INFORMATION WEEK Reports

NOVEMBER 2024

2024 The State of Data Management, Privacy, and Governance

Too much data, too little value. Too many privacy problems, too few privacy professionals. And AI is pushing every data management solution to its limits.

256653_IWK23

SPONSORED BY

DataBee

informatech

Table of Contents

3 DataBee Perspective
6 About the Author
7 Executive Summary
9 Key Findings
10 Research Synopsis
11 Introduction
12 Data Privacy Goes Public
13 Data Pileups and Backups
15 The AI Energy Crisis and Data Sustainability
20 Appendix

Figures

Figure 1 Data Privacy Drivers
Figure 2 Importance of Regulations
Figure 3 Data Privacy Leader
Figure 4 Data Privacy Confidence Statements
Figure 5 Data Volume Being Managed
Figure 6 Data Growth Drivers
Figure 7 Data Backups and Recovery
Figure 8 Tools to Enhance Data Privacy and Governance
Figure 9 Environmental Sustainability in Data Efficiency Efforts
Figure 10 Policies to Address Data Privacy
Figure 11 Data Governance Drivers
Figure 12 Data Privacy Reporting Structure
Figure 13 Data Governance Leader
Figure 14 Data Governance Reporting Structure
Figure 15 Data Management Leader
Figure 16 Data Management Reporting Structure
Figure 17 Structured Versus Unstructured Data
Figure 18 Data Growth
Figure 19 Frequency of Sharing Data
Figure 20 Request for Users' Private Data
Figure 21 Complying with Request For Data
Figure 22 Change in Data Requests
Figure 23 Respondent Job Title
Figure 24 Respondent Company Size
Figure 25 Respondent Industry
Figure 26 Respondent Company Revenue

SPONSORED CONTENT
DataBee Perspective

Data Defense 101: Secure, Govern, and Thrive

A security data fabric enables organizations to maintain consistent security and privacy controls as data volumes continue to increase.

Authors: Erin Hamm, Field Chief Data Officer at DataBee from Comcast Technology Solutions
Amy Heng, Director of Product Marketing at DataBee from Comcast Technology Solutions

From financial forecasting to customer experiences, data analytics is the foundation of the modern business model. The State of Data Management, Privacy, and Governance report only reinforces this reliance on data as 80% of survey respondents reported an increase in data volumes arising from these business initiatives.

Every benefit this data provides also comes with a responsibility to manage it, protect privacy, and govern use and access. To protect data, organizations increasingly adopt more cybersecurity solutions with the enterprise organization often managing over 100 tools. Yet, enterprise and security data have been separated historically, creating data silos that impact the organization's ability to create a global data strategy and gain the full benefit of its security data.

Enter the Security Data Fabric

Data fabric federation is an architecture that centralizes data so that organizations can converge data sources, data sets, and controls from their different sources.

The security data fabric gives organizations a way to gain two distinct benefits:

- Centralizing security data breaks down silos so that teams beyond the information security team can gain visibility and context for about incidents and data-driven business initiatives.
- Deliver high-quality, relevant data products by operationalizing data access, integration, and sharing that enhance an enterprise's existing technology stack.

Organizations historically struggled to include security data within their enterprise data strategies because normalizing the data requires having a data science team that understand the unique cybersecurity, risk, and compliance value and – often proprietary – data schemas. At Comcast, we realized the value of a security data fabric for improving our security analytics while aligning security data to our global data management and governance programs.

Using Data Lineage for Management and Governance

A security data fabric enables cybersecurity and compliance teams to have the data foundation they need to defend and protect the business. For example, with an understanding of data's journey from its source to its destinations in relation to the business, security analysts can quickly contain and respond to threats and compliance analysts can build policies to reduce and mitigate risk.

Data lineage acts as the foundation for the organization's data governance and management strategies by providing visibility into data origin, processing, and storage. Using a security data fabric to understand security data's journey from source to consumption layer enables the organization's global data strategy by:

- Implementing appropriate controls over protected information
- Understanding relationships between data and business for improved precision in analytics and governance
- Maintaining real-time and accurate data for critical decision-making
- Gaining upstream and downstream lineage for the data lifecycle
- Improving data discovery for more accurate analytics and self-service
- Advancing data strategies to align with modern data management objectives

Expanding Security Analytics Use Cases

Breaking down the silos between enterprise and security data also allows organizations to expand their security analytics use cases. Malicious insider threats are both a common security concern and fundamental challenge. The perpetrators use their legitimate access inappropriately. Organizations need to identify the threat actors and malicious insiders quickly - and accurately.

Coordinating a response across physical security, digital security, and human resources teams becomes time-consuming. However, a security data fabric can be configured to converge data from technologies across these functions and provides business organizational context to derive insights from:

- Badge reader logs
- Device logs
- Network logs
- Application logs
- Print logs
- Video camera logs, from building entry and exit
- And, if integrations are available, HR data that adds context including an employee's pending employment termination status

With all functions working with the same chronologically ordered datasets, also known as time-series analytics, the organization can more rapidly respond to the incident and communicate next steps.

Weaving Data into a Fabric of Insights

When the global data strategy is inclusive of security data, the organization optimizes its security and enterprise data's value for analytics while improving its overarching data governance profile. A security data fabric, like DataBee from Comcast Technology Solutions, enables the security team to gain data-driven insights, modernizing the function in alignment with the rest of the organization. Meanwhile, it allows the organization to apply the same data protection controls to security data as it applies to protected data, like personally identifiable information (PII) or cardholder data.

Author

Pam Baker
Contributing Writer

A prolific writer and analyst, Pam Baker's published work appears in many leading publications. She's also the author of several books, the most recent of which are "Decision Intelligence for Dummies" and "ChatGPT For Dummies." Baker is also a popular speaker at technology conferences and a member of the National Press Club, Society of Professional Journalists, and the Internet Press Guild.

Executive Summary

For executives who find anything to do with data to be mind-numbingly boring, this survey packs some eye-popping surprises. Suddenly, it seems, the corporate world put on its collective do-gooder shoes and danced its way to full accountability. “Data ethics/corporate responsibility” ranked as high as 4th (34%) out of 20 options on the “data governance drivers” question.

“Until there is accountability for AI gone bad or for breaches on insufficiently protected data being stolen, this is a blip on the radar rather than a sustained shift. DOJ, FTC, and HHS are trying to establish accountability, but there’s so much that they don’t have the proper resources,” said Michele Thomas, Co-Founder and CISO of TrustedTec, referring to the United States Department of Justice, Federal Trade Commission and Department of Health and Human Services.

But not all respondents believe that organizations will bail on data ethics and corporate responsibility in data management if given the chance to do so. Some believe that the challenges are so great that progress is just slowed, more so than resisted.

“I hold the view that data privacy is no longer just a buzzword; it’s a serious business concern,” said Brian Teater, a survey participant and the IT Manager at EXP. “While there’s increased awareness of its importance, many organizations are still struggling to translate this understanding into concrete actions, let alone achieve actionable outcomes in today’s fast-paced business environment. The complexities of data privacy regulations, the technical challenges of securing massive datasets, and the cultural shift needed to prioritize data protection are all significant hurdles to overcome.”

Even so, it’s highly likely that fear of punishment will power accountability more than peer or social pressures to do the right thing. Data privacy regulation--once again the top driver of data governance, named by 60% of respondents this year--is much more likely to force organizations to get a better grip on their data stores.

“Most organizations do not manage their data properly,” said Thomas. “They don’t even know where all their data is or how much duplicate data exists. They also do not protect data to the access level, much less with context, meaning under what circumstances who can do what to data when.”

PREVIOUS NEXT

Another big surprise is the flip in AI's impact on data management. If you think of your data stores as the brains in AI and the model as the nervous system, then it's easy to see how a brain-impaired model would fail more often than succeed. No matter how great and responsive the AI model is, if it can only operate with insufficient, incorrect, or outdated data, it cannot perform to expectations.

This brain-to-nerves, aka data-to-model, analogy explains in part why nearly one-third (31%) of respondents cite an increased use of AI on the technical side as a driver for data growth in their organization. On the project side, nearly half (42%) report an upswing in data-driven and analytics-driven business projects require more data.

Another eye-popping revelation is that despite the huge risks in failing to comply with data privacy laws worldwide, there's a real lack of dedicated leadership at most organizations. Only 8% said that a CPO is leading privacy initiatives, but for most it's a corporate leader or an IT leader--and not even an executive IT leader. There are more IT managers [12%] leading privacy than there are [8%] CPOs.

Oddly, while there's little to no consensus on how to manage data privacy, there is agreement on the importance of data sustainability driven in large part by the upswing in AI adoption.

"Companies are realizing that storing and processing data, especially with AI, can use a lot of energy. So, it's great to see them focusing on building more energy-efficient data centers and exploring greener and more sustainable ways to store data," said Teater.

An overwhelming 92% of respondents acknowledge at least that sustainability should be a factor and of that group, 39% said that it's already an essential part of their data management practice.

Key Findings:

- 16% of respondents are managing more than 10PB of data. This is a jump from 9% in last year's survey.
- Over one-third of respondents said the amount of data they manage has increased by 25% or more in the past year.
- 31% of respondents cited an increased use of AI as a driver for data growth in their organization.
- 60% of respondents said "privacy regulation" was a top driver for data governance programs, coming in as the No. 1 response.
- 34% of respondents said "data ethics/corporate responsibility" was a top driver for data governance programs.
- Only 8% of respondents said the chief privacy officer is leading their data privacy efforts.
- 92% said environmental sustainability is playing or should play a role in data management practices.
- Two out of three respondents (67%) are confident that their organization is compliant with all necessary privacy regulations.
- Yet only half of respondents (51%) are confident in their organization's ability to pay a fine and withstand sanctions if they violate a privacy regulation.
- 36% reported that a data privacy assessment is now a part of their technology acquisition process.

Research Synopsis

Survey Name: The 2024 InformationWeek State of Data Management, Privacy, and Governance Survey

Survey Date: August 2024

Primary Region: North America, with some worldwide representation

Number of Respondents: 152 IT executives, management, and cybersecurity professionals who are involved in the administration, storage, management, or governance of data or the management, planning, or enforcement of data privacy or data governance for their organizations. The margin of error for the total respondent base (N=152) is +/- 7.9 percentage points.

Methodology: InformationWeek surveyed IT and cybersecurity executives, directors, managers, and staff. Respondents were screened to qualify for the survey as working on data governance or data privacy projects or leading data governance or data privacy efforts. The survey questions asked about asked about data management, governance, and privacy at a representative sample of organizations. The survey was conducted online. Respondents were invited to participate via email invitations containing an embedded link to the survey. The emails were sent to a select group of Informa Tech's qualified database; Informa is the parent company of InformationWeek. Informa Tech research was responsible for all aspects of survey design, administration, data collection, and data analysis. These procedures were carried out in strict accordance with standard market research practices and existing US privacy laws.

Introduction

Data is the brains behind every organization. It is the driver of decisions, processes, and profits. Yet, this most valuable of all assets is commonly treated as if it were the cheapest of commodities. Perhaps that perception stems from the fact that data is quite literally everywhere and it's piling up higher and higher every day. In last year's report, 9% of those we surveyed said that they were managing over 10PB of data. This year, the InformationWeek Data Management, Governance and Privacy survey found that number almost doubled, jumping to 16%. But what accounts for that soaring growth of data under management?

"I'm convinced that it's a combination of both data hoarding and new data growth. While organizations are generating more data than ever before, there's also a tendency to retain data for longer periods, often without a clear purpose. This can lead to data clutter and increased storage costs," said Brian Teater, a survey participant and the IT Manager at EXP.

