data anywhere they go. Thousands of customers trust Netskope and its powerful NewEdge network to reduce risk and gain unrivaled visibility into any cloud, web, and private application activity—providing security and accelerating performance without compromise. Learn more at netskope.com.

©2025 Netskope, Inc. All rights reserved. Netskope, NewEdge, SkopeAI, and the stylized “N” logo are registered trademarks of Netskope, Inc. Netskope Active, Netskope Cloud XD, Netskope Discovery, Cloud Confidence Index, and SkopeSights are trademarks of Netskope, Inc. All other trademarks included are trademarks of their respective owners. 02/25 RR-814-2