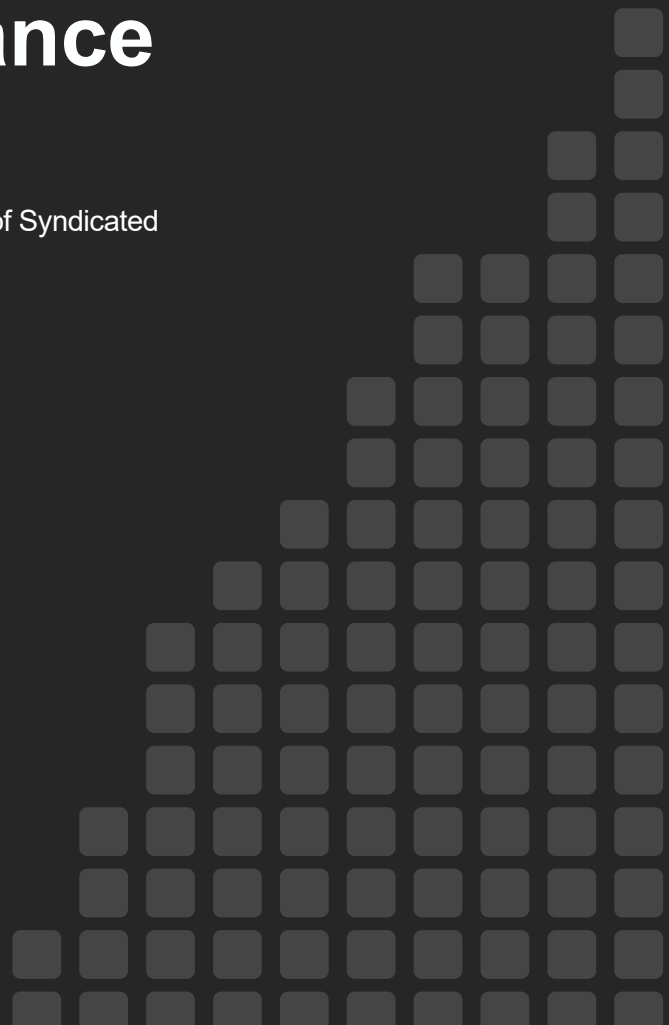RESEARCH REPORT

The Strategic and Evolving Role of Data Governance

By Christophe Bertrand, Practice Director, and Bill Lundell, Director of Syndicated Research

Enterprise Strategy Group

July 2023

Contents

Executive Summary

Report Conclusions

TechTarget's Enterprise Strategy Group (ESG) conducted an in-depth survey of 376 IT and business decision makers currently responsible for the governance technologies, processes, and programs used to manage their organizations' data at midmarket (100 to 999 employees) and enterprise (1,000 or more employees) organizations in North America (US and Canada).

Based upon the data gathered as part of this project, the report illustrates:

- **The snapshot of IT environments through a data governance lens is troubling.** Amid the ever-increasing and unstoppable growth of data, compliance-driven data governance has become a crucial matter for most organizations. The management of personally identifiable information (PII) is imperative to assure data compliance and diminish risk. Nevertheless, handling sensitive data at scale across multiple data-related applications presents a significant challenge for many organizations when it comes to PII management.

- **Data governance has moved up the corporate ladder.** The majority of data governance practices have been in place for at least five years, and most are supported by dedicated data governance teams consisting of managers, a steering committee, and even data stewards. The growing prominence of data governance programs has caught the attention of top-level executives, prompting organizations to acknowledge their significance. This development signifies that the responsibility for these programs is not limited to IT and storage management teams anymore. It has become evident that data governance is an issue that should concern the entire organization.

- **Dealing with data governance complexity requires more unified technology.** Organizations encounter numerous hurdles, such as intricate processes and the absence of a cohesive technology strategy when it comes to data governance. Failing to adhere to regulations may have detrimental consequences for organizations, including heightened exposure to cyber-threats and the reallocation of critical IT resources away from essential initiatives. Public cloud platforms have further exacerbated data governance challenges due to the presence of various data silos spread across multiple locations.

- **Managing data governance involves a lot of processes and technology.** To effectively manage data governance processes and technologies, data classification is crucial. Properly understanding data is necessary not just for minimizing compliance and security risks but also for determining the appropriate actions to be taken to optimize operational efficiency. Implementing robust data governance policies is impossible without classification, and the failure to classify data raises the level of organizational risk.

- **Cyber-risk is a serious consideration for data governance practices.** Organizations prioritize enhancing data security as a crucial factor in data governance programs due to the rise in cyber-threats and the constantly expanding attack surface. Other important aspects of data governance should also be considered, such as adhering to regulations, making informed business decisions, optimizing costs, and minimizing risks. IT departments are typically responsible for balancing these elements.

- **Data governance initiatives will garner more investment.** Many organizations have realized the advantages of data governance technologies and programs, but they continue to encounter difficulties in this field. To continue their journey, most organizations are planning to increase their spending on processes and technologies to optimize their data governance programs over the next 12-18 months. When it comes to the actual data governance technologies, organizations are prioritizing elements such as security, classification, personal information management systems, and as-a-service archive solutions.

Introduction

Research Objectives

For organizations well along on the path of their digital transformation journey, sound data governance practices are playing a strategic role. As the amount of data and value of that data to the business continue to increase, so too does the importance of managing its availability, usability, integrity, and security. Data governance is a loosely applied term in the data management space. As ecosystems evolve and become more distributed, end-users are struggling to connect the dots between the important elements of data governance like data classification, data indexing, data placement, e-discovery, and compliance.

In order to understand the benefits and challenges of data governance initiatives, establish the current state of deployments, identify gaps, and highlight future expectations, TechTarget's Enterprise Strategy Group (ESG) surveyed 376 IT and business decision makers currently responsible for the governance technologies, processes, and programs used to manage their organizations' data.

This study sought to answer the following questions:

- What is the approximate total volume of data organizations have stored on their corporate servers and storage systems? What is the approximate volume of *unstructured* data?

- At approximately what rate do organizations believe their total volume of data is growing annually? What technology features/capabilities do organizations use to manage overall data growth?

- What percentage of organizations' total data contains personally identifiable information (PII) or other sensitive data?

- In terms of data repositories, how distributed is the total volume of data for the average organization? How does this change, if at all, for PII and other sensitive information?

- For approximately how long have organizations had their data governance practices in place?

- How have stakeholder roles and levels of corporate involvement for organizations' data governance initiatives evolved over the last two years?

- Have organizations implemented or considered implementing a data governance team?

- What are the areas of greatest concern for organizations when it comes to potential non-compliance with data governance managed regulations?

- What is the biggest challenge for organizations when it comes to implementing and managing data governance initiatives?

- Generally speaking, how has the use of public cloud services impacted organizations' abilities to manage and execute data governance programs, processes, and procedures? Specifically, what SaaS application types present the biggest challenges to organizations in terms of implementing or extending data governance practices?

- Do organizations currently leverage any data classification tools or processes? For those that do, is data indexing and classification done at the metadata or content level?

- What are the most significant business drivers underlying organizations' data governance programs?

- Have organizations experienced a cybersecurity incident that impacted their ability to meet/adhere to data governance requirements in the last 12 months?

Survey participants represented a wide range of industries including manufacturing, technology, financial services, and retail/wholesale. For more details, please see the Research Methodology and Respondent Demographics sections of this report.
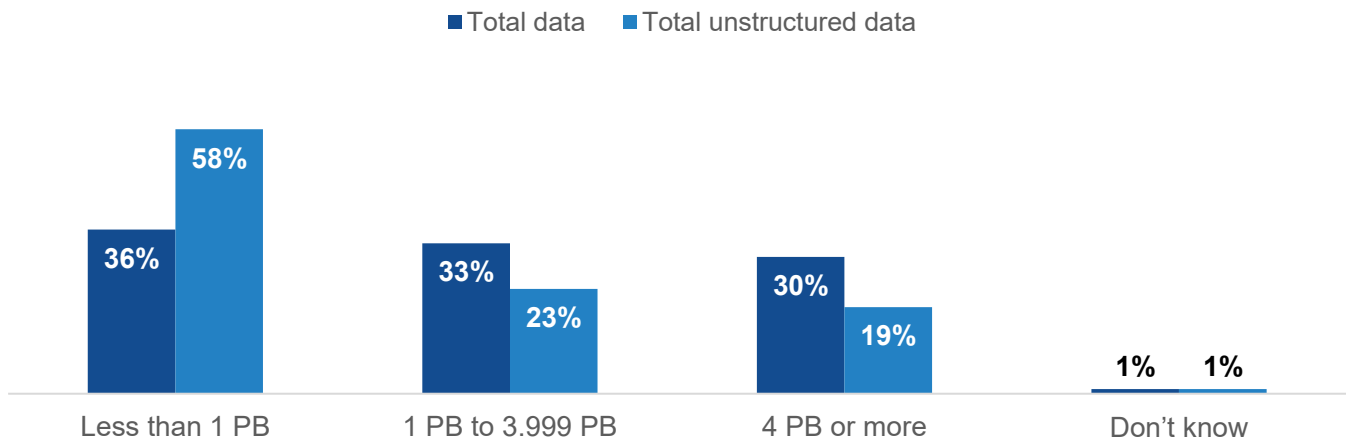
Research Findings

The Snapshot of IT Environments Through a Data Governance Lens Is Troubling

Data governance practices are evolving and becoming more strategic to most organizations; however, data governance programs are not immune to the constant challenges of data growth most organizations face, compounded by the fact that annual data growth rates are not slowing down. Indeed, nearly two-thirds (63%) of organizations report having at least 1 PB of data, meaning the average organization is managing approximately 3 PB of total data (see Figure 1). Much of this can be attributed to unstructured data, which consists of content including email messages, webpages, and audio files, among others. Specifically, more than four in ten organizations report having 1 PB or more of unstructured data, which equates to almost two-thirds of total data volumes being composed of unstructured data.

Figure 1. Organizations Have a Lot of Data to Manage and Most Is Unstructured

To the best of your knowledge, what is your organization's approximate <u>total</u> volume of data stored on corporate servers and storage systems? What is the approximate volume of <u>unstructured</u> data? (Percent of respondents, N=376)

■ Total data   ■ Total unstructured data

	Less than 1 PB	1 PB to 3.999 PB	4 PB or more	Don't know
Total data	36%	33%	30%	1%
Total unstructured data	58%	23%	19%	1%

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

And with an average annual growth in data of approximately 40% according to Figure 2, there is no relief in sight. For many organizations, this means their data will double approximately every two years. This type of data growth can put enormous stress on any IT discipline, especially less automated and mature data governance programs.

Further exacerbating general data management and growth trends is the fact that personally identifiable information (PII) is unavoidable and can't be ignored when it comes to sound data governance compliance and risk management. Nearly one-third (30%) of organizations believe that PII comprises more than 40% of their total volume of data, meaning that on average, this sensitive data accounts for approximately 35% of all data stored (see Figure 3).