In the survey, 42% of respondents cited "data-driven analytics projects" as the primary driver behind their data growth while 31% blamed "more use of AI."

But some of the data growth can be attributed to more human-based reasons like turf protection, said one respondent. "In organizations who do not have shared, enterprise data platforms there is a lot of duplicate data because each internal organization keeps their own and won't share it," said Michele Thomas, co-founder and CISO of TrustedTec.

Even so, there's obviously some data sharing going on. According to the survey, nearly half of respondents (48%) reported sharing data daily, and 22% said they share data weekly.

Whether newly created, newly acquired, duplicated, siloed, or captured in corporate politics, data growth shows no signs of slowing. According to Statista, the "volume of data/information created, captured, copied, and consumed worldwide" will jump from 120 zettabytes in 2023 to 147 zettabytes in 2024 and soar to 181 zettabytes in 2025. A zettabyte is equal to a billion terabytes.

How can something so ubiquitous have such a high value? The reasons are almost as infinite as the number of bytes that are collected and stored every day. Even so, cashing in on that value remains frustratingly elusive for many companies.

"It's like the person who tries to eat the whole elephant in one bite, chokes, and then wonders why things failed. Working on a [data] governance plan will help organizations to identify where their data is, what is it, what it's used for, what can be shared, what cannot be shared, what metadata is necessary to keep and share, how much data is duplicated, where the data is stored, where data should be stored, and who can access, change, delete the data," said Thomas.

The No. 1 factor driving data govern -ance initiatives? Privacy regulations, cited by 60% of respondents. Over one-quarter of respondents also said that compliance with non-privacy regulations was a leading driver.

Maybe then it's appropriate that data governance initiatives are most often led by chief compliance officers (13%). chief data officers (8%) and chief data governance officers (7%) do rank high on the list as well.

However, privacy pros hardly make the list--not even when it comes to running data privacy. More on this to come.

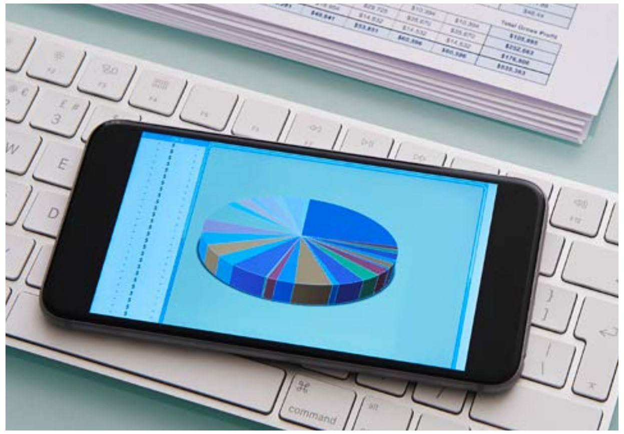
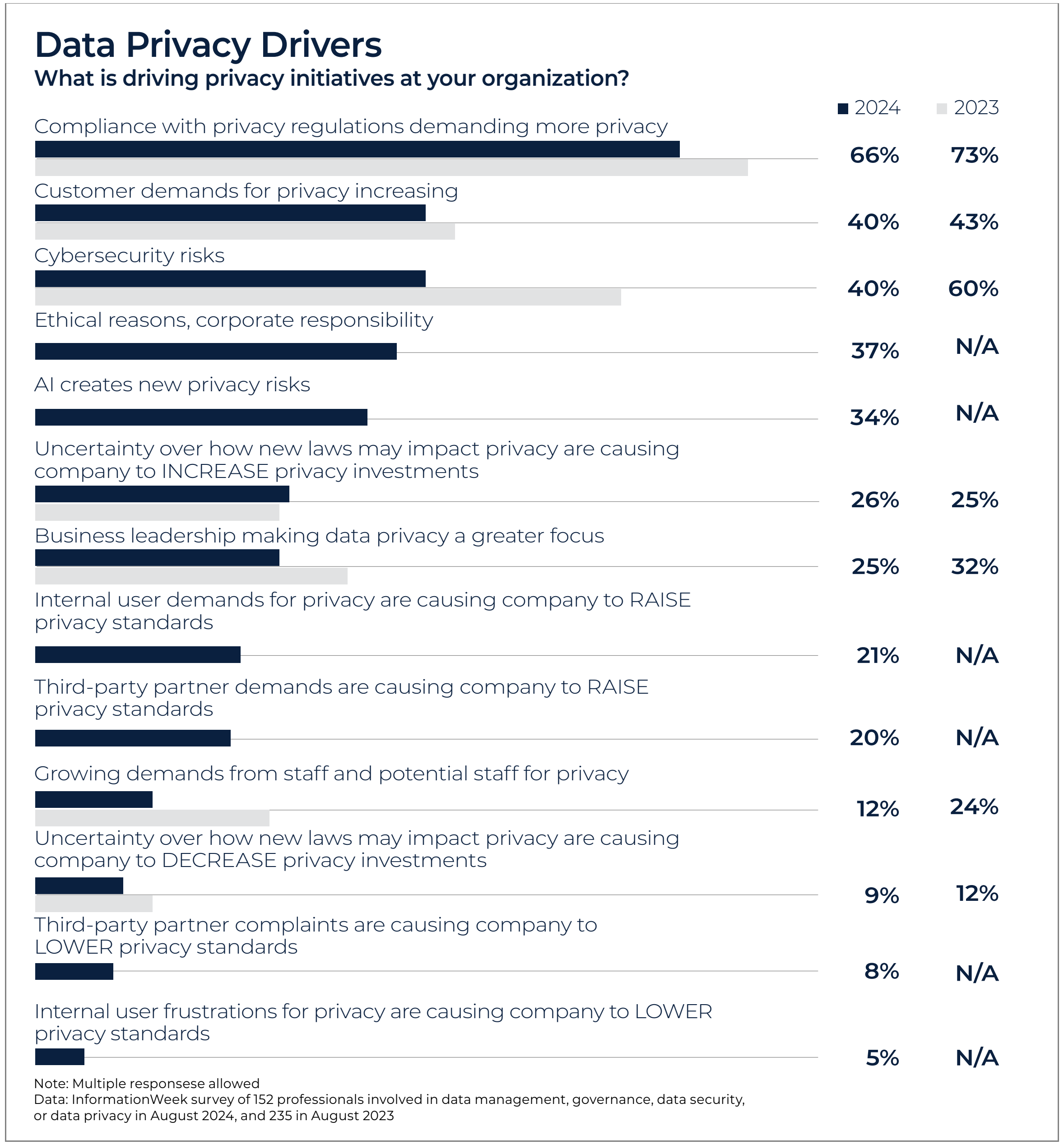


Figure 1



Data Privacy Drivers

What is driving privacy initiatives at your organization?

Note: Multiple responsese allowed
Data: InformationWeek survey of 152 professionals involved in data management, governance, data security, or data privacy in August 2024, and 235 in August 2023

Data Privacy Goes Public

There's no doubt that privacy is a huge issue in the public's eye.

As with governance, the No. 1 driver of data privacy initiatives is compliance with data privacy regulations, named by two out of three (66%) respondents **(Figure 1)**. The wide variety of regulations that respondents must comply with is staggering in terms of compliance requirements, complexities, conflicts between jurisdictions, and perils and penalties. Further, the uncertainty they're experiencing because of the possibility of even more such laws is causing changes in spending: 26% said they've increased privacy spending, while 9% said they decreased it.

The US Health Information Portability and Accountability Act (HIPAA) is by far the most important to our survey respondents, named as important or essential by 65% **(Figure 2)**. But about one-third of respondents said they must comply with everything on a list of 19 regulatory requirements. The list included state, federal, and international privacy laws (from India, the UAE, Brazil, China, and others). And in addition to privacy legislation, it included industry-specific regulations, like on financial data.

"With all the new data privacy rules like GDPR and CCPA popping up, it's like trying to hit a moving target. It's definitely challenging, but it also opens up new opportunities for businesses to do things better," said Teater. (He refers to the European Union's landmark General Data Protection Regulation and to California's trend-setting state legislation, the California Consumer Privacy Act.)

Regulation is by far the leading driver (66%), but the other top five on a list of are customer demands for privacy are increasing (40%), cybersecurity risks (40%), ethical reasons/corporate responsibility (37%) and AI creates new data privacy risks (37%). Some respondents also indicated that they are changing their privacy investments--some increasing spend, others decreasing it--in order to address users' or third parties' complaints *(see Figure 1)*.

Despite this quagmire of perils and penalties, the lack of fixed leadership to oversee data privacy is haphazard.

Only 8% said that a chief privacy officer is leading privacy initiatives **(Figure 3)**. For most it's a corporate leader or an IT leader--and not even an executive IT leader. There are more IT managers (12%) leading privacy than there are CPOs.

Balancing data privacy versus the corporate demands for data collection continue to be a challenge. Only 38% said it was relatively easy **(Figure 4)**. Curtailing the types and amount of data collected is one way to make these efforts more manageable.

"Organizations and their leadership should stop thinking about grabbing all the data they can, and instead look at the business use case, the value of the data use, and the investment required to do what's proposed," said Thomas.

Nixing personal data in particular is gaining traction as a prime way to mitigate some of the risks in data privacy laws.

"My organization is currently taking steps to reduce the amount of personal data we collect. We're conducting regular audits of our data collection practices to identify areas where we can minimize the data we collect and retain. We're also implementing data minimization principles to ensure that we only collect the data necessary to achieve our business objectives," said Teater.

Data Pileups and Backups

Data is quite literally everywhere and piling up higher and higher every day. Last year 9% of those surveyed said that they were managing over 10PB of data. This year the survey found that number almost doubled, jumping to 16% **(Figure 5)**. More than four in 10 (42%) of respondents cited data-driven analytics projects as the primary driver behind their data growth, while 31% blamed more use of AI **(Figure 6)**.

"Organizations are actively seeking to obtain more data to feed AI projects. While AI can certainly reuse existing data, the quality and quantity of data can significantly impact the accuracy and effectiveness of AI models. My organization as well as many other companies are investing in data acquisition strategies to ensure they have the nec-

