



Global Data Privacy Experts

Strength through privacy



How and why the US should
embrace best-practice
privacy management



Disclaimer

This report presents independent research funded by Securys Limited. The research is based on a survey, conducted by Momentum ITSMA in September 2024 with 100 executives with responsibility for privacy compliance in US businesses employing over 1,000 people across the E-commerce, healthcare and retail financial services (banking, insurance etc) sectors. Copyrighted material is referenced in this report on the basis of fair use for research purposes; the moral rights of the original authors are recognised. Links in this document are provided for the convenience of the reader and Securys is not responsible for the availability or content of these external sites. Securys does not endorse or recommend any commercial products, processes or services; references to brands and products in this report are purely informational.

The authors have made every effort to verify the data presented in this report but Securys makes no warranty as to its accuracy or completeness. Nothing in this report shall be deemed to constitute financial or other professional advice in any way, and under no circumstances shall Securys or the authors be liable for any direct or indirect losses, costs or expenses nor for any loss of profit that results from the content of this report or any material in it or website links or references embedded within it.

This report is produced by Securys in the United Kingdom and Securys makes no representation that any material contained in this report is appropriate for any other jurisdiction. These terms are governed by the laws of England and Wales and you agree that the English courts shall have exclusive jurisdiction in any dispute.

Copyright

Securys Limited 2025. All rights reserved. You may share this report with others both within and outside your organisation in its entire and unaltered form, including but not limited to the Securys branding, contact information and this copyright notice. You may not make any other use of this report outside your organisation without express prior written permission from Securys. However, you may extract and use material from this report for internal purposes only provided that any such use includes attribution to Securys and recognition of our copyright.

Contents

Foreword	4
Key findings	6
Part 1: Why now is the time to build solid privacy management foundations	8
Multiple benefits but defense leads the debate	10
Privacy risks are on the increase	12
AI raises the stakes	14
Part 2: Towards more effective privacy governance	16
The building blocks for privacy are in place	18
Tracking risks and liabilities	22
The case for stronger oversight	24
Part 3: Transforming privacy operations	26
Building for success	28
Stepping up best practice	30
Building the business case	34
Recommendations	36
About Securys	38
Methodology	39

Foreword

Around the world, individuals are gaining control of their personal data.

Backed by legislators and regulators conscious of the transformative impacts of artificial intelligence (AI), people are determined to address the asymmetries in the relationships between individuals and large data-intensive organizations. In the past five years, the proportion of the world's population covered by data protection laws has grown from **10% to 82%**.

Yet in the world's largest economy, the legislative framework governing data protection remains remarkably immature. In the US, there is no federal privacy act that provides a clear view of organizations' responsibilities to safeguard personal data. Efforts to create a unified legal framework for privacy by the National Institute of Standards and Technology (NIST) and the Federal Trade Commission (FTC) are not backed by the full force of the law and individual states.

Where individual states have produced modern privacy and cyber laws, there is limited alignment, although California is emerging as a model for other states. Even so, US state privacy laws tend to focus on consumers and large-scale processing, overlooking many other activities that require regulation.

That puts the US at odds with its neighbors and international peers. On its borders, both Canada and

Mexico have implemented principles-based privacy regimes. Further afield Europe along with much of Latin America, Africa and Asia have constructed a raft of data protection regulations. China may approach the question from a different perspective, but it too has introduced comprehensive legislation.

A significant challenge to US organisations is their exposure to both regulatory and litigational risk arising from the complex interaction of sectoral federal laws, state privacy biometric data and cyber security legislation and the wider international context. Ironically, far from reducing the risks arising from the processing of personal data, the lack of a federal data privacy law makes privacy risk management both more demanding and more urgent. This is only exacerbated by the ever-accelerating development and adoption of AI in very aspect of modern business.

Against this backdrop, we wanted to understand how those on the front line of privacy management in corporate America now see their roles – and what that says about their organizations' approach to privacy. How do US businesses oversee privacy governance, how do they manage privacy operations, and how do they build a business case for investments in privacy?



In the world's largest economy, the legislative framework governing data protection remains remarkably immature.



We wanted to understand how those on the front line of privacy management in corporate America now see their roles – and what that says about their organizations' approach to privacy.