Figure 2. Data Growth Rates Are Not Slowing

At approximately what rate do you believe your organization's total volume of data is growing annually? (Percent of respondents, N=376)

Category	Percent
20% or less annually	26%
21% to 50% annually	42%
More than 50% annually	32%
Don't know	1%
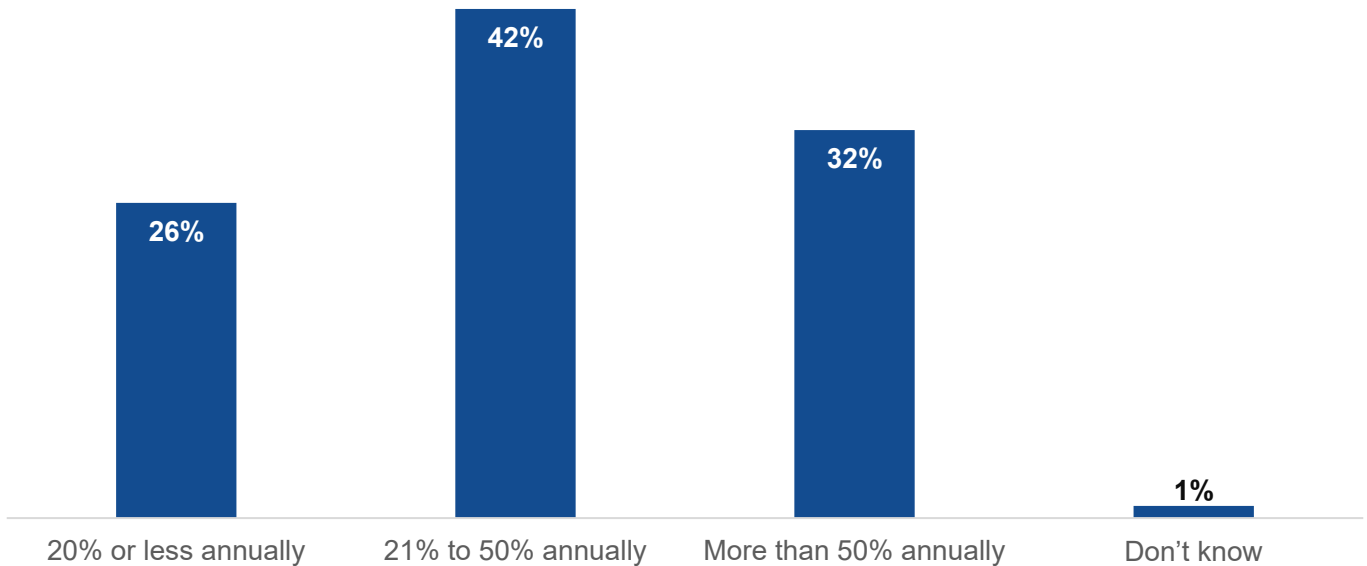
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Figure 3. Personally Identifiable Information and Other Sensitive Data Is Pervasive

What percentage of your organization's total data do you believe contains personally identifiable information (PII) or other sensitive data? (Percent of respondents, N=376)

Category	Percent
1% to 10%	5%
11% to 20%	10%
21% to 30%	30%
31% to 40%	24%
41% to 50%	21%
More than 50%	9%
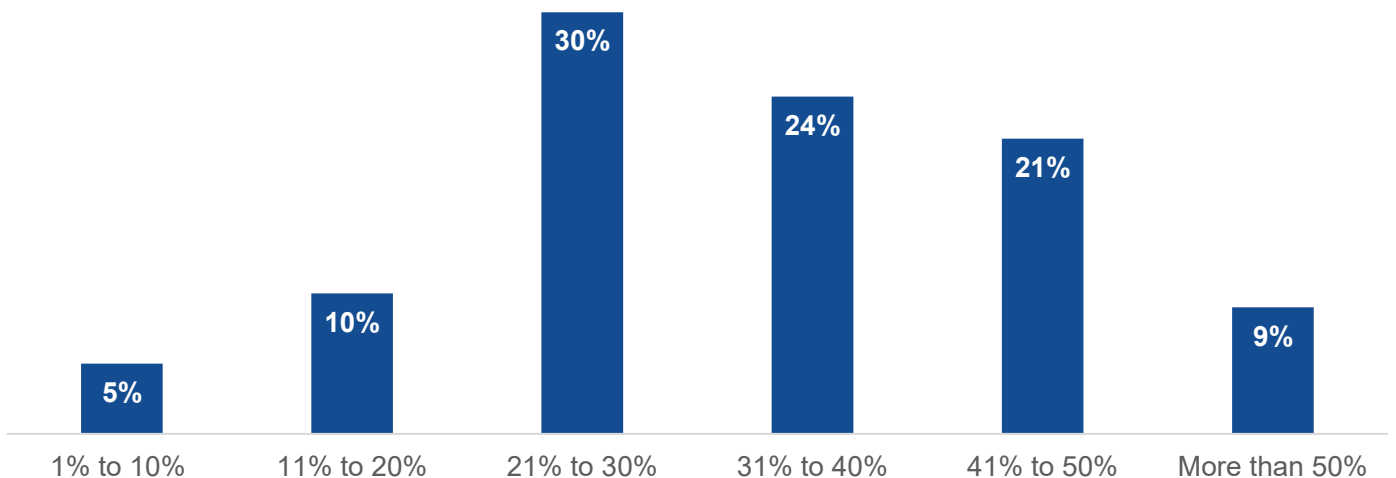
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

As seen in Figure 4, data resides in many different environments spanning the typical IT ecosystem. This means a distributed IT environment has the potential to create data sprawl, which makes data management harder and more treacherous considering the 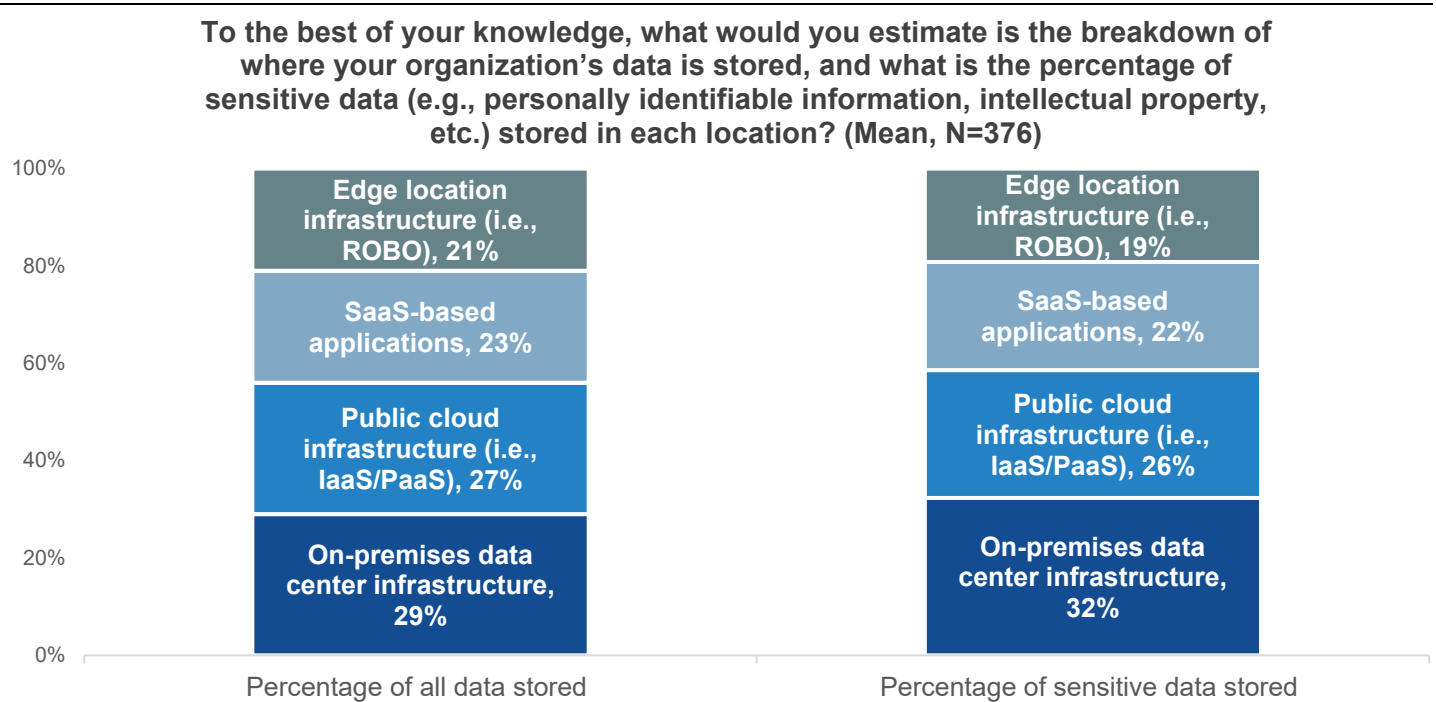amount of PII that can likely be found. While unstructured data often feeds structured repositories, and organizations report having more unstructured data than structured data, interestingly 88% of respondents believe the majority of their organization's PII resides in their *structured* data sets (see Figure 5).

Figure 4. Sensitive Data Is Distributed

To the best of your knowledge, what would you estimate is the breakdown of where your organization's data is stored, and what is the percentage of sensitive data (e.g., personally identifiable information, intellectual property, etc.) stored in each location? (Mean, N=376)

Percentage of all data stored:
- Edge location infrastructure (i.e., ROBO), 21%
- SaaS-based applications, 23%
- Public cloud infrastructure (i.e., IaaS/PaaS), 27%
- On-premises data center infrastructure, 29%

Percentage of sensitive data stored:
- Edge location infrastructure (i.e., ROBO), 19%
- SaaS-based applications, 22%
- Public cloud infrastructure (i.e., IaaS/PaaS), 26%
- On-premises data center infrastructure, 32%

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Figure 5. Most *Believe* the Majority of Personally Identifiable Information Is in Structured Data

Do you believe the majority of your organization's personally identifiable information (PII) or other sensitive data resides in unstructured or structured data sets? (Percent of respondents, N=376)
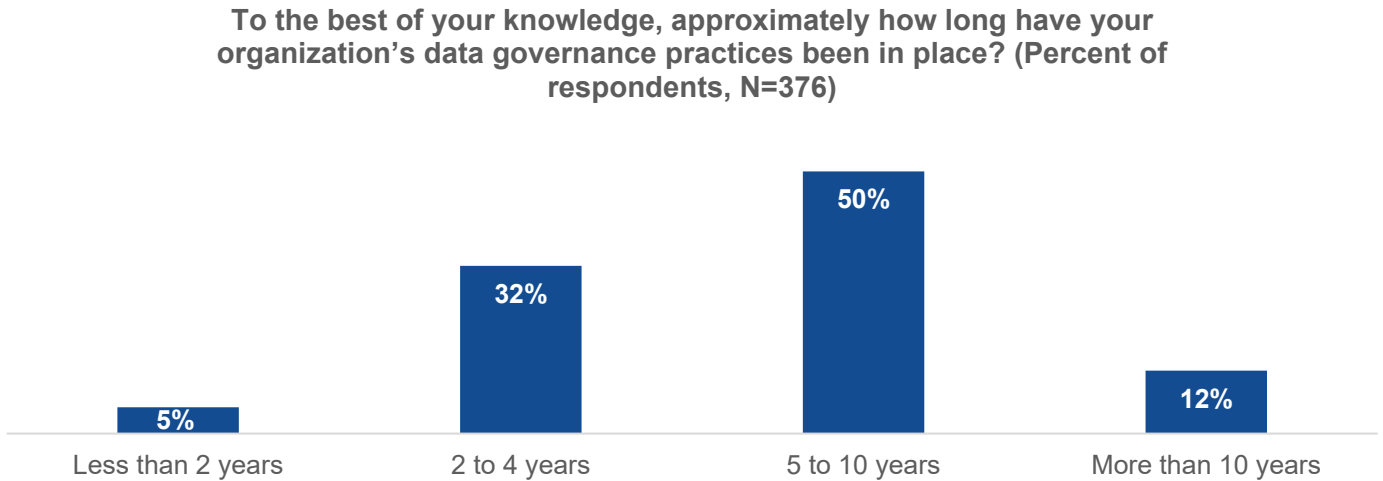
Unstructured, 12%
Structured, 88%
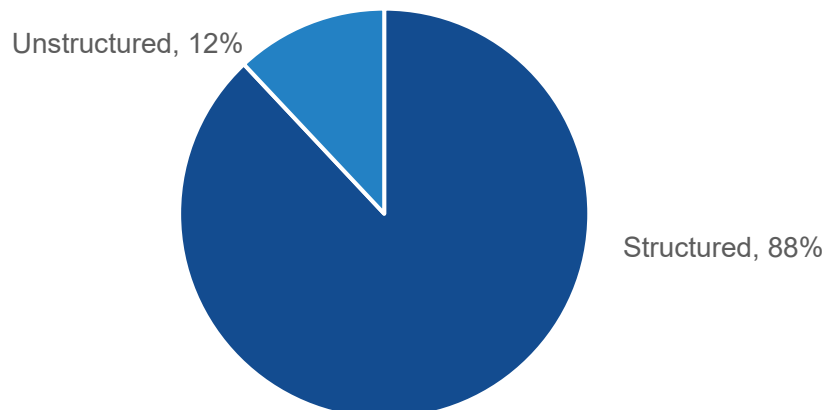
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Data Governance Has Moved Up the Corporate Ladder

Data governance is the process of managing the availability, usability, integrity, and security of the data in enterprise systems based on internal data standards and policies that also control data usage. According to Figure 6, the majority (62%) of data governance practices have been in place for at least five years.