Figure 2

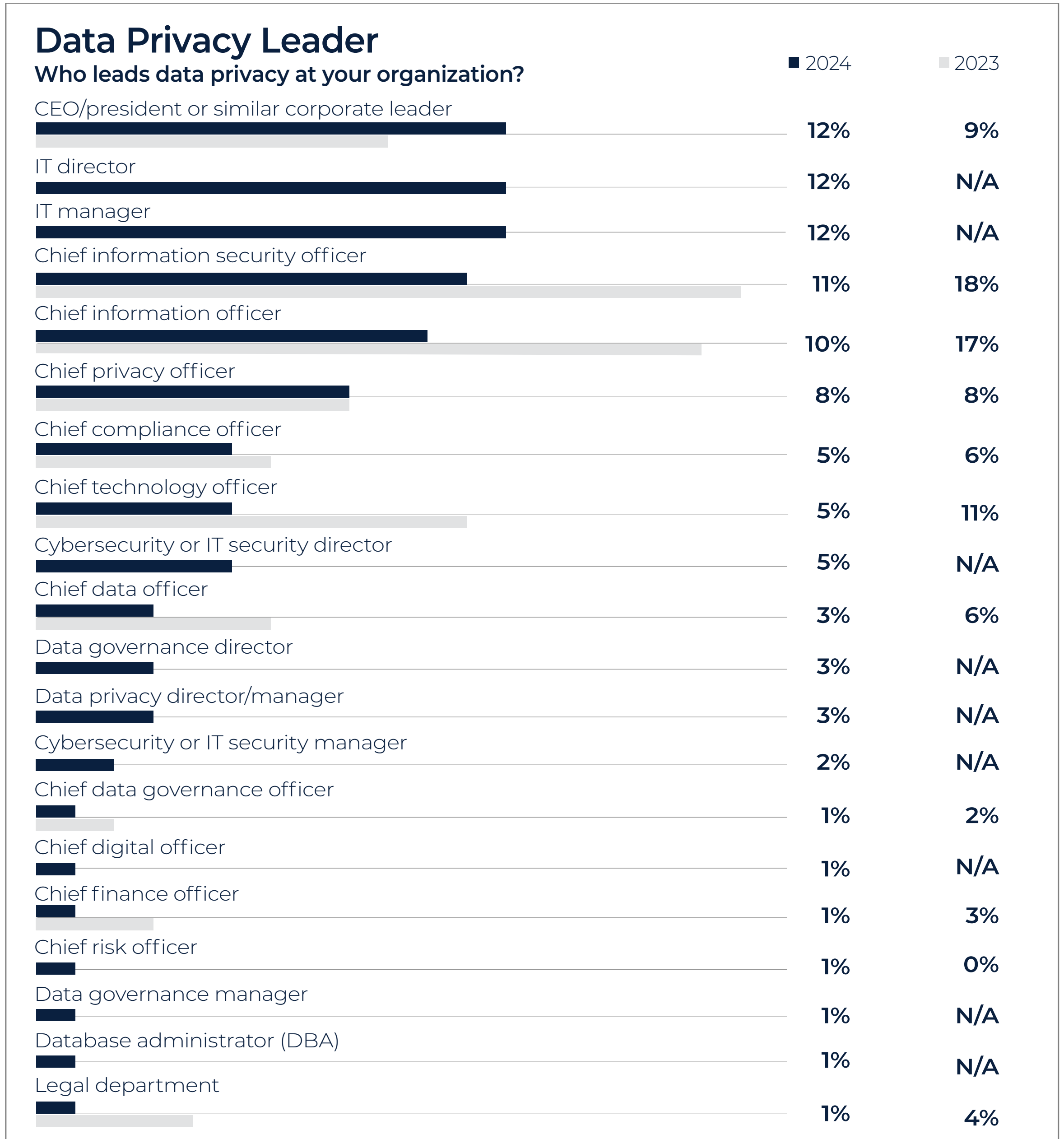
Importance of Regulations

Please rate the importance of these regulations to your business.

	1 Rarely comes up	2	3	4	5 Compliance is essential	Not sure
HIPAA (U.S. Health Insurance Portability and Accountability Act	18%	5%	7%	11%	54%	5%
PCI-DSS (Payment Card Industry Data Security Standard)	16%	7%	11%	11%	44%	11%
(SOX) Sarbanes-Oxley	17%	7%	8%	15%	42%	11%
GDPR (E.U. General Data Protection Regulation)	20%	8%	12%	13%	41%	6%
CCPA (California Consumer Privacy Act)	18%	5%	11%	16%	37%	13%
Other U.S. state-specific privacy legislation	18%	8%	13%	13%	37%	11%
FISMA (Federal Information Security Management Act)	16%	7%	9%	21%	36%	11%
COPPA (Children's Online Privacy Protection Act)	24%	9%	8%	13%	36%	10%
NYDFS Cybersecurity Regulation (23 NYCRR 50)	20%	6%	9%	18%	30%	17%
UK: Privacy and Electronic Communications Regulation	34%	9%	7%	8%	28%	14%
(GLBA) Gramm Leach Bliley Act	20%	9%	6%	17%	27%	21%
Trans-Atlantic data transfer rules (EU-U.S. Data Privacy Framework)	33%	7%	8%	11%	26%	15%
UK: Data Protection Act	34%	9%	8%	12%	25%	12%
Canada: PIPEDA (Personal Information and Protection and Electronic Documents Act)	39%	3%	8%	12%	24%	14%
UAE: Protection of Personal Data Law	38%	8%	5%	8%	24%	17%
India: DPDPA (Digital Personal Data Protection Act, 2023)	40%	6%	5%	10%	22%	17%
Australia: Privacy Act	41%	5%	5%	12%	21%	16%
Brazil: LGPD (Lei Geral de Proteção de Dados Pessoais)	42%	3%	5%	9%	21%	20%
China: PIPL (Personal Information Protection Law)	41%	5%	7%	13%	17%	17%

Data: InformationWeek survey of 152 professionals involved in data management, governance, data security, or data privacy, August 2024

Figure 3



Data Privacy Leader

Who leads data privacy at your organization?

Data: InformationWeek survey of 152 professionals involved in data management, governance, data security, or data privacy in August 2024, and 235 in August 2023

essary resources to drive their AI initiatives," said Teater.

Data pileups and increased AI use are also driving data sustainability initiatives, with a few exceptions.

"The impact is in what it takes to store data and how to get to it. AI and quantum computing have both demonstrated that there is a lot behind the curtain and decisions should be made realistically and cautiously. Sustainability is a good thing. Understanding what you really need can help determine if sustainability is a decision point or not," said Thomas.

Besides the costs and risks in storing a lot of data are similar issues in managing this data, backing it up, securing it, and retrieving such large quantities on demand, particularly in an emergency.

Cloud (63%) and disk backups (47%) are the leading tools applied in storing and recovering backups, followed by data encryption (39%), data loss prevention (30%), and tape backups (28%). Note: We did not specify a difference between tape and tape-as-a-service, but we will do so in future surveys **(Figure 7)**.

Respondents cited a wide variety of tools for managing data privacy as well. The top three were no surprises: encryption (72%), VPNs (60%), and identity and access management (46%). However, other fundamental tools made the list, like records management (27%), as did some specialized or emerging technologies, including identity security platforms (20%) and synthetic data (13%) **(Figure 8)**.

"People usually think of data as separate from cybersecurity. To me they are so close as to almost be directly related. People talk about breaches--a cybersecurity thing, right?--but do you really realize that most breaches aren't for the hell of it. No, they are to get to the data and steal it. That's data privacy and data protection. In the public sector where I've worked, data protection was a cybersecurity partnership," said Thomas.

The AI Energy Crisis and Data Sustainability

When it comes to sustainability, an overwhelming 92% of respondents acknowledged at least that sustainability should be a factor, and of those people, 39% said that it's already an essential part of their data management practice **(Figure 9)**. While the data center industry has been working on sustainability improvements for some time, it's the sudden and soaring adoption of generative AI that is causing the IT industry to redouble efforts.

Recently, Sam Altman, CEO of OpenAI, which makes the now famous ChatGPT chatbot, admitted at the World Economic Forum's annual meeting that AI is headed for an energy crisis. Considering that all forms of AI, including generative AI, are data-dependent for their performance, it's imperative to consider the environmental costs of storing the huge data hordes that an army of AI models will need. Hence the renewed drive to make data management, storage, and governance more sustainable too. Even so and somewhat shockingly, only one-quarter (25%) of respondents reported using data governance management platforms *(previously cited in Figure 8)*, and only 39% reported revisiting or revamping their data retention policies **(Figure 10)**.

"Most organizations do not employ data governance. It's not lip service as much as not understanding what their data posture is or what their data infrastructure looks like. Until they do, they can't protect it sufficiently, much less use it for AI," said Thomas.

How we think about and use AI and data requires a rethink. It's either that or watch one AI project after another run out of gas.

"Many organizations don't use [data] governance to help determine if they need a large language model or a small one. So most just opt for large; they have more than they need and spend a lot of money on storage space. This can also slow processing down with the more data to look at. Using a governance model can help identify data ownership, use, how it's managed, and whether the business use case warrants a large or small data set," said Thomas.

The energy drain from data centers is no joke. According to The International Energy Agency (IEA) report, "after globally consuming an estimated 460 terawatt-hours (TWh) in 2022, data centers' total electricity consumption could reach more than 1,000 TWh in 2026. This demand is roughly equivalent to the electricity consumption of Japan."

Figure 4

Data Privacy Confidence Statements

Please tell us how much you agree or disagree with the following statements.

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
I am confident in my company's ability to respond to a court's e-discovery demand	3%	6%	25%	44%	22%
Improvements in data quality have increased the value of data and helped us reach business goals	5%	5%	24%	46%	20%
I am confident in my company's ability to fulfill individuals' lawful privacy requests	3%	9%	22%	47%	19%
My organization is valuing my skills more and more	6%	7%	27%	45%	15%
I am confident that my organization is compliant with all necessary privacy regulations	2%	9%	22%	54%	13%
My public-facing websites do an adequate job of letting users manage their personal data and privacy rights	3%	11%	26%	47%	13%
Improvements in data privacy have helped us reach business financial goals	6%	11%	34%	38%	11%
My developers apply the "privacy by design" principle	5%	11%	34%	40%	10%
My company is using data storage resources efficiently	3%	15%	22%	51%	9%
I am confident in my organization's ability to pay a fine and withstand sanctions if we violate a privacy regulation	7%	11%	31%	42%	9%
My organization's data practices are rarely impacted by socio-political events	5%	23%	27%	36%	9%
It's easy to balance data privacy and business demands for data collection	7%	30%	25%	29%	9%
My company has a solid plan for handling a major increase in the amount of data	5%	13%	24%	50%	8%

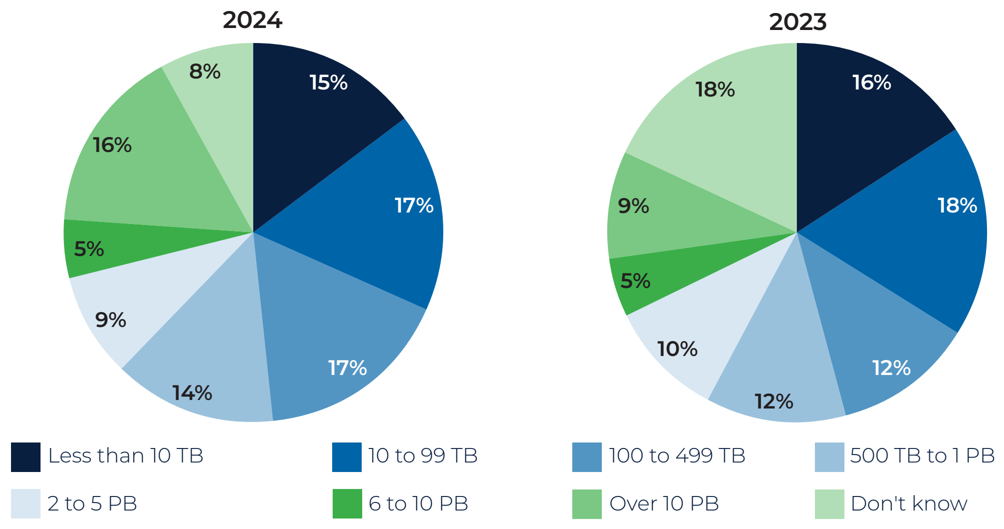
Data: InformationWeek survey of 152 professionals involved in data management, governance, data security, or data privacy, August 2024

Appendix

Figure 5

Data Volume Being Managed

What is the total amount of data being managed by your organization?

