privacera

EBOOK

2023 State of Data Security Governance

Why Unclear Ownership and Hybrid Data Estates Slow Progress

Companies today face immense competitive pressure to become more data driven.

Besides optimizing their data, they must ensure it remains secure and compliant with industry and governmental regulations.

Behind these challenges is the friction of under-resourced IT teams trying to balance governance and fine-grained access controls needed to secure their data and meet compliance requirements. These critical functions often go beyond what their current data platforms can deliver, putting these companies at significant risk for a data breach. How do they plan to address and solve these challenges?

That's what Privacera wanted to know. In January 2023, the company conducted an independent study to learn more about the current data management and data security governance landscape and how companies are keeping up with it. The survey went to 250 CIOs, CAOs, CDAOs, and CISOs in the US at companies across various industries and with annual revenues of at least $500 million.

The survey focused on understanding the following aspects of data security governance management:

- Current data security governance strategies, goals, and data processes
- Challenges related to data accessibility, compliance, and governance
- Outlook for effective data security governance solution adoption and investment

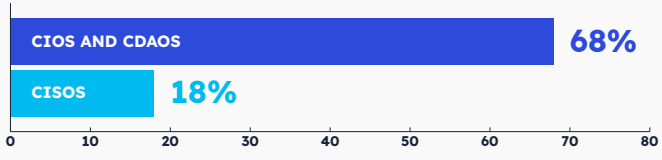
This report examines our findings and shows how companies are pivoting toward tighter security and compliance while achieving faster time to data insights to move ahead and remain competitive.

Current Landscape

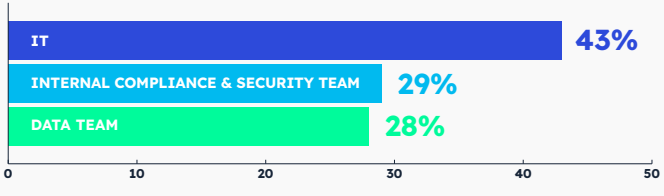
To understand the current data management landscape, the survey dug into who currently oversees data governance, the strategy these companies follow, and their data access practices.

Divided Approach

Data governance ownership is often a source of friction for organizations. Is that still the case today? In fact, yes. When asked about who's responsible for data governance, most respondents (68%) pointed to their CIOs and CDAOs. Only 18% place CISOs in charge of it.



Meanwhile, on the implementation side, 43% responded that IT should oversee implementation of the data security platform, compared to 29% who responded it should fall on the internal compliance and security team. The remaining 28% felt the data team should own implementation.



Technical and Business Goals

When asked about the key goals of their DSG strategy, most respondents pointed to data protection and security. Among the range of options, 82% prioritized protecting all data assets within the organization, with 60% assessing their risk level and implementing mitigation strategies for the organization.

Meanwhile, 58% focus their key goals on reducing time to insights/analytics, and 52% focus on creating scalable, automated workflows.

Top data security governance strategy goals

- **Protecting all data assets**
- **Assessing risk level and implementing mitigation strategies**
- **Reducing time to insights/analytics**
- **Scalable and automated workflows**

On the business side, the goals focused on increasing revenue or customer growth (73%) and improving customer experience (70%). Other goals included investing in R&D (54%) and brand development (50%), followed by expanding geographies or markets (39%) and expanding partnerships (41%).

Top business goals

- **Revenue or customer growth**
- **Customer experience**
- **R&D**
- **Brand development**

Data Access and Process

Most organizations (75%) reported storing their data assets in the cloud using singular or multiple cloud providers. The remaining 23% plan to keep some data assets on-premises for the foreseeable future.

However, 60% reported distributing their data across multiple heterogeneous locations and systems. Meanwhile, 40% distribute their data from and store it in one central place.

Organizations favor some level of automation for governance and compliance. Among respondents, **66% mix manual and automation processes,** but

only 23% use fully automated processes.

→ What the Numbers Mean

The current data management landscape reflects a divide regarding who should handle data security governance and who should implement it—the data team, the security team, or IT team. This divide carries through in the key goals for the data security governance strategy, with organizations prioritizing data protection, security, and business growth. Also, although most organizations store their data assets in the cloud, they distribute their data across multiple locations and systems using a combination of manual and automatic processes.

These results highlight the imbalance between who handles data security governance and who should implement it. This misalignment between teams creates friction in data democratization and creates blind spots in governance. The fact is, data security governance requires C-suite collaboration between the CIO, CDAO, and CISO that encourages data and security teams to work together.

Organizations often consider security a defensive and risk mitigation strategy, as indicated by the data security governance goals. However, the business goals, which prioritize growth, customer experience, and innovation, demonstrate an offensive strategy to stay ahead in the current business climate.

Challenges

Next, to gain insights into how the current landscape impacts organizations' ability to use their data effectively, we asked about their ability to access their data securely while staying compliant.