Figure 6. Data Governance Practices Are Maturing

To the best of your knowledge, approximately how long have your organization's data governance practices been in place? (Percent of respondents, N=376)

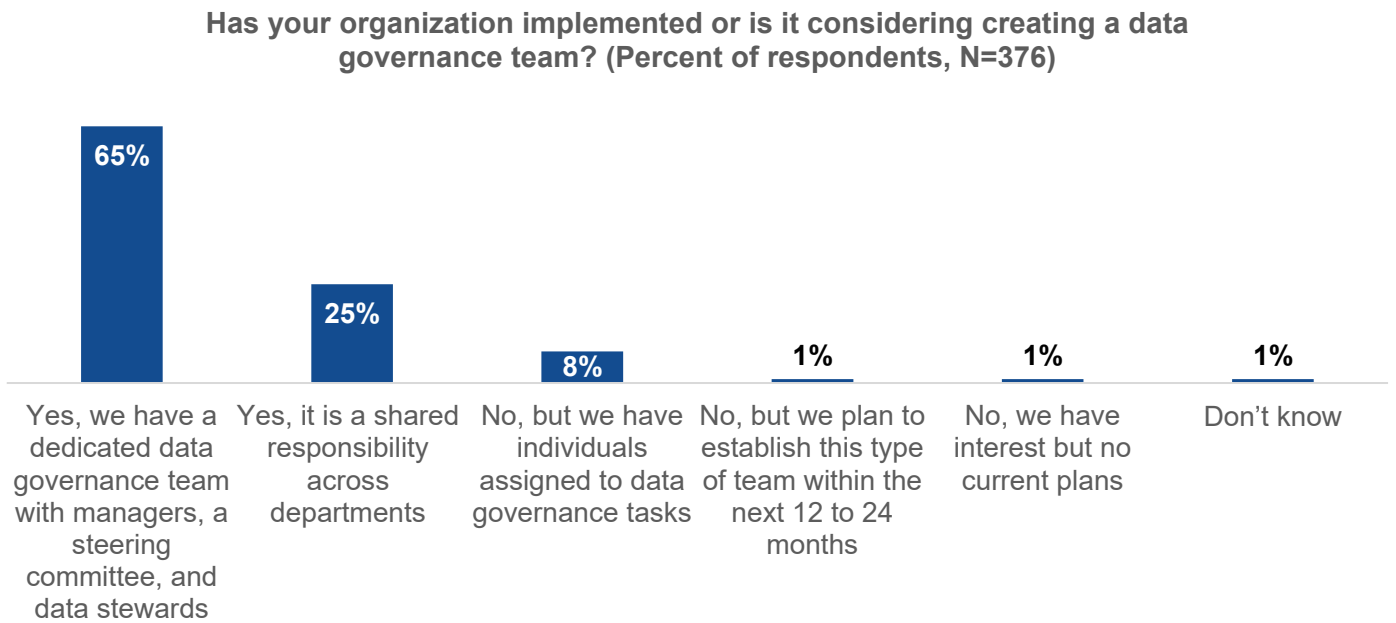| Less than 2 years	2 to 4 years	5 to 10 years	More than 10 years
5%	32%	50%	12%

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Given this, it follows that nearly two-thirds (65%) of organizations report having a dedicated data governance team consisting of managers, a steering committee, and even data stewards (see Figure 7). At a minimum, a quarter say they tackle data governance as a shared responsibility across departments.

This means data governance programs are gaining additional visibility in many organizations among newer audiences. Indeed, nearly half say IT is no longer the sole owner of data governance programs, and involvement now includes c-level executives and even boards of directors for oversight and guidance (see Figure 8). Effective data governance can no longer be just storage administration best practices.
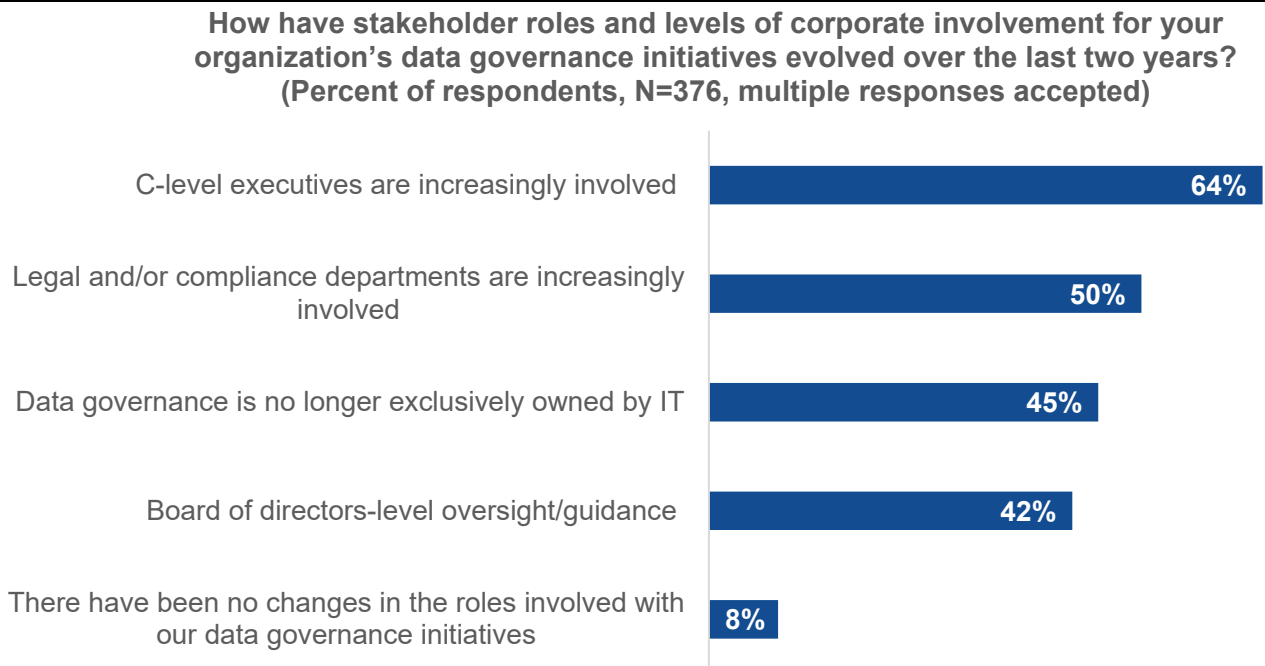
Figure 7. Status of Data Governance Team Implementations

Has your organization implemented or is it considering creating a data governance team? (Percent of respondents, N=376)

65%	Yes, we have a dedicated data governance team with managers, a steering committee, and data stewards
25%	Yes, it is a shared responsibility across departments
8%	No, but we have individuals assigned to data governance tasks
1%	No, but we plan to establish this type of team within the next 12 to 24 months
1%	No, we have interest but no current plans
1%	Don't know

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Figure 8. Evolution of Roles Involved with Data Governance Programs

How have stakeholder roles and levels of corporate involvement for your organization's data governance initiatives evolved over the last two years? (Percent of respondents, N=376, multiple responses accepted)

C-level executives are increasingly involved	64%
Legal and/or compliance departments are increasingly involved	50%
Data governance is no longer exclusively owned by IT	45%
Board of directors-level oversight/guidance	42%
There have been no changes in the roles involved with our data governance initiatives	8%

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Enterprise Strategy Group
by TechTarget

Dealing with Data Governance Complexity Requires More Unified Technology

Overall, organizations are contending with a lot of complexity and a lack of a unified technology approach. General challenges fall into the following categories: data, regulations, technology, and strategy. Specifically, when it comes to regulations, non-compliance has a wide range of negative business impacts, including severe concerns such as increased cyber-risk and diversion of IT resources from important projects (see Figure 9).

Figure 9. Non-compliance Has a Range of Negative Business Impacts

What is the area of greatest concern related to your organization's potential non-compliance with its data governance managed regulations? (Percent of respondents, N=376, one response accepted)

| Category	Percent
Increased cyber-risk	22%
Diversion of IT resources from long-term or business-critical projects	19%
Cost of recovery to achieve compliance	11%
Impact on public perception/reputation	11%
Legal action as a result of compliance failures	9%
Competitive disadvantage	7%
Fines/penalties related to compliance failures	7%
Loss of business revenue/impact on sales	6%
Loss of accreditation/certification	4%
None of the above	3%

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

When it comes to the biggest overall data governance challenges in the context of data types, the majority (65%) of respondents report that structured data is the biggest pain point (see Figure 10). In terms of SaaS applications, relational data sets like DBaaS, CRM, and ERP together account for biggest percentage of challenges (see Figure 11). This is likely because data sets such as email, file sharing, and collaboration were some of the first data types included in initial data governance applications like those used for discovery, indexing, and classification.

Figure 10. Most View Structured Data as the Bigger Data Governance Challenge

What is the biggest challenge for your organization when it comes to implementing and managing its data governance initiatives? (Percent of respondents, N=376)

Don't know, 1%

Unstructured data, 34%

Structured data, 65%
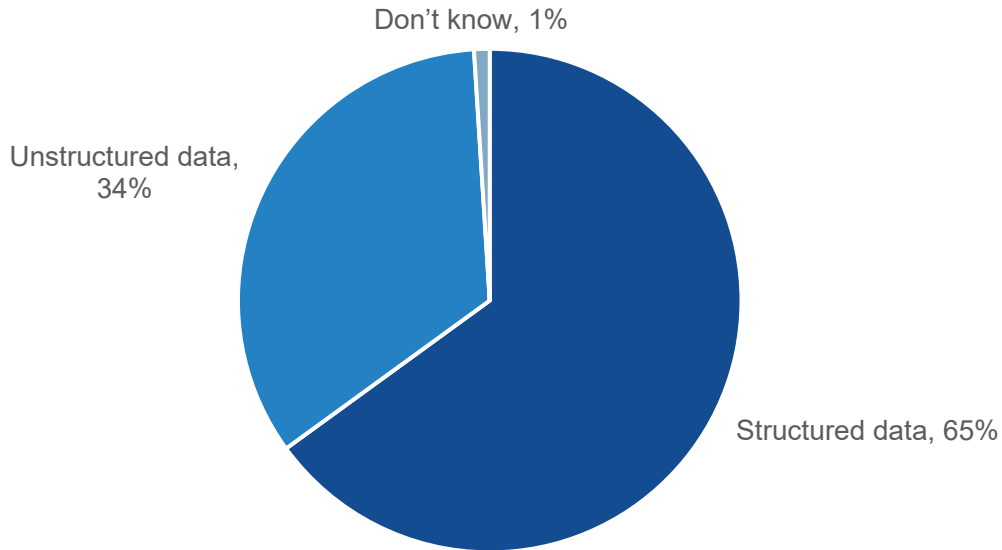
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