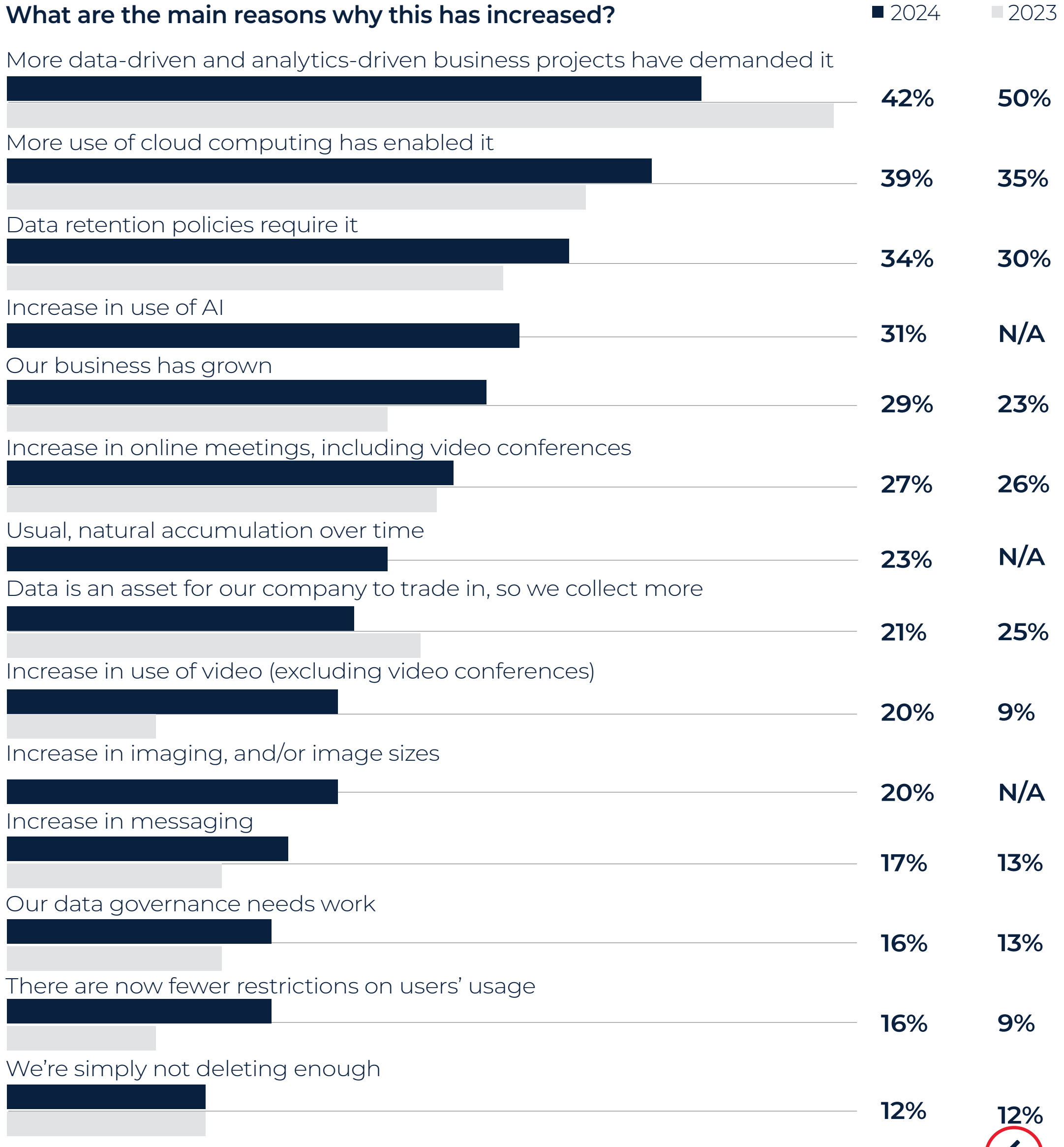


Data: InformationWeek survey of 152 professionals involved in data management, governance, data security, or data privacy in August 2024, and 235 in August 2023

Figure 6

Data Growth Drivers

What are the main reasons why this has increased?



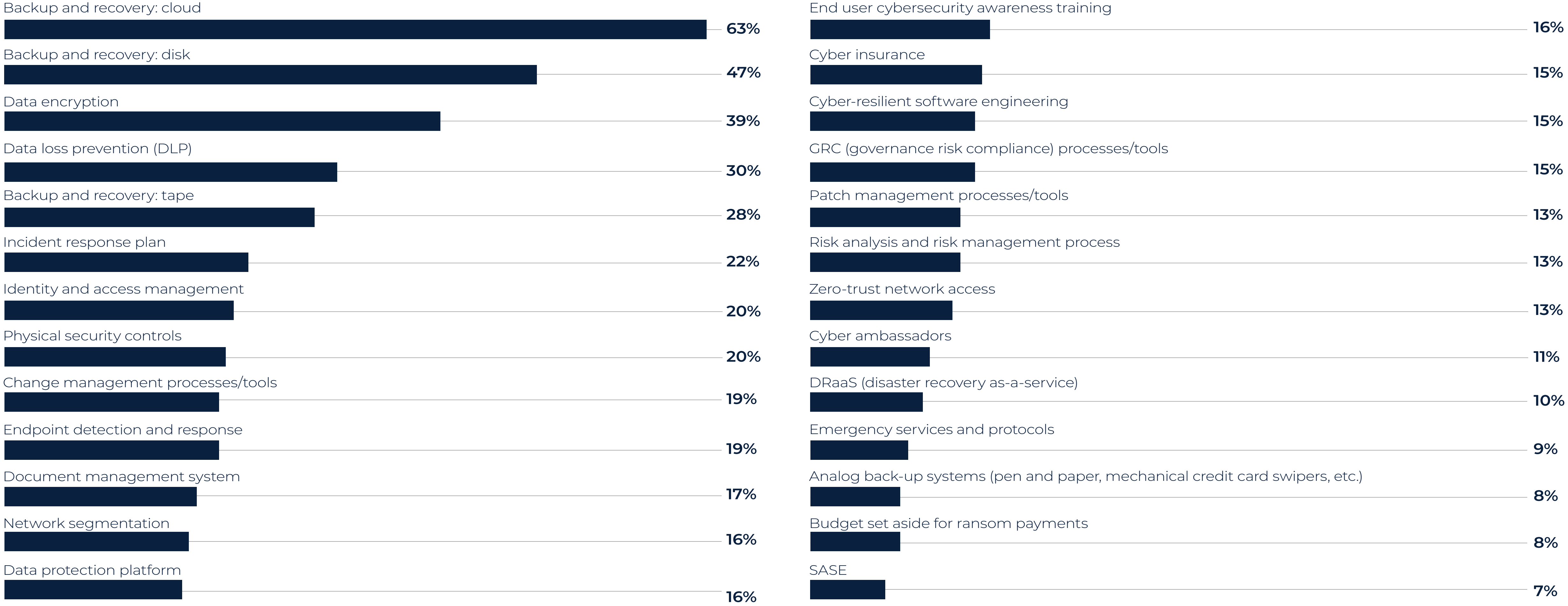
Base: 122 and 176 respondents who reported an increase in the amount of data managed. Note: Maximum of five responses allowed
Data: InformationWeek survey of 152 professionals involved in data management, governance, data security, or data privacy in August 2024, and 235 in August 2023

PREVIOUS NEXT

Figure 7

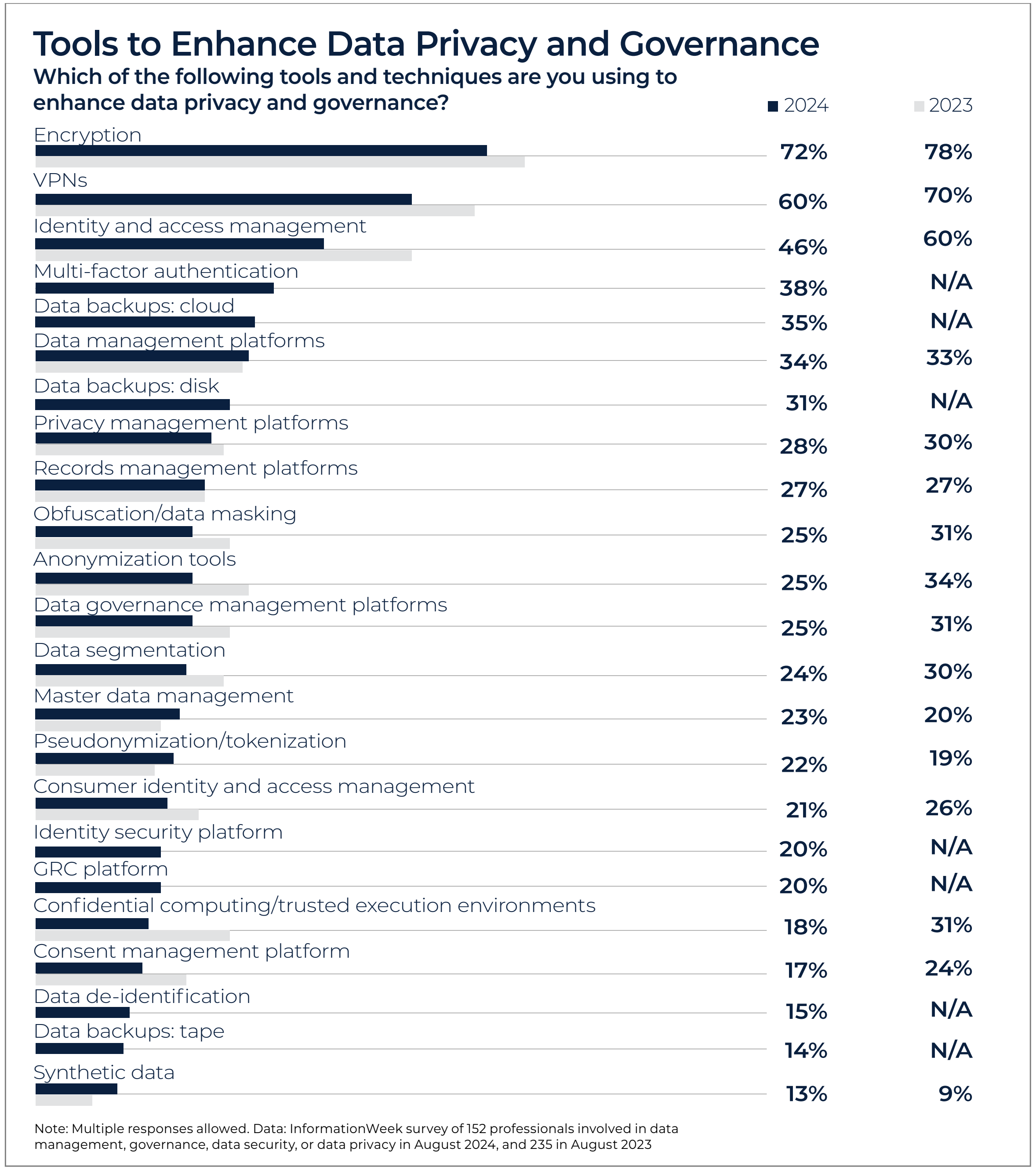
Data Backups and Recovery

How do you handle data backups and recovery in your current system?