This report sets out the answers to these questions and more. Through a survey of 100 senior leaders with responsibility for privacy compliance in three industries at the heart of this debate – e-commerce, healthcare, and retail financial services – we explore how US organizations are building governance and operational structures that are fit for purpose in today's environment.

At Securys, we believe the benefits of effective privacy management are wide-ranging – from brand trust to efficient data processing – and that the risks of a misstep are both significant and growing by the day. The US's data privacy regime may be immature by international standards, but individual organizations ready to take a proactive lead have much to gain.

With more than a decade of experience helping enterprise organizations manage privacy across jurisdictions and in complex data-sharing ecosystems, Securys has both the expertise to identify your risks and challenges, and the capability to deliver solutions.



Ben Rapp

Group Chief Executive Officer
SECURYS

Key findings

Benefits

US businesses **recognize the potential benefits** of effective privacy management



75% say it **boosts trust** in their brand



69% expect it to help them **maximize the value** of data

Measurement

Many have **yet to adopt important measures**



39% of US businesses **fail to carry out privacy audits**

44%

fail to benchmark their practices against those of other organizations



Governance

Some of the **building blocks** for privacy governance are in place



70% have **developed a formal privacy policy** and associated procedures

83% have adopted the **NIST Privacy Framework**

NIST

Structures

But **governance structures** are a cause for concern

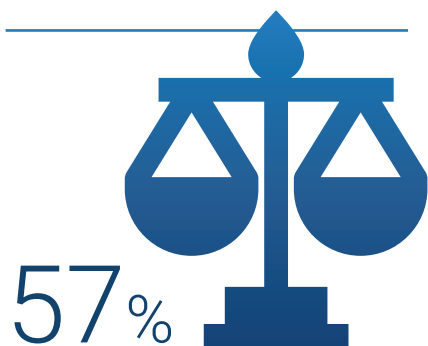
58%

of respondents say their privacy governance is **overseen by the executive who is also responsible for its delivery**



Risk

Risk reduction is front of mind



have invested in privacy management to minimize legal disputes



50%
have invested to reduce regulatory risk

Capabilities

Moreover, US businesses are **insular in their approach** to privacy

67%

are missing best practice expertise from specialist privacy consultancies even though only 36% are very or completely confident they can recruit the talent they need

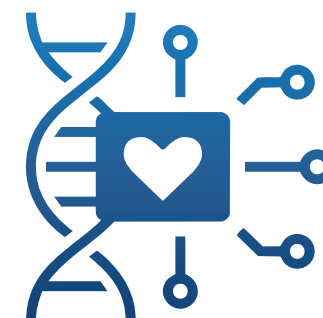
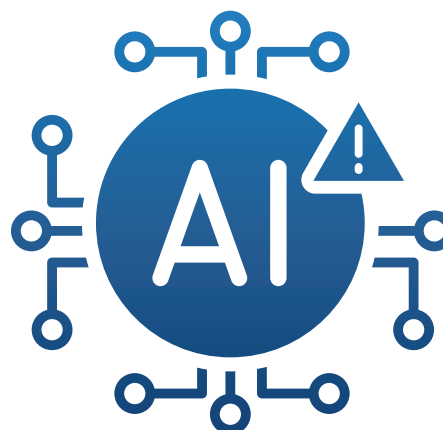


AI

Despite this immaturity, US businesses are **confident in their ability** to address the data-related risks of AI

65%

are very or completely confident they can deal with such risks



Customers do not agree

75%

worry that healthcare providers will move too fast*

*Data from Pew Research Center



Global Data Privacy Experts

Part 1

Why now is the time
to build solid privacy
management foundations

Strength through privacy

INTRODUCTION

When it comes to privacy management, US businesses stand at a crossroads.

One path requires little or no action in the short term: given the lack of principles-based regulation around data protection and privacy, there is little to force businesses that operate within US borders to act. But this path exposes them to increasing risk and a growing opportunity cost, particularly as the adoption of AI accelerates.

The other route requires immediate effort to build strong foundations for privacy management. This path leads to potential competitive advantage and superior risk management.





Multiple benefits but defense leads the debate

Respondents to our survey see a range of potential benefits from improving the effectiveness of their privacy management (Figure 1).