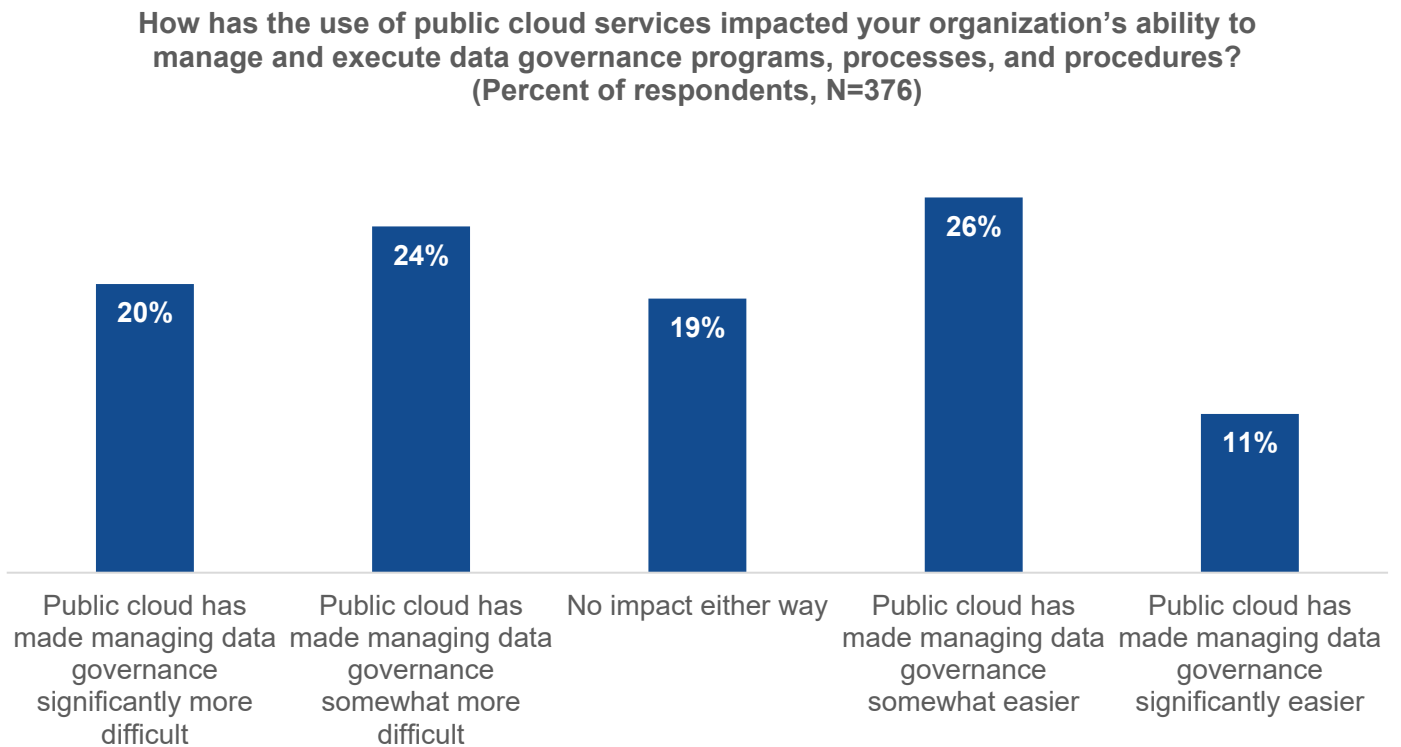**Figure 11.** DBaaS and CRM Are SaaS Applications that Provide the Biggest Data Governance Challenges

Which SaaS application type presents the biggest challenge to your organization when it comes to implementing or extending its data governance practices? (Percent of respondents, N=353)

ERP, 9%

File sharing, 10%

Email, 13%

Collaboration, 15%

CRM, 20%

Database-as-a-service (DBaaS), 34%
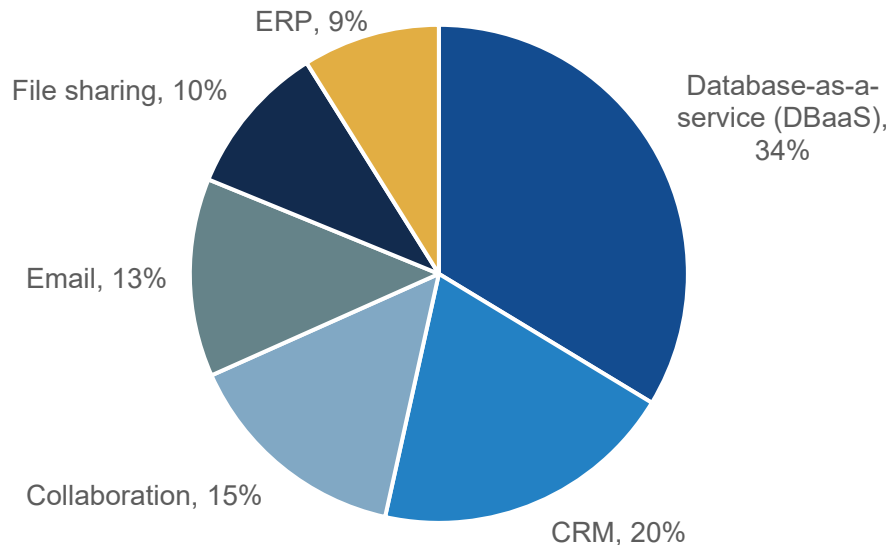
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

How is the cloud impacting data governance initiatives? The prevalence of hybrid and multi-cloud infrastructure has led to a rapid increase in cloud adoption. However, this has resulted in a challenge for data governance initiatives due to the presence of various data silos spread across multiple locations. Without proper knowledge of the data's location, type, and quantity, implementing data governance standards becomes an arduous task. As such, it is not surprising that more than four in ten respondents say public cloud services make data governance somewhat (24%) or significantly (20%) more difficult (see Figure 12).

Figure 12. Plurality of Organizations Believe Public Cloud Services Have Made Data Governance More Difficult
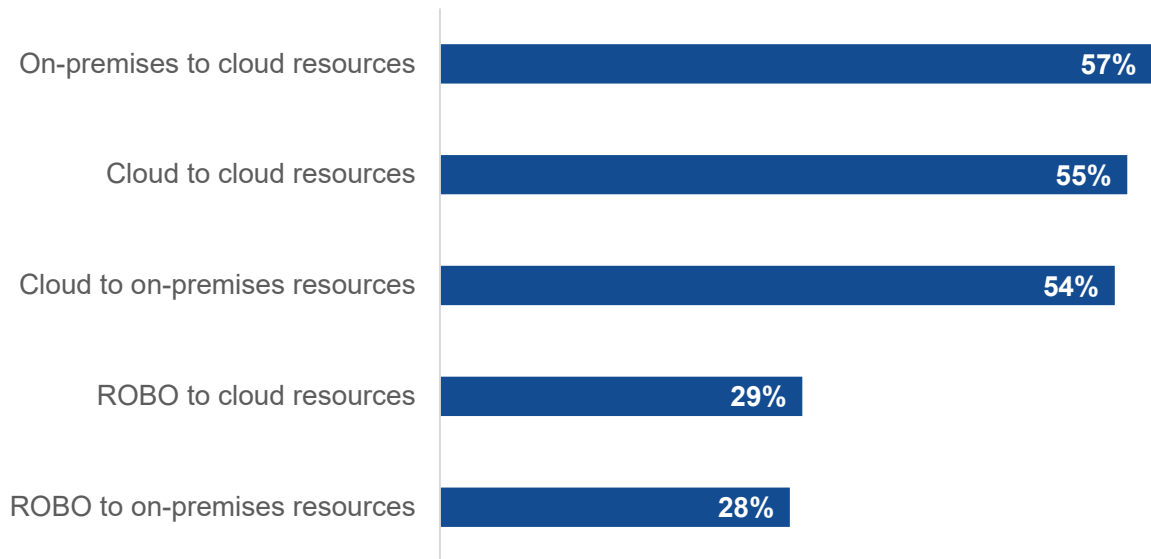
How has the use of public cloud services impacted your organization's ability to manage and execute data governance programs, processes, and procedures? (Percent of respondents, N=376)

20%	24%	19%	26%	11%
Public cloud has made managing data governance significantly more difficult	Public cloud has made managing data governance somewhat more difficult	No impact either way	Public cloud has made managing data governance somewhat easier	Public cloud has made managing data governance significantly easier

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Digging a little deeper into cloud and distributed environments challenges, it's clear that most organizations experience difficulties moving data to and/or from public cloud repositories (see Figure 13). And, in general, legacy challenges like maintaining file system information, the size of the data sets, and network latency and bandwidth still plague data movement operations (see Figure 14).

Figure 13. Cloud Provides Most Common Data Movement SLA Challenges
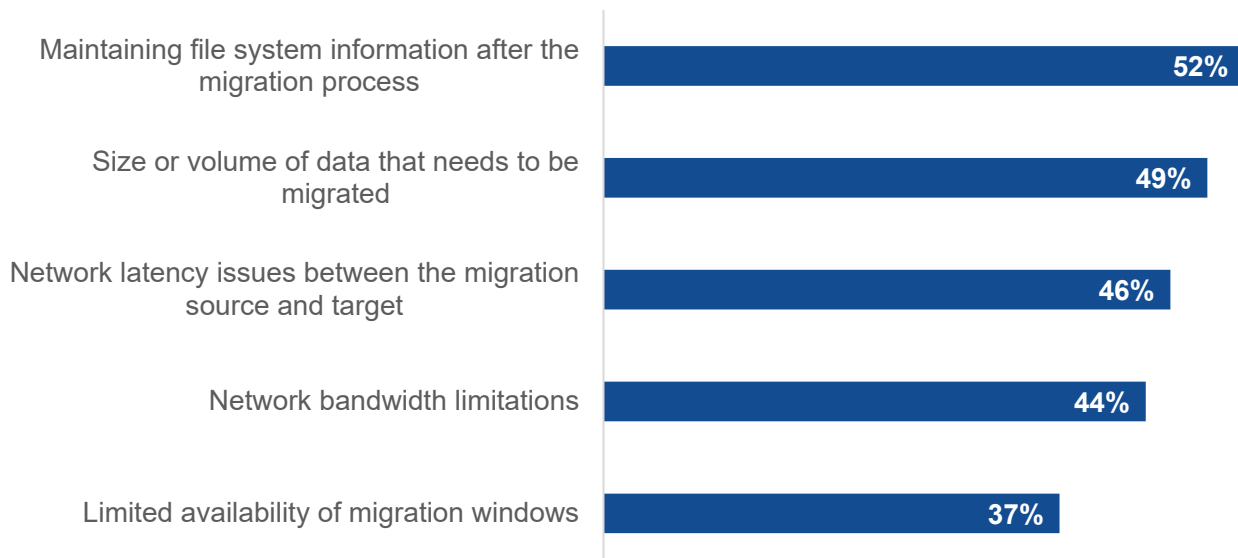
Which location movements typically provide your organization with data movement/placement SLA challenges? (Percent of respondents, N=267, multiple responses accepted)

Category	Percent
On-premises to cloud resources	57%
Cloud to cloud resources	55%
Cloud to on-premises resources	54%
ROBO to cloud resources	29%
ROBO to on-premises resources	28%

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Figure 14. Biggest Data Movement Challenges Faced Meeting Data Access SLAs

What are the biggest data movement/placement challenges your organization faces in meeting its data access SLAs when migrating or moving data between locations during data tiering operations? (Percent of respondents, N=267, multiple responses accepted)

Category	Percent
Maintaining file system information after the migration process	52%
Size or volume of data that needs to be migrated	49%
Network latency issues between the migration source and target	46%
Network bandwidth limitations	44%
Limited availability of migration windows	37%

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Managing Data Governance Involves a Lot of Processes and Technology

When it comes to data governance process and technology, data classification plays a key role. Data classification is defined as the process of identifying data by relevant categories so that it may be stored, protected, and leveraged more efficiently for business outcomes. Understanding data is essential not only for compliance risk mitigation, but also to identify what should be done about it. Without classification, it is impossible to implement sound data governance policies. Data that is not classified also increases risk. Additionally, content-level classification enables organizations to implement more advanced data governance procedures. It follows then that more than three-quarters (77%) of organizations currently leverage some form of data classification technologies and/or processes (see Figure 15).