Note: Multiple responses allowed
Data: InformationWeek survey of 152 professionals involved in data management, governance, data security, or data privacy, August 2024

Figure 8

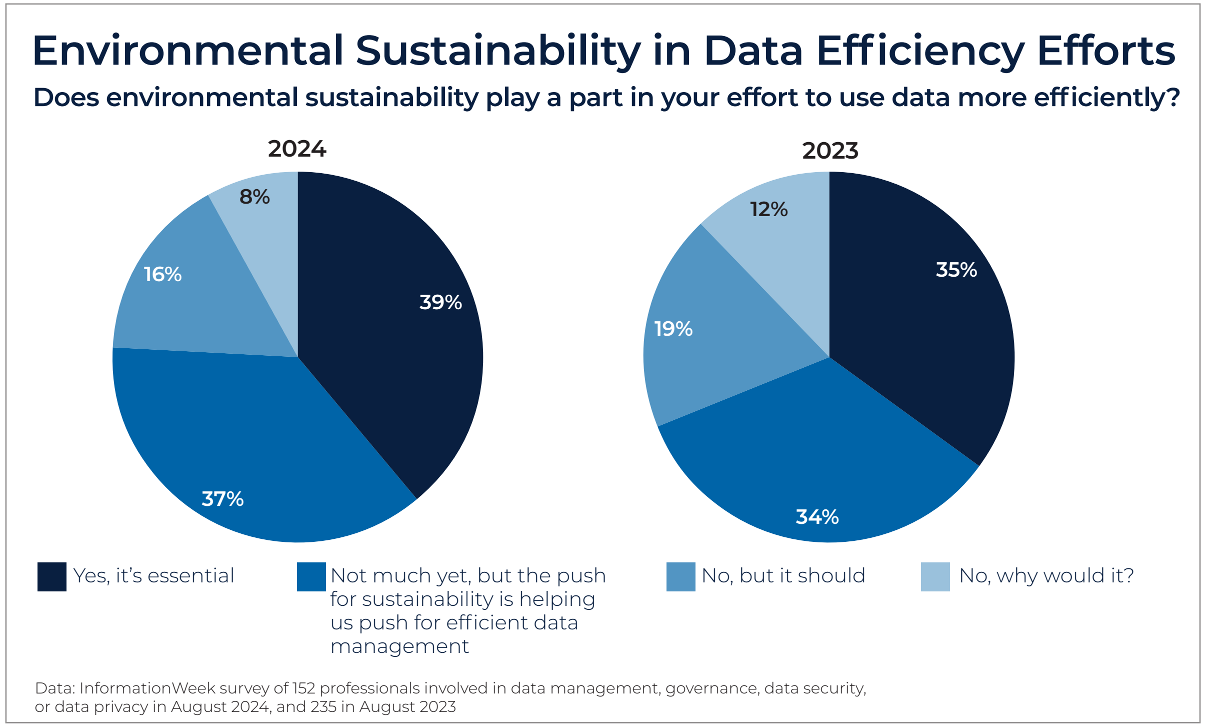


Tools to Enhance Data Privacy and Governance

Which of the following tools and techniques are you using to enhance data privacy and governance?

Note: Multiple responses allowed. Data: InformationWeek survey of 152 professionals involved in data management, governance, data security, or data privacy in August 2024, and 235 in August 2023

Figure 9



Environmental Sustainability in Data Efficiency Efforts

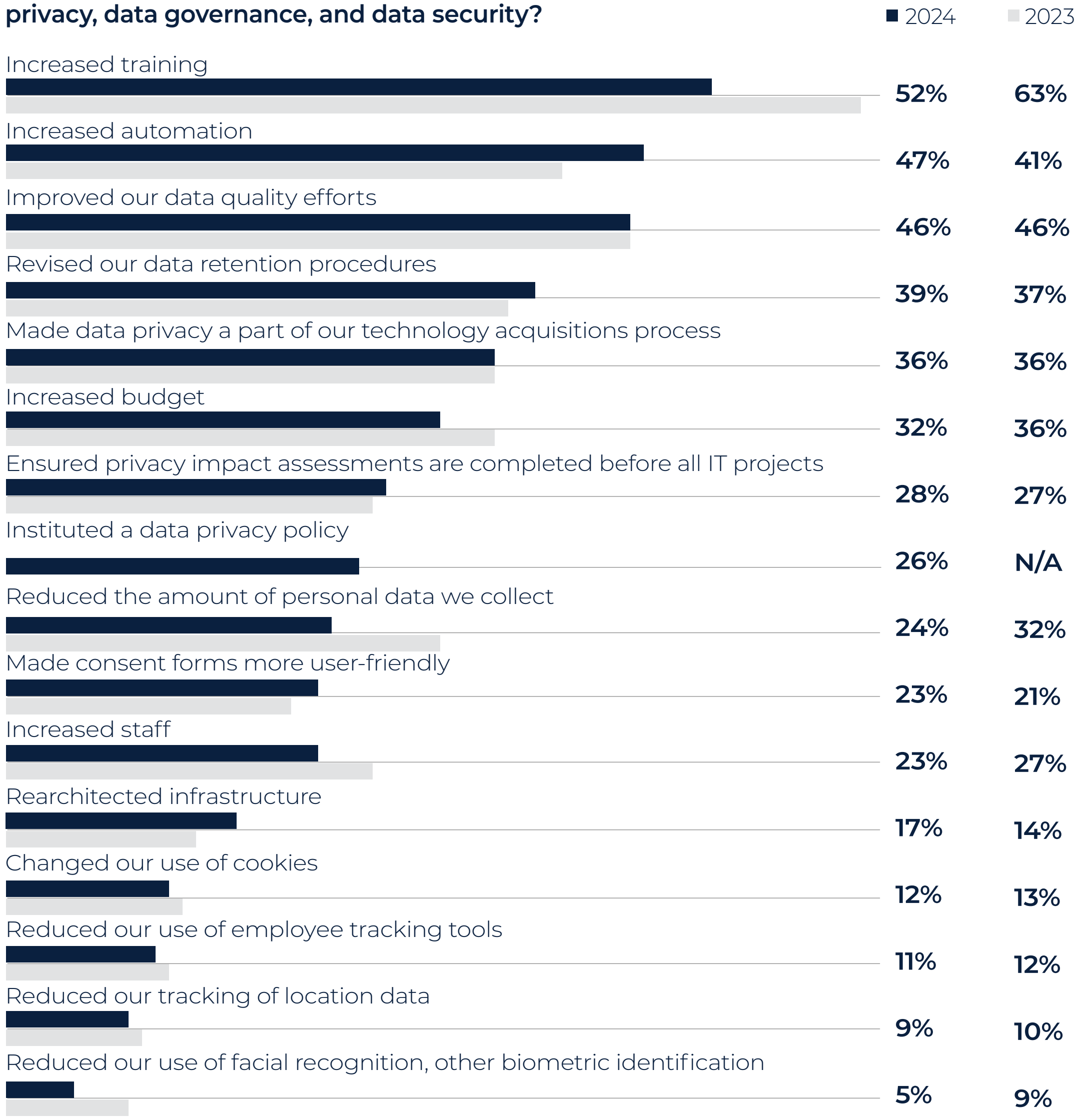
Does environmental sustainability play a part in your effort to use data more efficiently?

Data: InformationWeek survey of 152 professionals involved in data management, governance, data security, or data privacy in August 2024, and 235 in August 2023

Figure 10

Policies to Address Data Privacy

What policies and procedures have you taken to address data privacy, data governance, and data security?



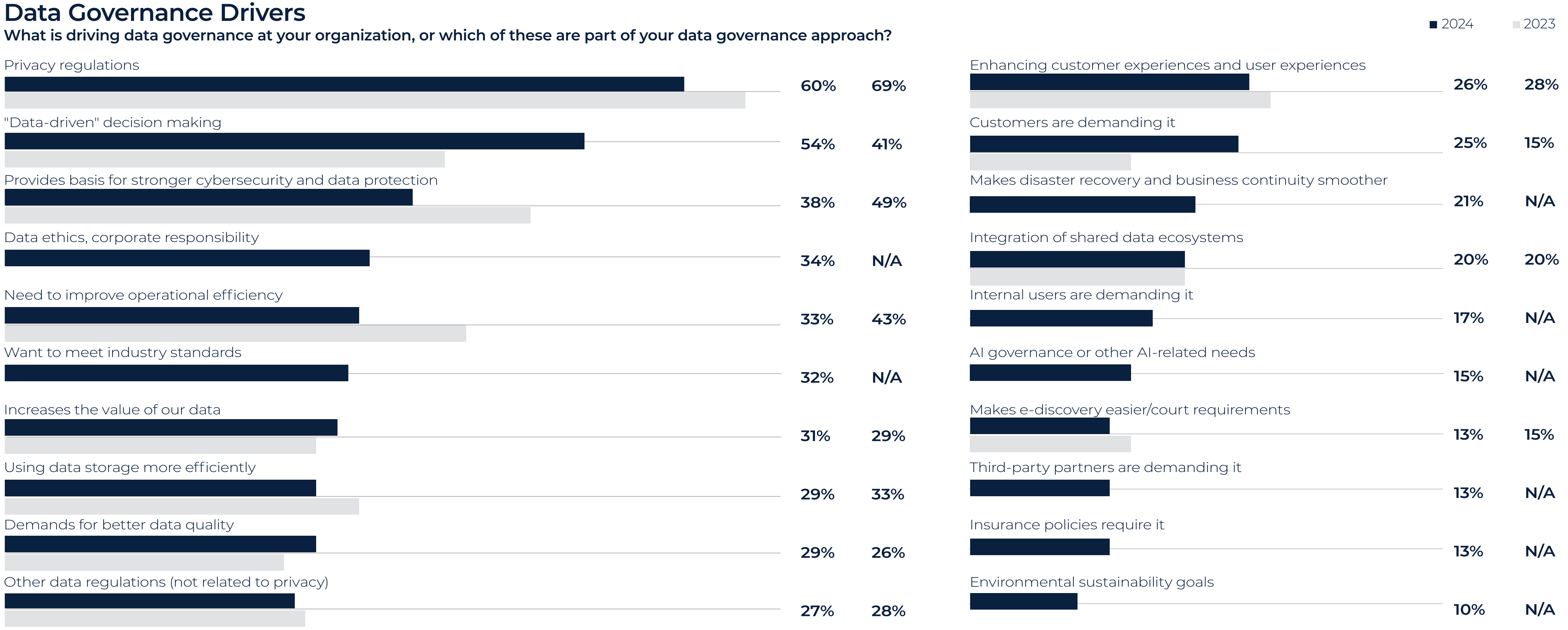
Note: Multiple responses allowed
Data: InformationWeek survey of 152 professionals involved in data management, governance, data security, or data privacy in August 2024, and 235 in August 2023

PREVIOUS NEXT

Figure 11

Data Governance Drivers

What is driving data governance at your organization, or which of these are part of your data governance approach?