Data Asset Accessibility

Data-driven organizations require easy access to the data assets their users need. However, over half of organizations (53%) find their employees are spending too much time and effort trying to access their data to get valuable business insights. Of those organizations, 12% reported their employees find it fairly time-consuming to access their data.

Data access challenges at this level prevent organizations from becoming data driven.

For the 47% who responded that their data is easily accessible to derive business insights, an essential question remains: are they accessing relevant or accurate data in a timely manner?

Governance and Compliance

For the respondents who mix manual and automation processes, their challenge is achieving a consistent security posture across all data. Without it, they face an increased risk for a data breach. Regardless of the process they use, they agree on the main compliance and data governance challenges in today's global business environment.

The biggest concern is stable data quality (56%), followed by data discovery (52%) and defining consistent data access policies (53%). Other challenges in this area correspond to enforcing a scalable data policy (49%) and ensuring proper data masking (45%), followed by data residency regulations (25%).

Top 3 compliance and governance challenges:

- Stable data quality
- Defining consistent data access policies
- Discovery of the proper data assets

What the Numbers Mean

The current landscape of data management and data security has created two main challenges. First, employees are spending too much time and effort trying to access the data they need. And for those that can easily access their data to get insights, it's unclear whether they're accessing relevant or accurate data in a timely manner. If they can't, they're not getting optimal insights to make innovative and effective decisions.

And second, the mix of manual and automated processes presents big concerns surrounding stable data quality, data discovery, and data access policies. This situation creates an inconsistent security posture across their data, leaving them open to greater risk of a data breach.

2023 Outlook

Finally, the survey looked into how companies plan to adjust their current strategy to become more data driven in today's competitive business environment.

More Governance and Compliance Automation

As companies seek to enable broader and secure data access, the majority (74%) see an increasing need for a scalable data security governance strategy in their organization in the next 6-12 months. Among those who don't currently use a data security platform, 44% plan to implement a data security platform in the next 12–24 months.

The biggest business driver behind this shift is technology (69%) as organizations seek the benefits of technology assisted automation. Respondents placed near equal importance on the cause being strategy and operations (59%) and cost and profit margins (57%).

Top 3 drivers for scalable data security governance strategy

1. Technology
2. Strategy and operations
3. Cost and profit margins

As regulatory requirements change in the US and overseas, most companies (76%) are staying ahead by investing in processes and technologies that help with automating data governance and broader compliance initiatives. However, only 24% prefer to address each new regulation one at a time.

Budget Increases for Data Security Governance

To support the shift in their data governance strategy in 2023 and beyond, almost all companies (91%) plan to invest more in data security governance. Among them, 54% plan to make a substantial investment, 37% plan to invest somewhat, and only 7% will invest minimally.

These investments require sufficient budgets to support their new strategy. In fact, 92% of companies plan to increase their budget, with 42% increasing them 16%–30%.

→ What the Numbers Mean

To address their data management challenges, organizations are looking to improve and streamline theirleaning toward solving the current state of data security governance. They have identified a greater need for a scalable data security governance strategy. In support of this strategy, they plan to stay ahead of data demands and compliance requirements by investing in automating data governance and compliance, with budget increases specifically for data security governance.

What the Current State of Data Security Means for You

Data security governance is at the forefront of today's organizations, especially considering the inherent complexities of data management in the cloud. As a starting point toward a stronger data security strategy, establish clear ownership of data security and collaboration between your data, IT, and security teams.

In hybrid and multi-cloud environments, work with company stakeholders to align data, IT, and security teams to take a unified approach to data governance and compliance across these different environments. This approach reduces team friction and creates a consistent security and governance framework by simplifying and securing data access, security, and privacy for analytical workloads across your entire data and analytical ecosystem.

Orient your data security governance strategy toward revenue-positive business outcomes. This strategy will outperform one that focuses only on reducing risk by creating better defenses. With the emergence of broad-based data security platforms, you can substantially improve consistency and productivity through end-to-end data security automation.

Fortune 500 enterprises trust Privacera for their universal data security, access control, and governance. Discover how to streamline data security governance with Privacera.

Take a unified approach to data access, privacy, and security with Privacera.

REQUEST A DEMO CONTACT US

Privacera, based in Fremont, CA, was founded in 2016 by the creators of Apache Ranger™ and Apache Atlas. Built on the principle of delivering trusted data access to data consumers, the company provides data privacy, security, and governance on its SaaS-based data security and access governance platform. It serves numerous Fortune 500 clients in the finance, insurance, life sciences, retail, media, consumer industries, and government agencies and entities. Privacera has been recognized as a leader in the 2023 GigaOM Radar for Data Governance and has achieved AWS Data and Analytics Competency Status. The company was also named a 2022 CISO Choice Awards Finalist and received the 2022 Digital Innovator Award. Recently, it was named a “Sample Vendor” for data security platforms in the Gartner Hype Cycle for Data Security, 2022. Learn more about Privacera at privacera.com.

privacera