Three-quarters (75%) believe better privacy management could boost brand trust, while almost as many (74%) say it could help them meet their commitments on environmental, social and governance (ESG) issues. Nearly seven in ten (69%) believe effective privacy management lets them maximize the value they secure from their customer and employee data.

But there are also points of disconnect. Most strikingly, 70% of respondents regard data privacy as a necessary cost of compliance but not a discipline that adds value. This may explain why so many US organizations are investing in privacy management for defensive reasons, rather than to secure positive benefits.

For example, 57% of respondents say they invest in privacy management with a view to minimizing the risk of legal disputes; 50% invest with regulatory risk

in mind. By contrast, only 33% of organizations include competitive advantage in their privacy management investment plans. Fewer than a quarter (24%) are motivated by the desire to minimize the costs of managing customer and employee data.

Moving the needle requires a shift of mindset. In many US organizations, privacy management is primarily seen as an issue for the legal function. And in the absence of regulation that applies to all organizations, many hope their legal teams can help them keep compliance work to a minimum.

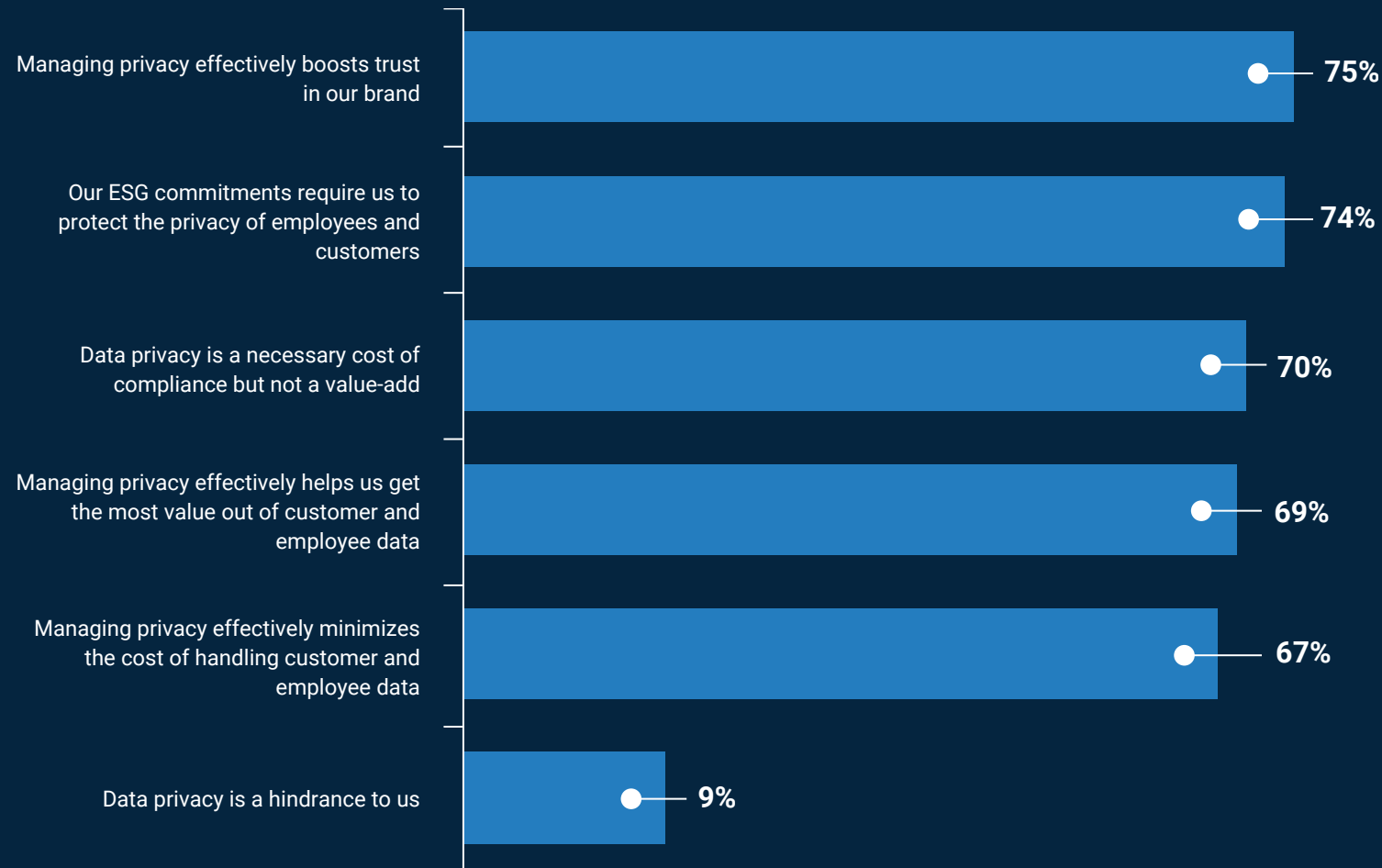
This is problematic in two ways. First, it ignores the march of privacy regulation in other jurisdictions worldwide; critically, that regulation applies to every US business hoping to do business in those jurisdictions. Secondly, it denies the direction of travel in the US, which has been towards regulation, albeit at a slower pace than elsewhere. Even during a second Trump presidency, privacy regulation looks set to increase – not least because many consumers are demanding it, as [separate Securys research has shown](#).