Figure 15. Majority of Organizations Use Data Classification Tools or Processes

Does your organization currently leverage any data classification tools or processes? (Percent of respondents, N=376)

- Yes: **77%**
- No, but we have plans to do so over the next 12-24 months: **18%**
- No, and we have no plans to do so: **5%**
- Don't know: **1%**
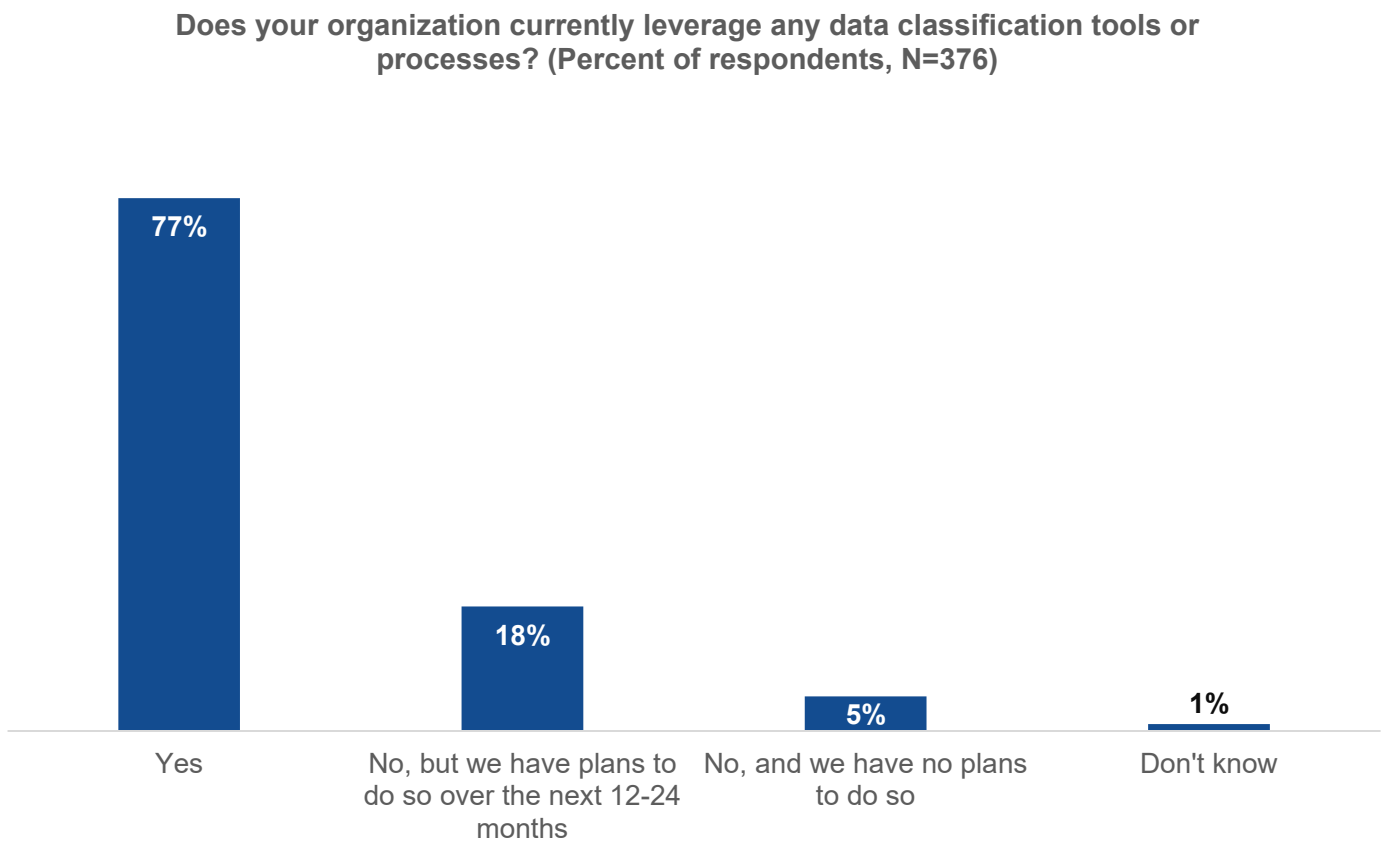
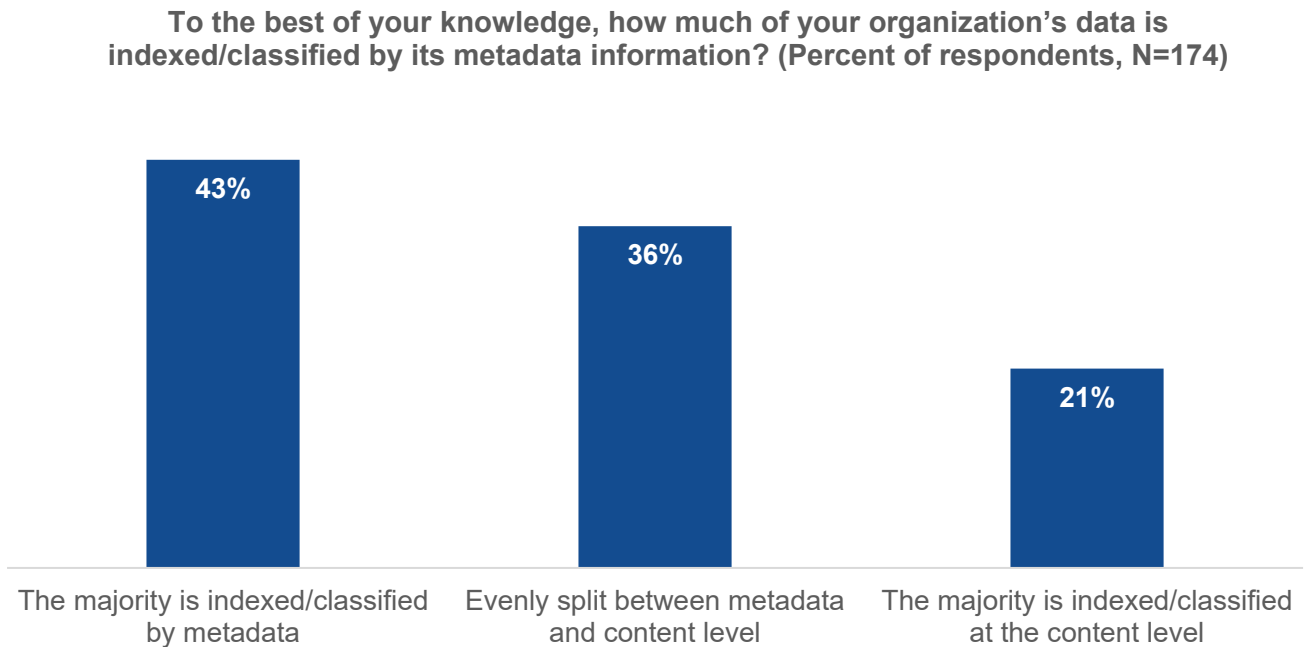*Source: Enterprise Strategy Group, a division of TechTarget, Inc.*

Currently, the majority of organizations that are classifying their data take a hybrid approach. Indeed, Figure 16 reveals that 60% of organizations that currently employ data classification technologies and/or processes both analyze and classify metadata and look into each file by examining and classifying its content. Among these organization taking a hybrid approach, the plurality (43%) indicates a skew toward indexing and classifying at the metadata level, with another 36% reporting an even split between metadata- and content-level classification (see Figure 17).

Figure 16. Primary Approach to Data Classification

Which of the following best describes your organization's approach to data classification? (Percent of respondents, N=289)
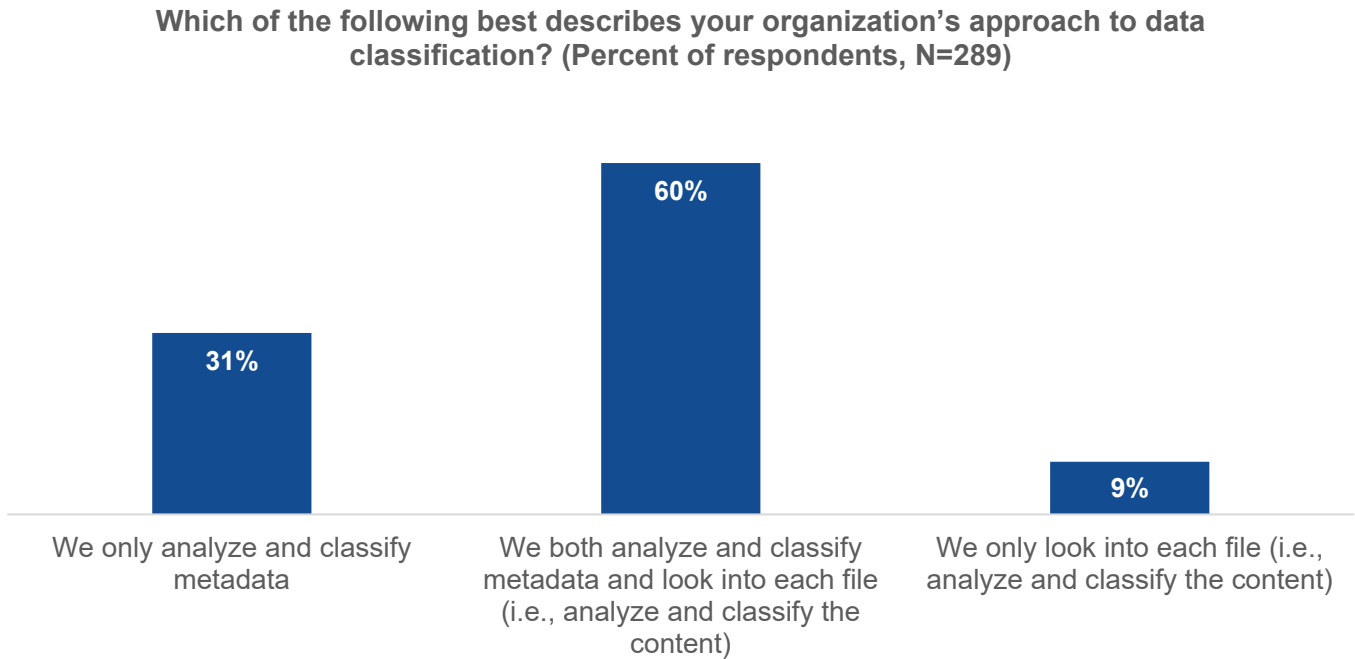
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Figure 17. Metadata Indexing Is the Preferred Approach of Organizations with Hybrid Data Classification Strategies
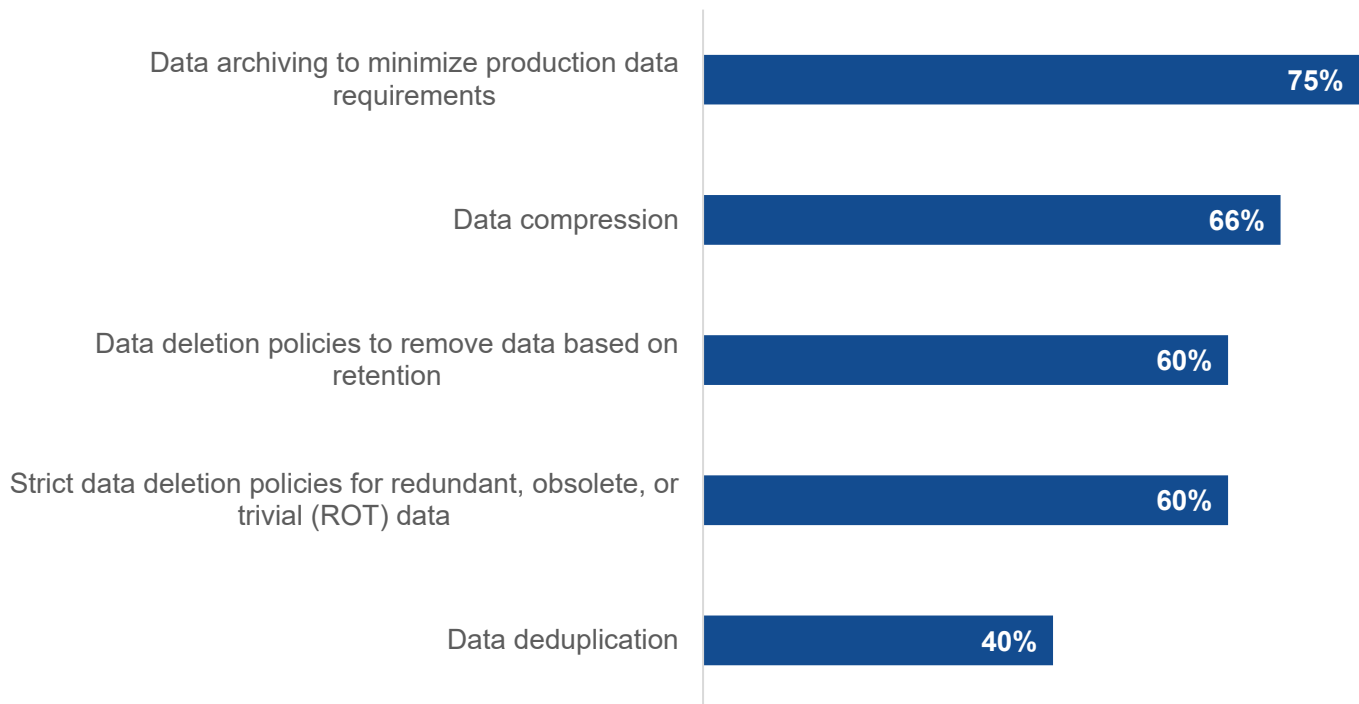
To the best of your knowledge, how much of your organization's data is indexed/classified by its metadata information? (Percent of respondents, N=174)

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

In the not-too-distant past, businesses kept most data on an indefinite basis. Now, organizations better understand the risks of keeping data beyond its usefulness or a regulated period. When it comes to managing overall data growth, at least two-thirds of organizations leverage data archiving and/or compression (see Figure 18). However, there does seem to be more receptiveness to deleting unnecessary data, with more than 8 in 10 organizations pointing to deletion policies for data with retention requirements and/or redundant, obsolete, or trivial (ROT) data.