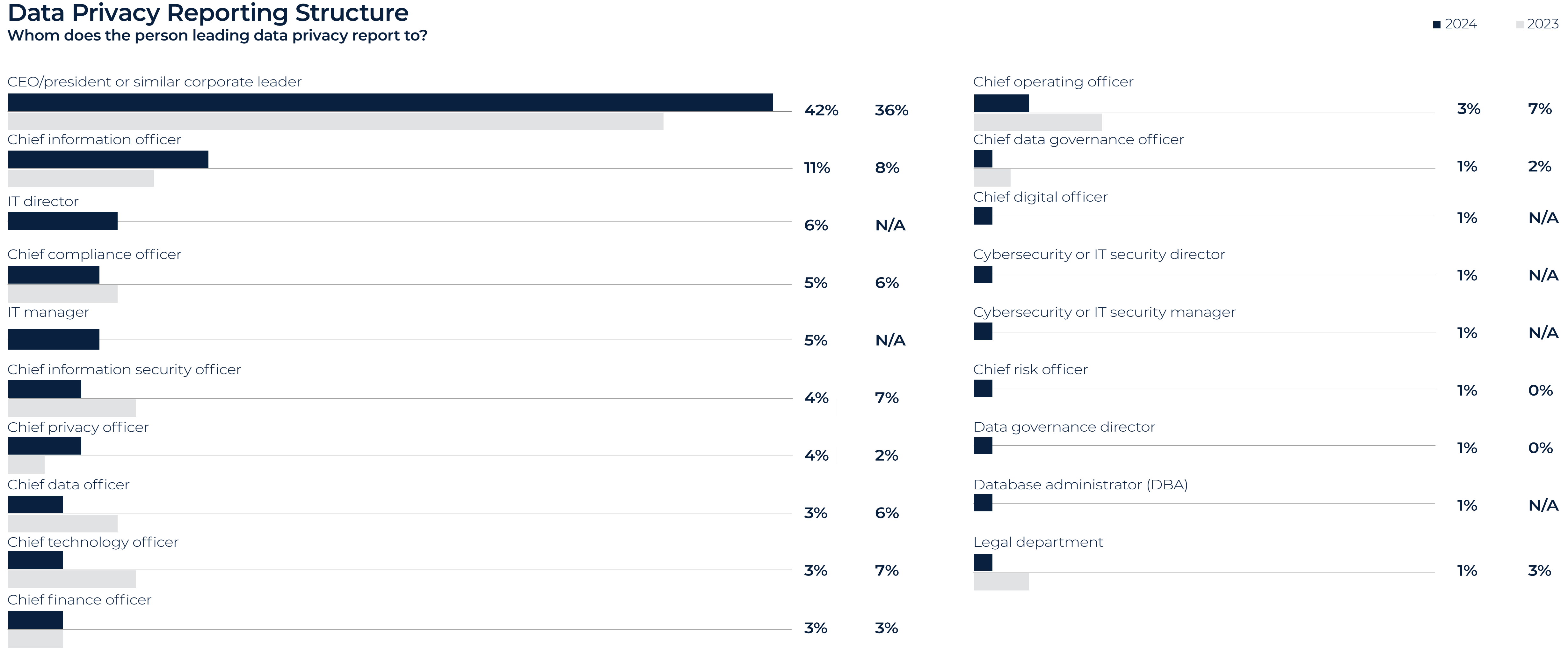
Data: InformationWeek survey of 152 professionals involved in data management, governance, data security, or data privacy in August 2024, and 235 in August 2023

PREVIOUS NEXT

Figure 12

Data Privacy Reporting Structure

Whom does the person leading data privacy report to?

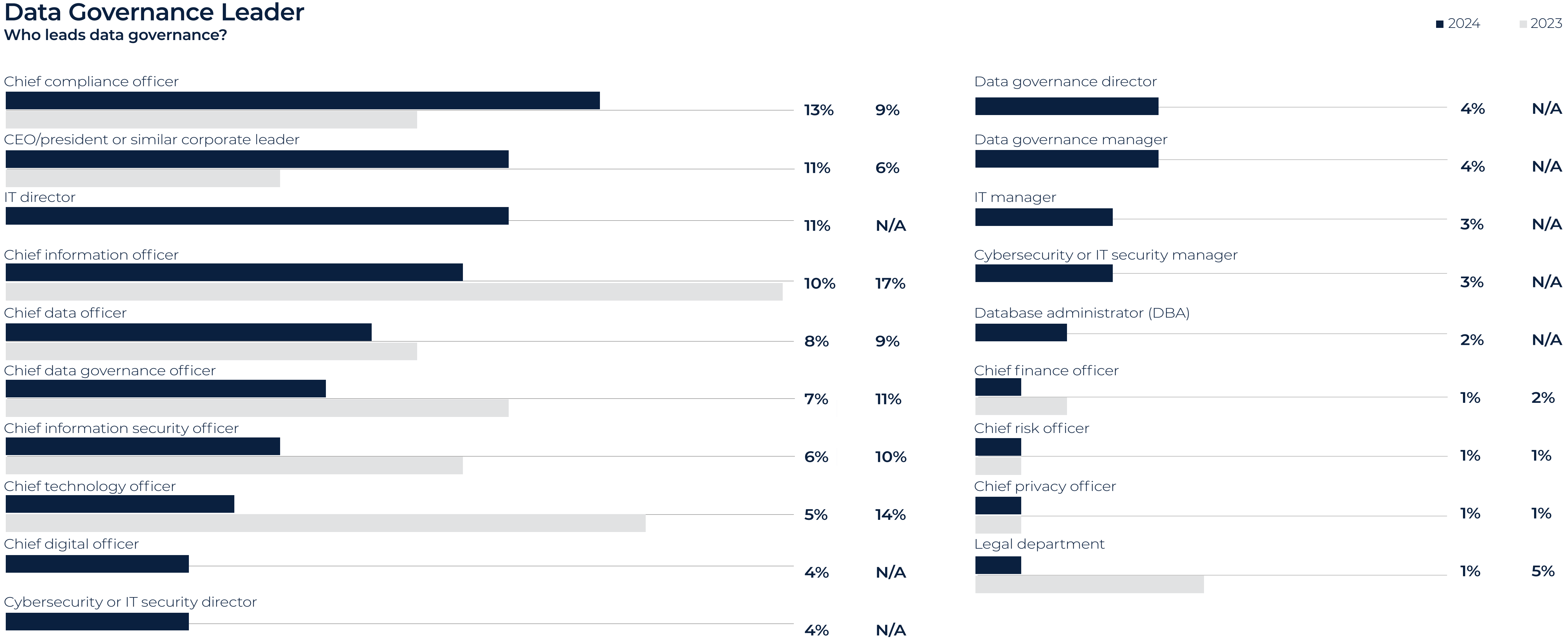


Data: InformationWeek survey of 152 professionals involved in data management, governance, data security, or data privacy in August 2024, and 235 in August 2023

Figure 13

Data Governance Leader

Who leads data governance?

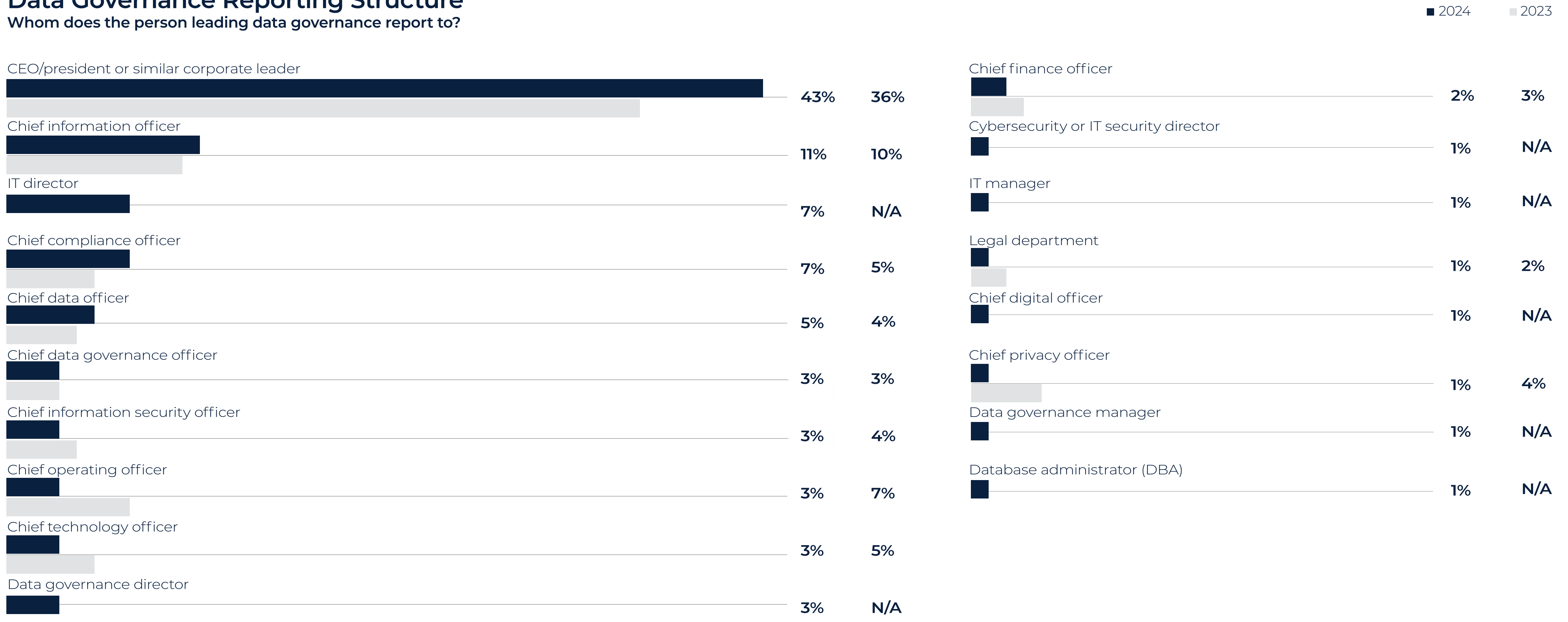


Data: InformationWeek survey of 152 professionals involved in data management, governance, data security, or data privacy in August 2024, and 235 in August 2023

Figure 14

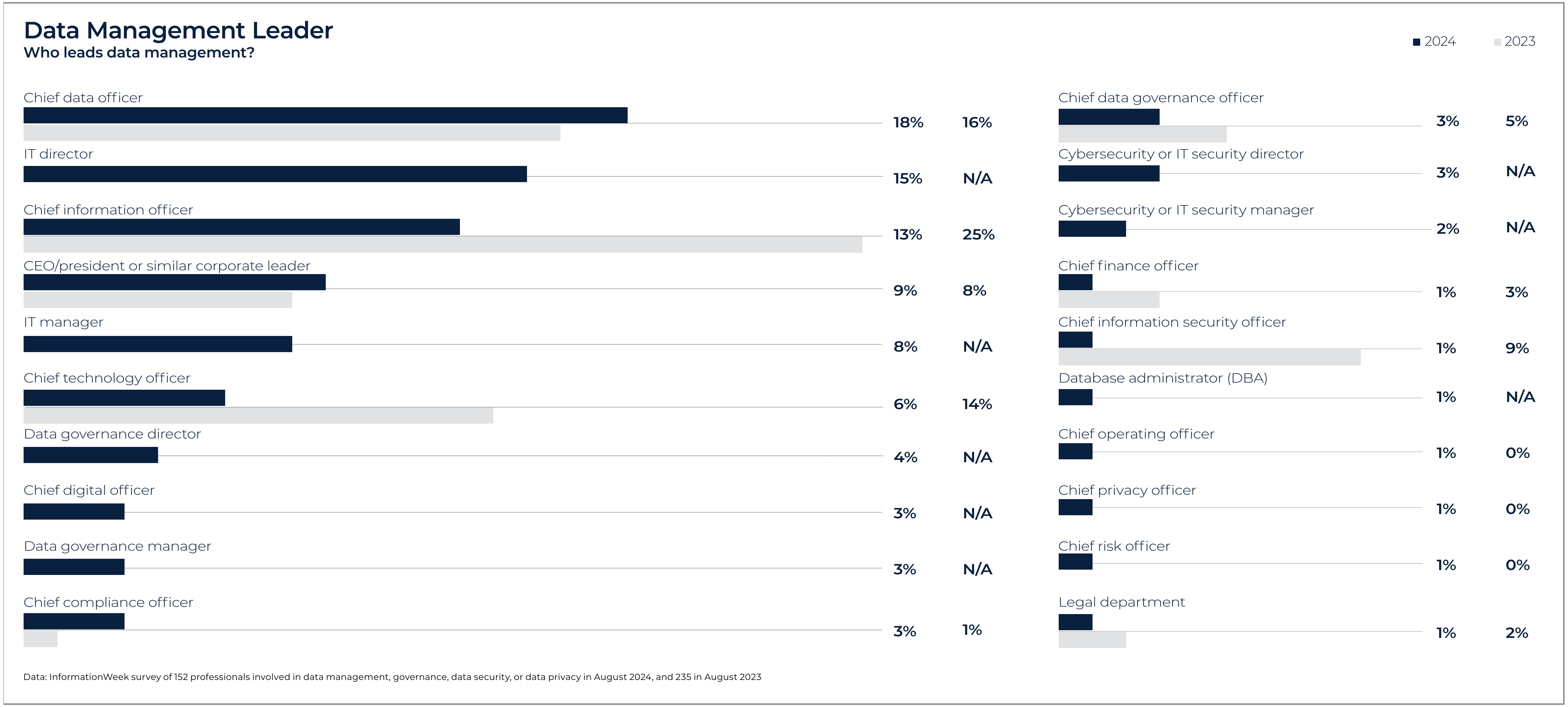
Data Governance Reporting Structure

Whom does the person leading data governance report to?