Figure 18. Data Archiving and Compression Most Commonly Used Tools to Manage Data Growth

What technology features/capabilities does your organization use to manage its overall data growth? (Percent of respondents, N=376, multiple responses accepted)

Category	Percent
Data archiving to minimize production data requirements	75%
Data compression	66%
Data deletion policies to remove data based on retention	60%
Strict data deletion policies for redundant, obsolete, or trivial (ROT) data	60%
Data deduplication	40%

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

For data that is kept indefinitely, secondary data reuse generates broad benefits that are not just for IT, including greater data visibility and subsequent business agility. However, given the amount of sensitive data included in secondary data sets, this reused data must be compliant. Organizations cannot risk exposing sensitive data to unauthorized personnel such as test and development engineers. Though many data obfuscation techniques are in use for this objective, automation takes center stage in the form of data masking, synthetic data creation, or tokenization, and this is a key element to successful data reuse (see Figure 19). Unfortunately, 41% of respondents still report using manual processes, which can lead to more sensitive data exposure incidents.

Enterprise Strategy Group
by TechTarget

Figure 19. Automated Data Masking Most Commonly Used to Ensure Data Reuse Compliance

**What process or technology feature does your organization use to make sure
its data reuse processes maintains its data governance and compliance?
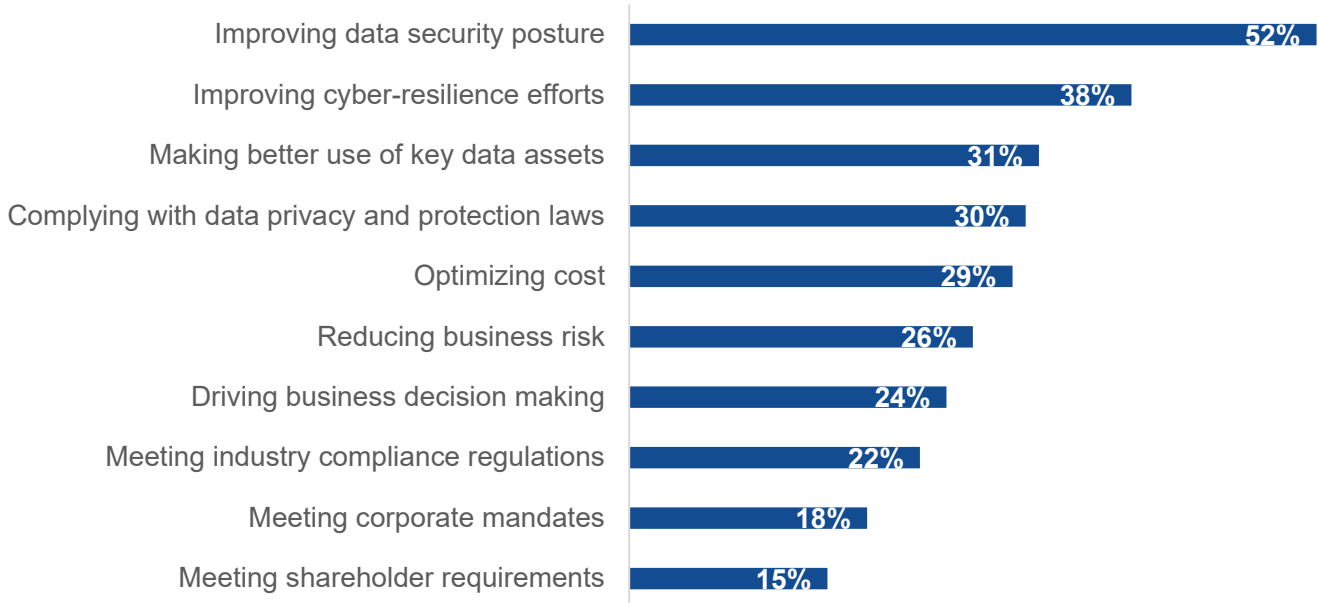(Percent of respondents, N=367, multiple responses accepted)**

Category	Percent
Automated data masking for sensitive data sets	63%
Automated creation of synthetic data for sensitive data sets	55%
Automated data tokenization for sensitive data sets	54%
Manual processes	41%
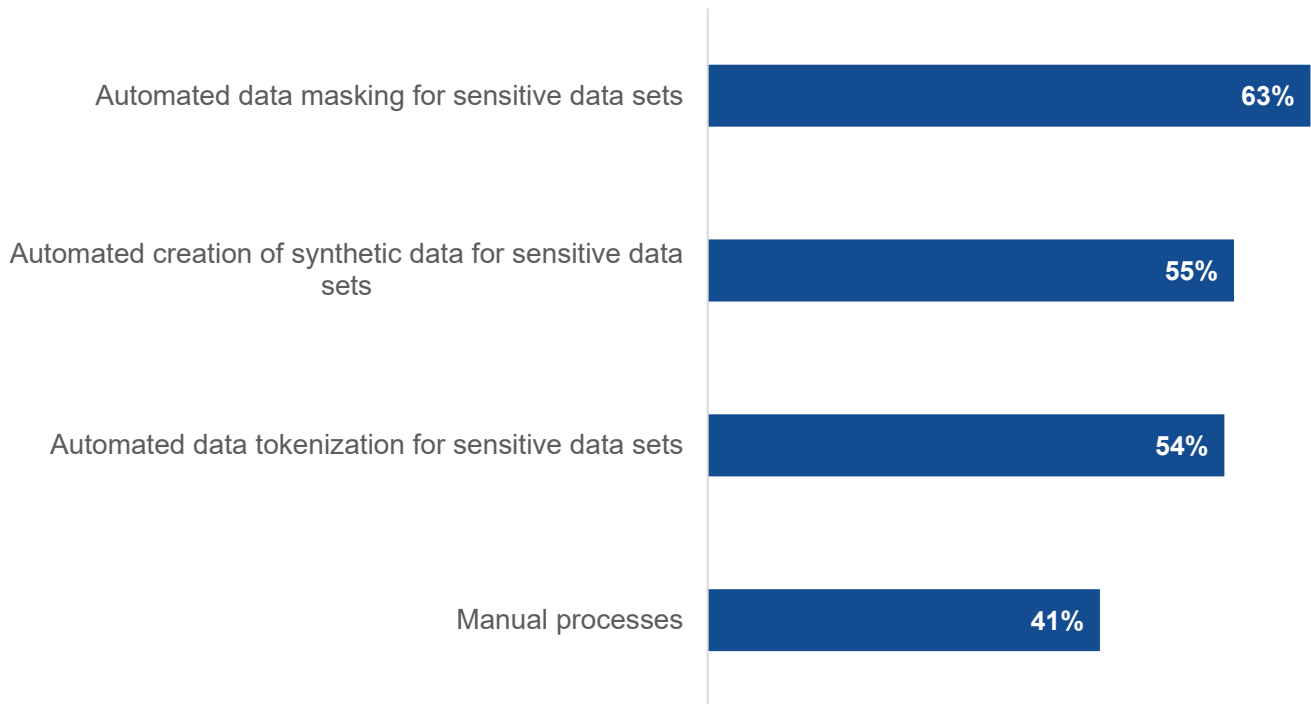
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Cyber-risk Is a Serious Consideration for Data Governance Practices

Improved data security is at the top of the list for both most significant data governance business drivers and most important data governance features/capabilities (see Figure 20 and Figure 21). This is likely due to the current increase in cyber-risk and the pervasiveness of ransomware attacks. In fact, 70% of organizations cited improving data security and/or their cyber-resilience efforts as key drivers of their data governance programs, underscoring the link between data governance and a strong cybersecurity posture. However, key data governance elements such as meeting regulations, improving business decisions, optimizing cost, and reducing business risk must not take a backseat to security, and IT is often tasked with striking this balance.

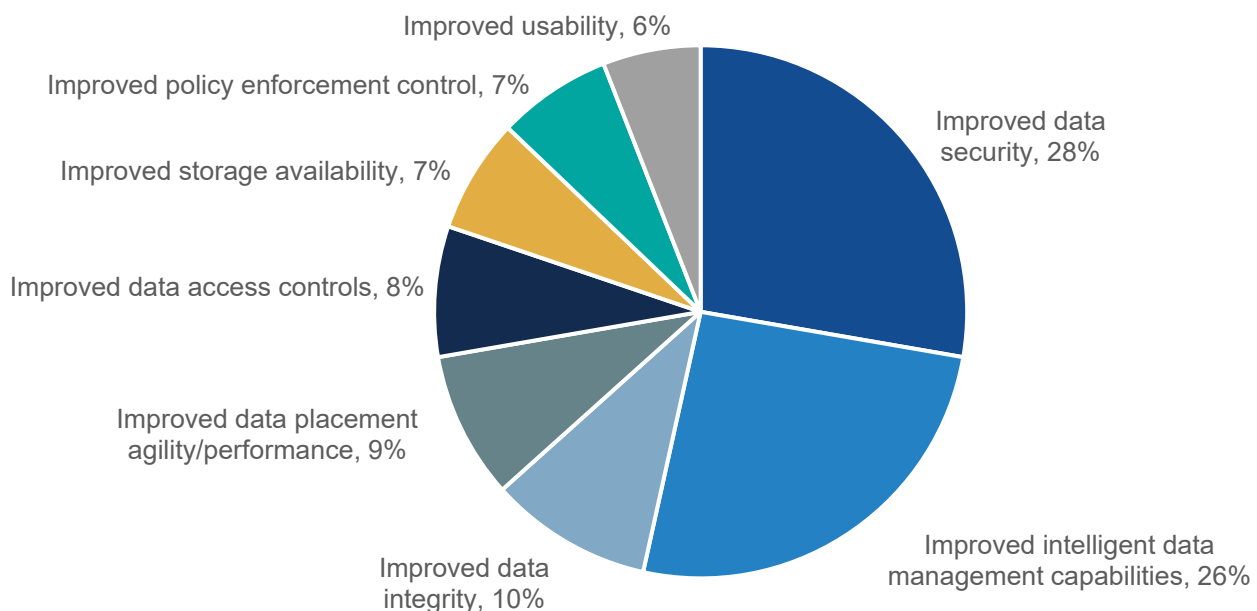**Figure 20.** Data Security and Cyber-risks Are Driving Data Governance Decisions

What are the most significant business drivers underlying your organization's data governance programs? (Percent of respondents, N=376, three responses accepted)

Driver	Percent
Improving data security posture	52%
Improving cyber-resilience efforts	38%
Making better use of key data assets	31%
Complying with data privacy and protection laws	30%
Optimizing cost	29%
Reducing business risk	26%
Driving business decision making	24%
Meeting industry compliance regulations	22%
Meeting corporate mandates	18%
Meeting shareholder requirements	15%

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Figure 21. Most Important Data Governance Feature/Capability Is Improved Data Security

What is the most important feature/capability your organization would like to have in its data governance solutions? (Percent of respondents, N=376)

- Improved usability, 6%
- Improved policy enforcement control, 7%
- Improved storage availability, 7%
- Improved data access controls, 8%
- Improved data placement agility/performance, 9%
- Improved data integrity, 10%
- Improved data security, 28%
- Improved intelligent data management capabilities, 26%

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

With such a focus on security, data governance practices clearly are not immune to cyber-threats. Indeed, more than half (56%) of organizations have experienced a cyber-incident such as ransomware or data exfiltration that impacted their ability to meet data governance requirements (see Figure 22). Nearly three-quarters (73%) reported that the event led to the exposure of sensitive data. And while 59% of organizations indicated they were temporarily unable to access data, of greater concern is the fact that 53% faced the permanent loss of data (see Figure 23).

Figure 22. Cyber-incidents Are Leading to Non-compliance with Data Governance Requirements

Has your organization experienced a cybersecurity incident (e.g., ransomware, data exfiltration, etc.) that impacted its ability to meet/adhere to its data governance requirements in the last 12 months? (Percent of respondents, N=376)

Don't know, 1%

No, 43%

Yes, 56%
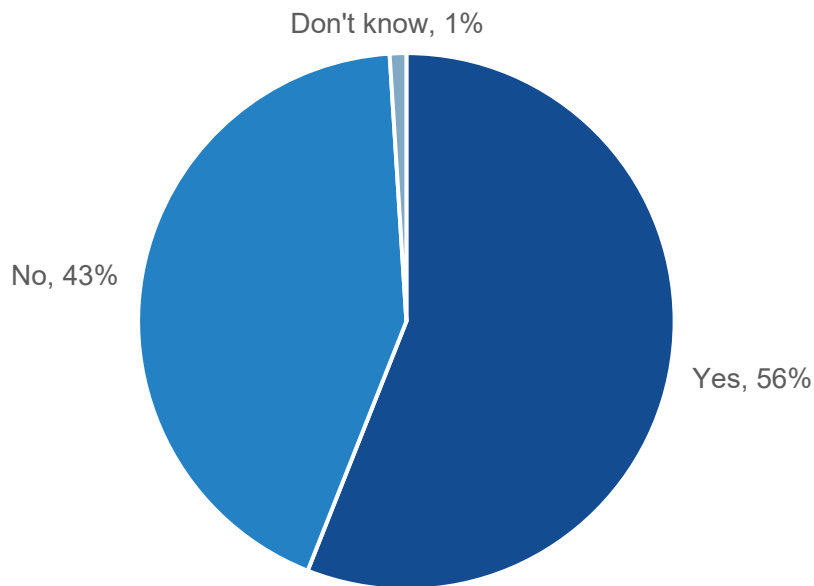
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Figure 23. Impact Cyber-incident(s) Had on Ability to Meet Data Governance Requirements

How did the cybersecurity incident you experienced impact your organization's ability to meet/adhere to its data governance requirements? (Percent of respondents, N=211, multiple responses accepted)

Sensitive data exposure	73%
Temporary inability to access data	59%
Permanent deletion of data	53%
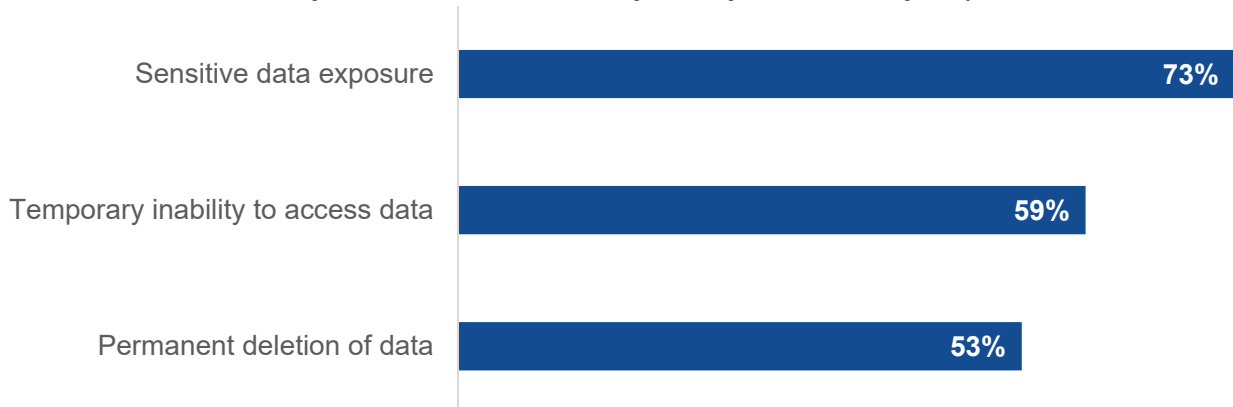
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

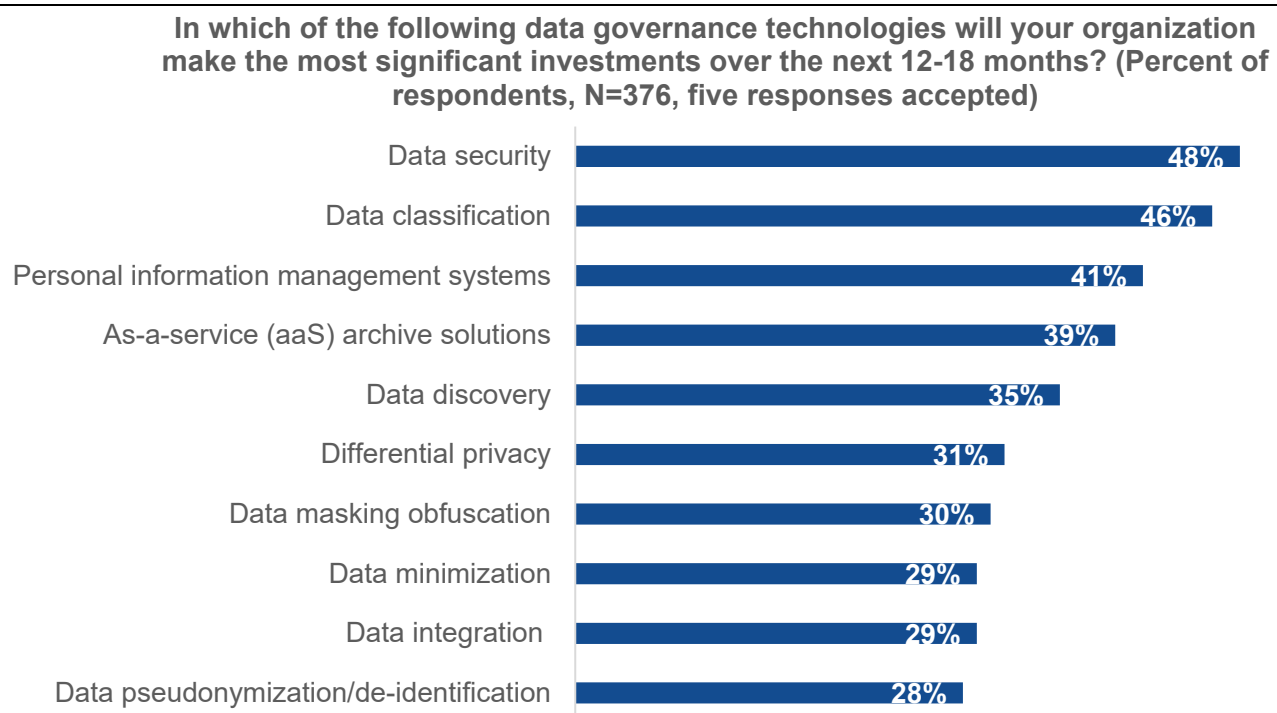## Data Governance Initiatives Will Garner More Investment

While organizations have reaped the benefits of data governance technologies and programs, they still face challenges in this area, so it makes sense that 85% of organizations expect to increase spending on data governance technologies over the next 12-18 months (see Figure 24). When it comes to the actual data governance technologies, organizations are prioritizing elements such as security, classification, personal information management systems, and as-a-service archive solutions (see Figure 25).

Figure 24. Most Organizations Plan to Increase Data Governance Spending

How would you describe your organization's change, if any, in spending on data governance technologies and programs over the next 12-18 months? (Percent of respondents, N=376)

Increase significantly	31%
Increase slightly	54%
No change	15%
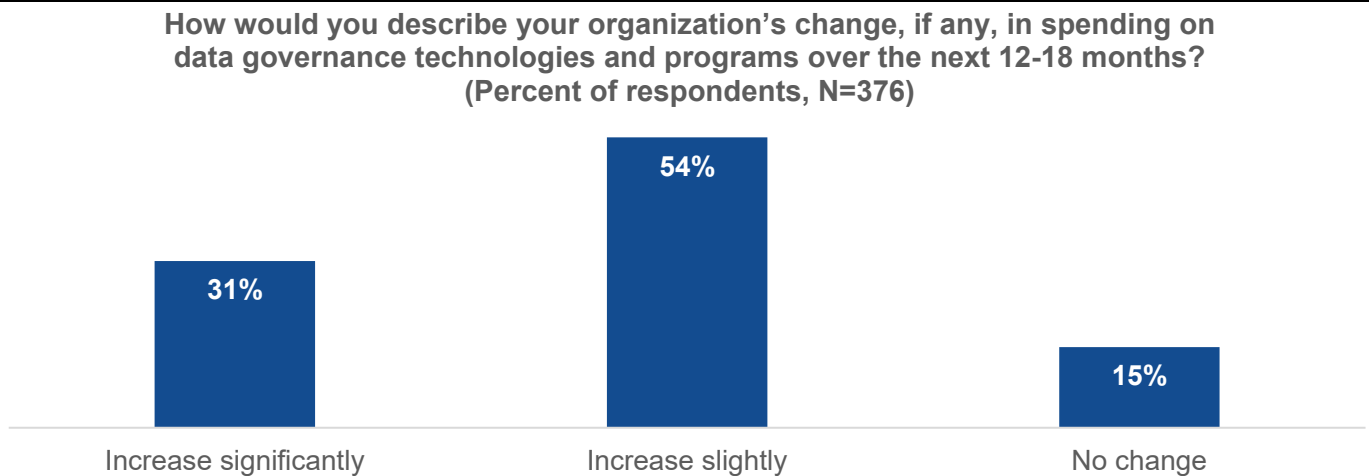
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Figure 25. Data Security and Classification Likeliest to See Most Significant Investments

In which of the following data governance technologies will your organization make the most significant investments over the next 12-18 months? (Percent of respondents, N=376, five responses accepted)

Data security	48%
Data classification	46%
Personal information management systems	41%
As-a-service (aaS) archive solutions	39%
Data discovery	35%
Differential privacy	31%
Data masking obfuscation	30%
Data minimization	29%
Data integration	29%
Data pseudonymization/de-identification	28%

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Conclusion

Data governance fueled by compliance mandates has become a top priority for most organizations against a backdrop of constant and massive data growth. Respondents to our research correctly identify that it is necessary to consider personally identifiable information for sound data governance compliance and risk management, as it simply cannot be overlooked from a risk perspective. Yet organizations today are struggling, and ESG believes that there is a PII disconnect undermining many other data-related initiatives. This is likely associated with the reported complexity of managing sensitive data at scale in structured data sets such as databases and specific data-related SaaS applications.

Many organizations are starting to recognize the importance of data governance programs, as they gain more visibility among executive leadership. This means that IT and storage management teams are no longer the only ones responsible for these programs. ESG believes that involving c-level executives and board members in overseeing and guiding data governance is crucial for its effectiveness. It has become evident that data governance is a business-level issue.

Organizations are facing a great deal of complexity in the realm of technology, and without a unified approach to management, they are struggling to keep up. The prevalence of hybrid and multi-cloud infrastructure only adds to the challenge, leading to difficulties in data governance as a result of data silos being dispersed across numerous locations. Understanding data is crucial for compliance risk mitigation and determining appropriate actions. The role of data classification is significant in this regard, as it allows for the implementation of sound data governance policies. Failure to classify data can increase the risk of mishandling sensitive information. ESG's perspective is that classification must go beyond just metadata and include content-level analysis, which is key to de-risking organizations from PII and content standpoints.

This is especially pertinent in the current climate of constant and heightened cyber-risk. Indeed, not surprisingly, organizations have identified advancing data security and bolstering cyber-resilience as fundamental factors driving their data governance initiatives. This highlights the crucial connection between data governance and a robust cybersecurity posture, and underscores one of the many reasons organizations are prioritizing data governance initiatives and allocating more budget toward data governance technologies over the next 12-18 months.

In order to enable organizations to address current data governance challenges and meet their objectives, Enterprise Strategy Group highlights the following:

- **Data governance is a "team sport."** As an IT professional or user, it would be beneficial to utilize the insights from this research as a means to initiate discussions with executive and business teams regarding the governance implications of handling large volumes of data. It is crucial to develop cross-organizational strategies and procedures for analyzing, categorizing, and securing data, particularly the most sensitive assets.

- **There can be no reuse without governance.** To prevent the negative consequences of mishandling or cyber-related threats to sensitive data like personally identifiable information, IT leaders must enforce rigorous processes and rules regarding any further utilization of this data, such as for analytical purposes, throughout the organization. Non-compliant data should not be reused.