Data: InformationWeek survey of 152 professionals involved in data management, governance, data security, or data privacy in August 2024, and 235 in August 2023

Figure 15



Data Management Leader

Who leads data management?

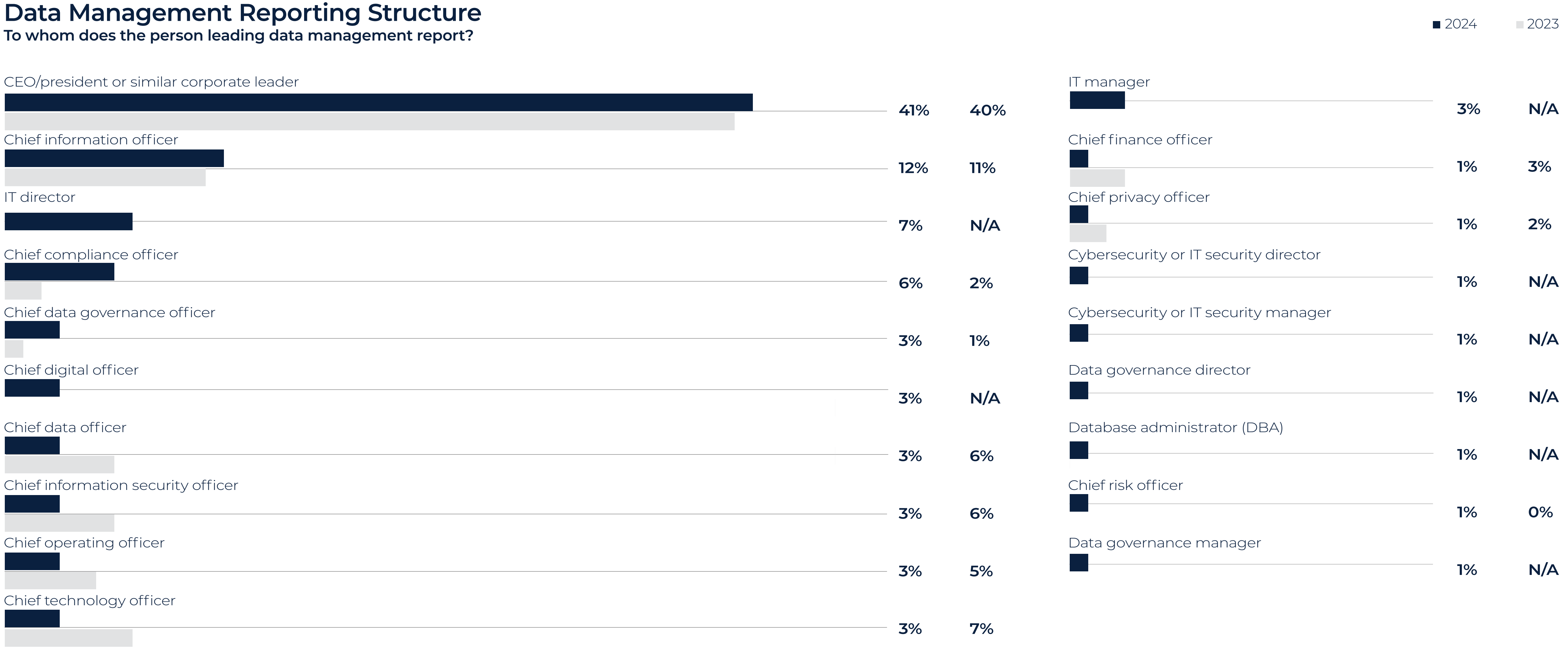
Data: InformationWeek survey of 152 professionals involved in data management, governance, data security, or data privacy in August 2024, and 235 in August 2023

PREVIOUS
NEXT

Figure 16

Data Management Reporting Structure

To whom does the person leading data management report?

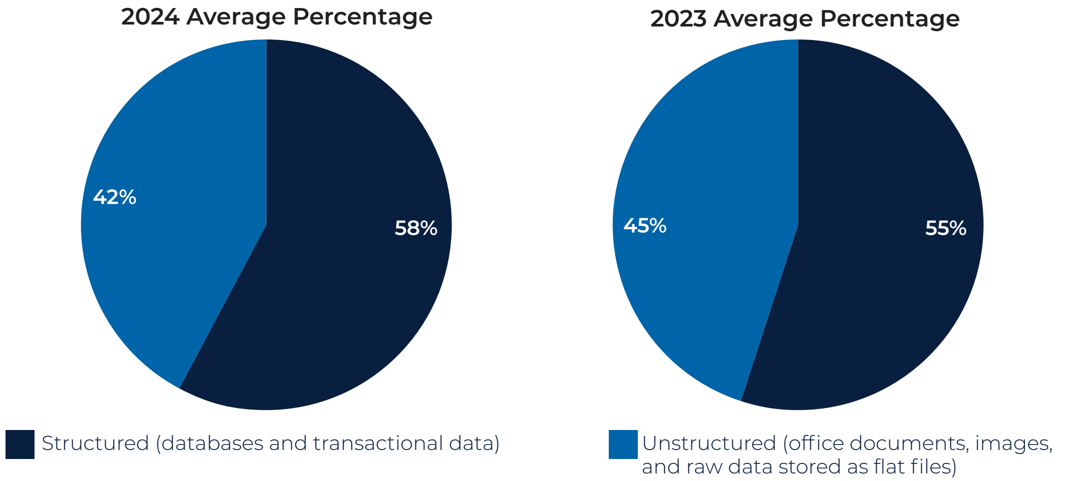


Data: InformationWeek survey of 152 professionals involved in data management, governance, data security, or data privacy in August 2024, and 235 in August 2023

Figure 17

Structured Versus Unstructured Data

Using your best estimate, what percentage of your data is structured vs. unstructured?

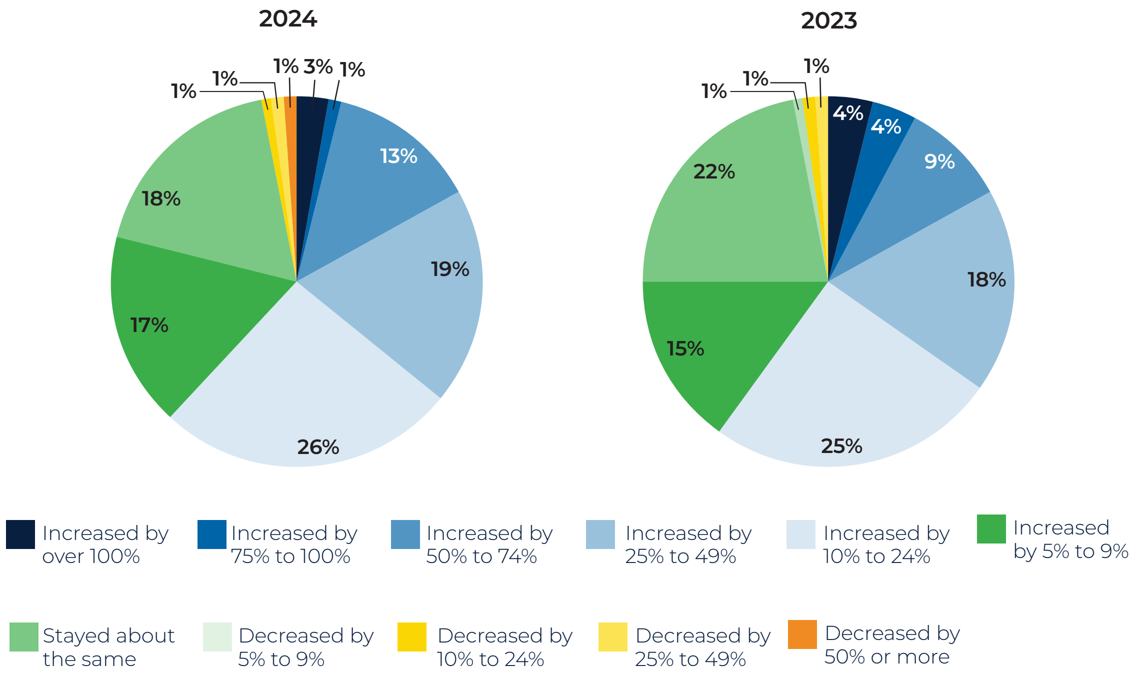


Data: InformationWeek survey of 152 professionals involved in data management, governance, data security, or data privacy in August 2024, and 235 in August 2023

Figure 18

Data Growth

Thinking back to the total amount of data managed you answered previously, approximately how much has the amount changed in the past 12 months?

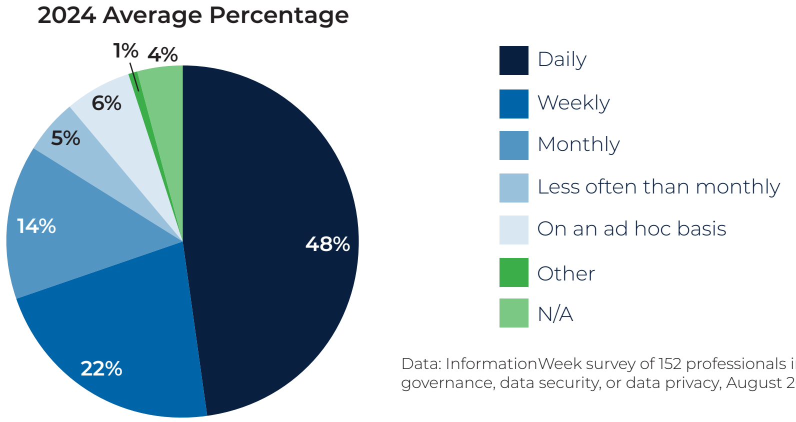


Data: InformationWeek survey of 152 professionals involved in data management, governance, data security, or data privacy in August 2024, and 235 in August 2023

Figure 19

Frequency of Sharing Data

How often do you need to share your data with others both internally and externally?