- **Vendors have a unique opportunity.** As organizations continue to allocate more funds toward data governance, vendors within the data management, compliance, and governance ecosystem are presented with new opportunities to offer their technologies to a wider range of clients. In order to succeed as part of this ecosystem solution, it is becoming increasingly important for vendors to focus on areas such as data classification and analysis. Additionally, certain markets and categories, including cyber-resilience, data management, and governance management, are beginning to converge and should also be considered core partnership opportunities for solution development.

Hitachi Vantara

Hitachi Vantara, a wholly-owned subsidiary of Hitachi Ltd., delivers the intelligent data platforms, infrastructure systems, and digital expertise that supports more than 80% of the Fortune 100. To learn how Hitachi Vantara turns businesses from data-rich to data-driven through agile digital processes, products, and experiences, visit hitachivantara.com.

LEARN MORE

Research Methodology

To gather data for this report, Enterprise Strategy Group conducted a comprehensive online survey of IT and line-of-business professionals from private- and public-sector organizations in North America (United States and Canada) between August 2, 2022 and August 5, 2022. To qualify for this survey, respondents were required to be personally familiar with and/or responsible for the data governance technologies, processes, and programs used to manage their organizations' data. Additionally, organizations were required to have implemented some kind of data governance technology, program, or process. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on a number of criteria) for data integrity, we were left with a final total sample of 376 IT and line-of-business professionals.

Please see the *Respondent Demographics* section of this report for more information on these respondents.

Note: Totals in figures and tables throughout this report may not add up to 100% due to rounding.

Respondent Demographics

The data presented in this report is based on a survey of 376 qualified respondents. Figure 26 through Figure 29 detail the demographics of the respondent base at an organizational level.

Figure 26. Respondents by Number of Employees

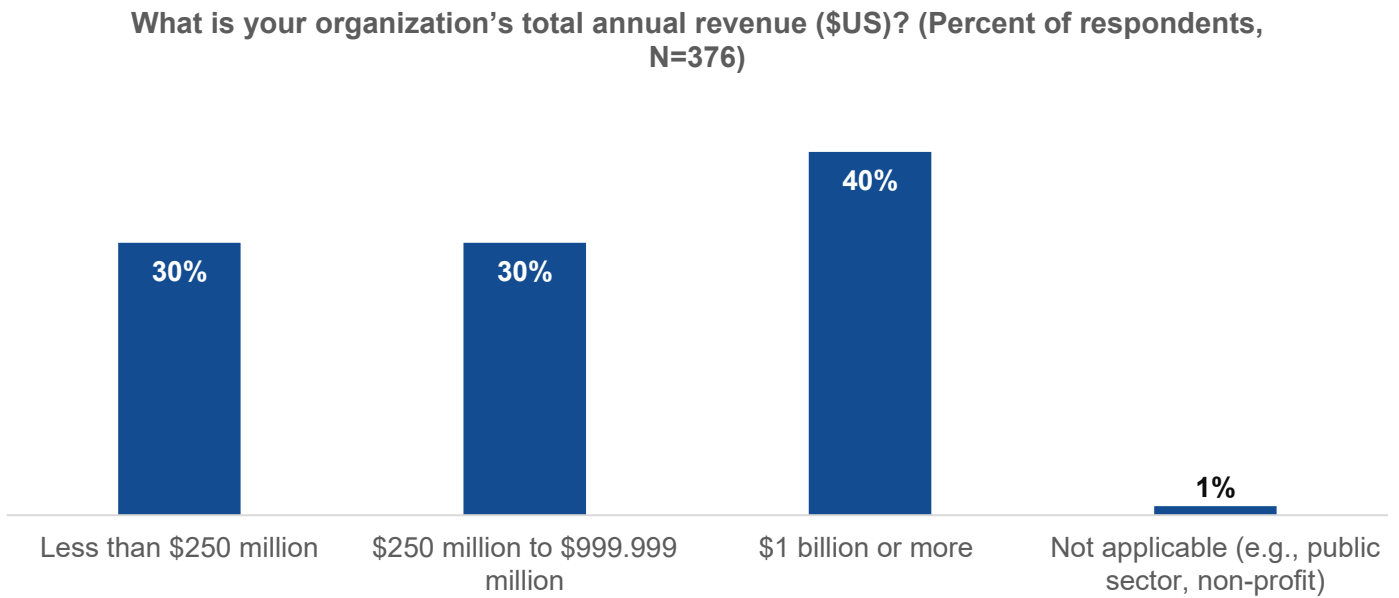**How many total employees does your organization have worldwide? (Percent of respondents, N=376)**
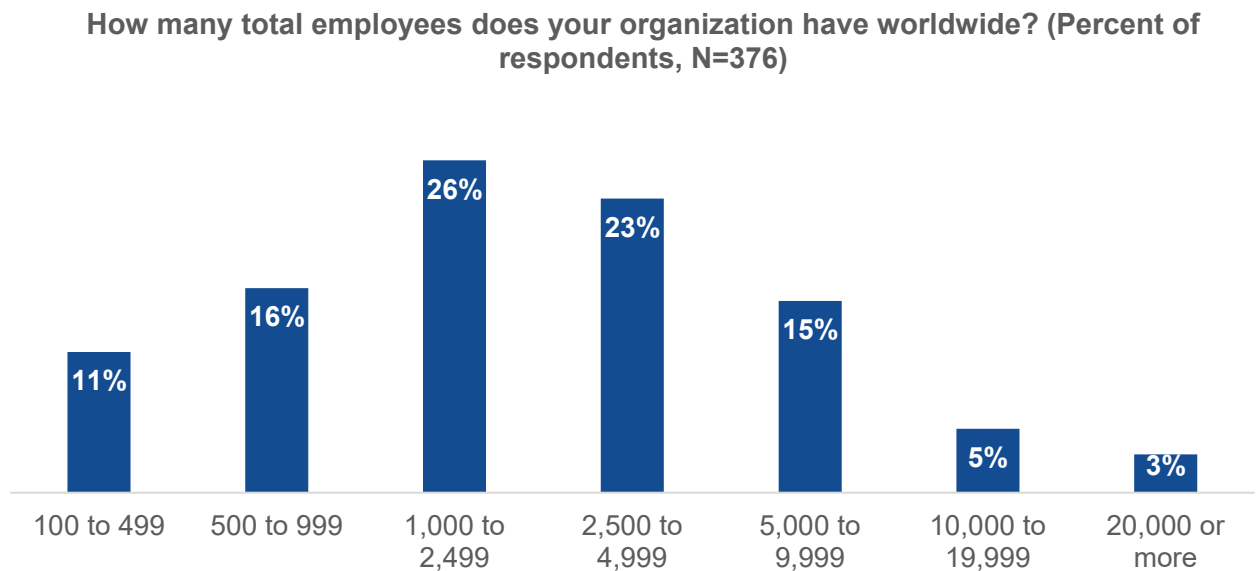
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Figure 27. Respondents by Age of Organization

**For approximately how long has your current employer been in existence?
(Percent of respondents, N=376)**
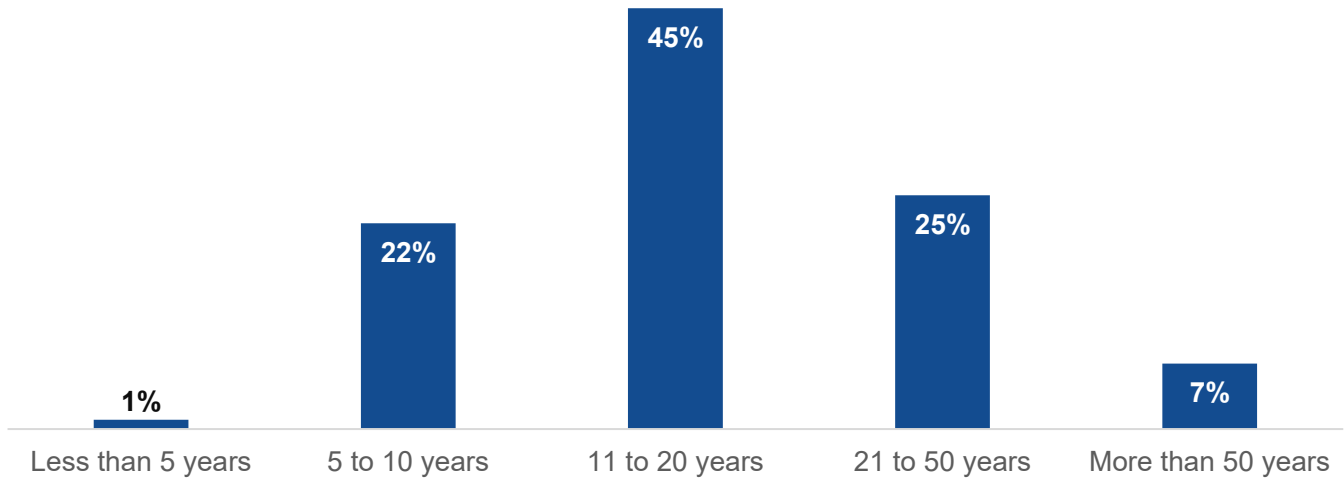
Source: *Enterprise Strategy Group, a division of TechTarget, Inc.*

Respondents were asked to identify their organization's primary industry. In total, Enterprise Strategy Group received completed, qualified responses from individuals in 21 distinct vertical industries, plus an "Other" category. Respondents were then grouped into the broader categories shown in Figure 28.

Figure 28. Respondents by Industry

What is your organization's primary industry? (Percent of respondents, N=376)
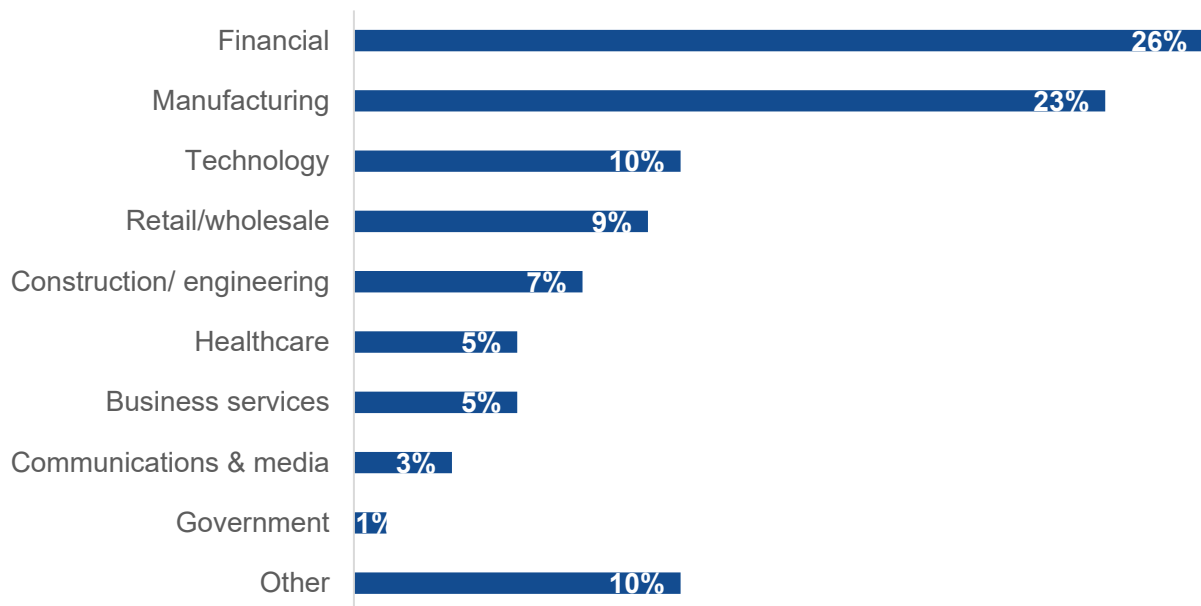
Source: *Enterprise Strategy Group, a division of TechTarget, Inc.*

Figure 29. Respondents by Annual Revenue

25

What is your organization's total annual revenue ($US)? (Percent of respondents, N=376)

| Less than $250 million | $250 million to $999.999 million | $1 billion or more | Not applicable (e.g., public sector, non-profit) |
| 30% | 30% | 40% | 1% |

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

About Enterprise Strategy Group
TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

contact@esg-global.com

www.esg-global.com