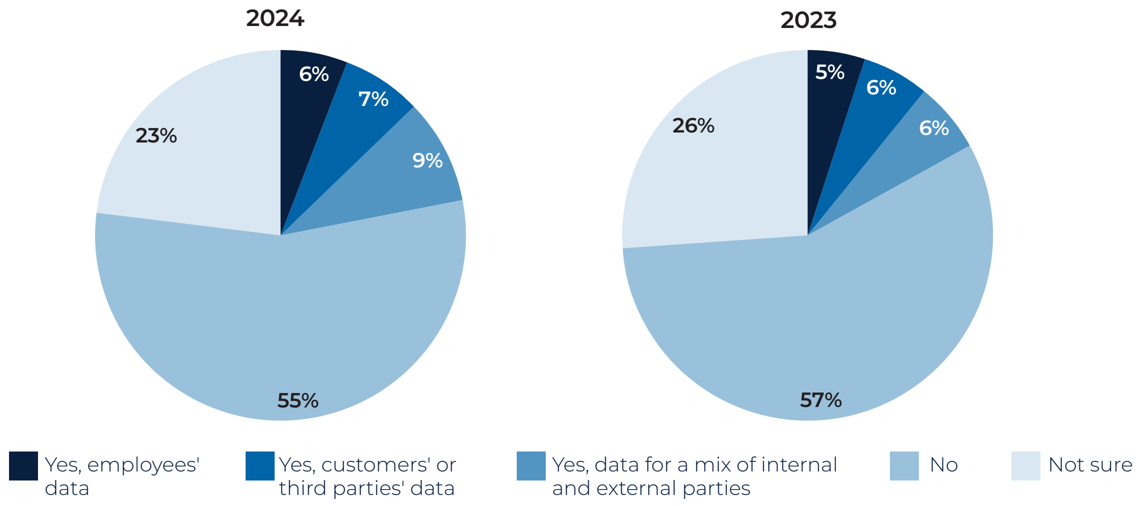


Data: InformationWeek survey of 152 professionals involved in data management, governance, data security, or data privacy, August 2024

Figure 20

Request for Users' Private Data

Have law enforcement or government agencies requested you turn over users' private data in the past 12 months?

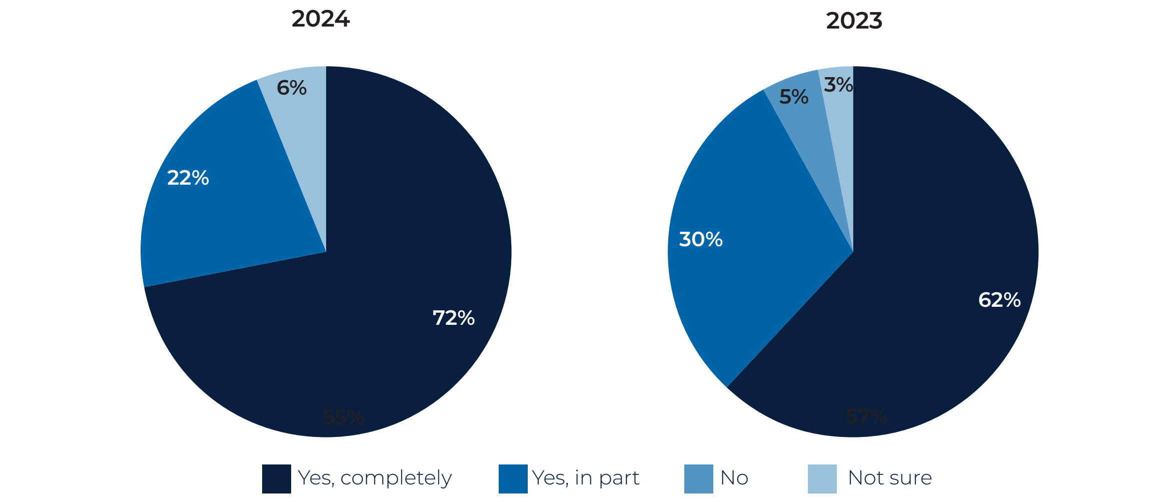


Data: InformationWeek survey of 152 professionals involved in data management, governance, data security, or data privacy in August 2024, and 235 in August 2023

Figure 21

Complying with Request For Data

Did you comply with the request for data?

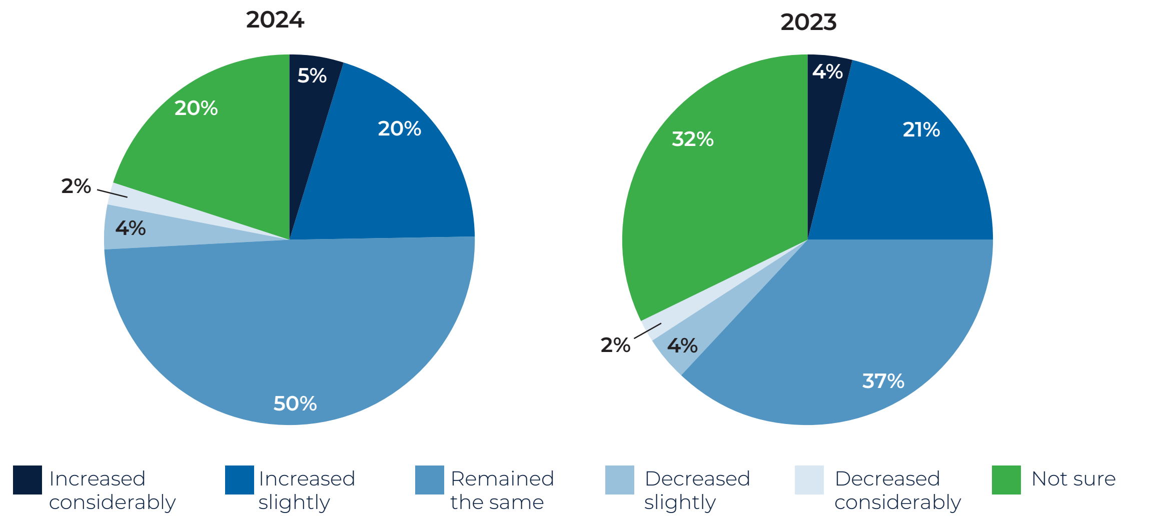


Base: 33 and 37 respondents who have had request for private data
Data: InformationWeek survey of 152 professionals involved in data management, governance, data security, or data privacy in August 2024, and 235 in August 2023

Figure 22

Change in Data Requests

Have these types of requests for data increased or decreased in the last 12 months?

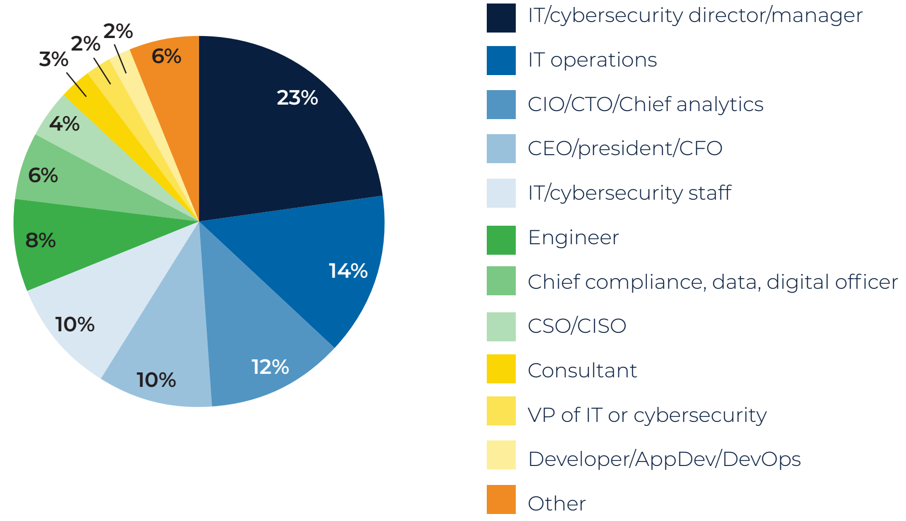


Data: InformationWeek survey of 152 professionals involved in data management, governance, data security, or data privacy in August 2024, and 235 in August 2023

Figure 23

Respondent Job Title

Which of the following best describes your job title?

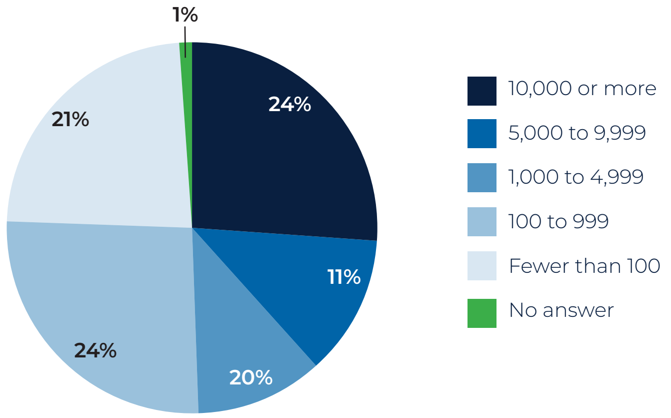


Data: InformationWeek survey of 152 professionals involved in data management, governance, data security, or data privacy, August 2024

Figure 24

Respondent Company Size

How many employees are in your organization in total?

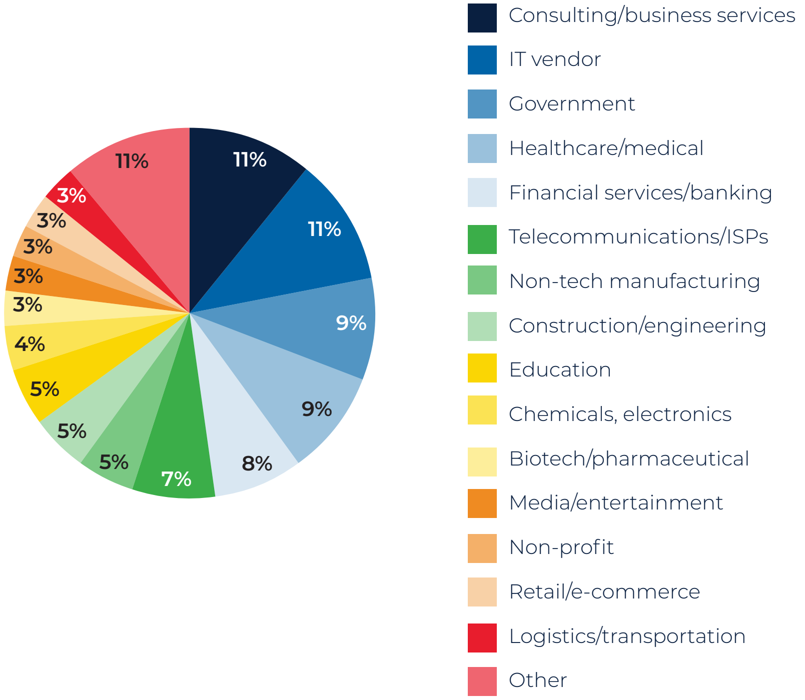


Data: InformationWeek survey of 152 professionals involved in data management, governance, data security, or data privacy, August 2024

Figure 25

Respondent Industry

What is your organization's primary industry?

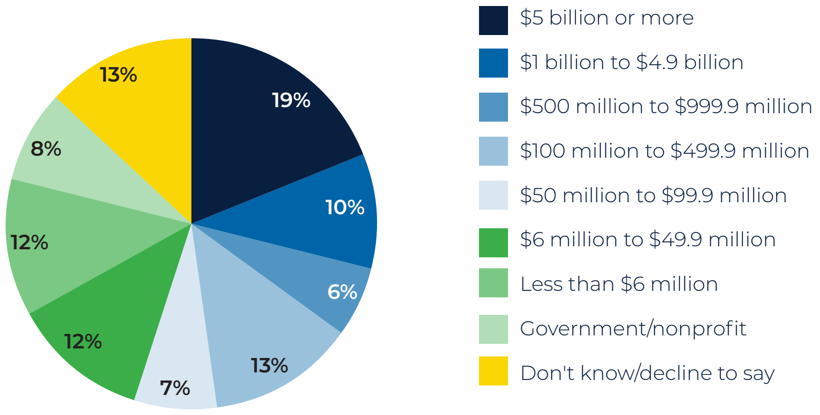


Data: InformationWeek survey of 152 professionals involved in data management, governance, data security, or data privacy, August 2024

Figure 26

Respondent Company Revenue

What is the annual revenue of your entire organization?



Data: InformationWeek survey of 152 professionals involved in data management, governance, data security, or data privacy, August 2024