Moving the needle requires a shift of mindset. In many US organizations, privacy management is primarily seen as an issue for the legal function.

FIGURE 01

How privacy management drives advantage

? To what extent do you agree or disagree with the following statements?
(% 'strongly' or 'somewhat' agree)



75%

believe better privacy management could boost brand trust



Privacy risks are on the increase

Relegating privacy management to the legal function prevents organizations from getting ahead of the problem proactively and coherently. This approach threatens the benefits from better privacy management; it may even stymie US businesses' efforts to grow in new territories overseas, or in other states moving faster on regulation.

Worse, depending on legal teams to rescue the organization from onerous privacy management responsibilities looks increasingly risky. US organizations may be comfortable with a culture in which concepts such as data protection are litigated in the courts rather than dictated by principles-based regulation, but this culture is becoming outdated.

California's Privacy Rights Act came into full effect on 1 January 2023, though it includes certain retrospective provisions. The legislation, first agreed in 2018, has proved influential. By the start of 2025, 19 separate states had enacted privacy laws. With each new regulatory regime, the definitions, scope and enforceability of privacy management provisions evolve a little further.


Internationally, the regulatory environment is moving even faster. In the European Union, the General Data Protection Regulation (GDPR) has inspired privacy regulators worldwide, with tough enforcement provisions and severe penalties for failures. In the worst cases, GDPR gives regulators the right to fine companies up to 4% of their global turnover for a compliance breach. Equally, however, national lawmakers are building on the GDPR with new requirements. Global privacy laws now number more than 100, with 270 regulators policing these regimes.

Facing this onslaught from both domestic and international regulators, US organizations cannot afford to be complacent. Even if they are not compelled by the promise of competitive advantage, good risk management now demands a new mindset.

Even if they're not compelled by the promise of competitive advantage, good risk management now demands a new mindset.



California's Privacy Rights Act legislation has proved influential with 19 separate states having enacted privacy laws by the start of 2025.



US organizations cannot
afford to be complacent.



AI raises the stakes

There is more. For those organizations that remain unconvinced, the advent of AI is the final nail in the coffin for a laissez-faire approach to privacy management.

Already, American consumers are deeply concerned about the advance of AI. [Data from Pew Research Center](#) suggests that 52% of Americans are more concerned than excited about AI. In certain fields, alarm is even higher; 75% of Americans worry healthcare providers will move too fast using AI, Pew's work warns.

To ease this anxiety, US businesses must build trust in AI by committing to transparency and high ethical standards. They must also define legal and ethical data use within AI models, avoid bias and unfairness, and ensure proper consents are secured.

These are concepts that policymakers in other jurisdictions are already beginning to enshrine in regulation. The EU AI Act, for example, introduces a [range of safeguards and requirements](#) designed to protect privacy and fundamental human rights.

One trend that US businesses should note is the focus in many jurisdictions on outcomes, as well as technical compliance. Many regulators appear to be more concerned whether organizations are delivering safe AI outcomes than the process they follow. For US businesses, that may be a challenging idea.

Worryingly, US organizations appear to be remarkably confident about their readiness for the data governance implications of AI (Figure 2). Almost two-thirds of respondents to our survey (65%) describe themselves as very or completely confident about their ability to deal with the additional risks that implementing AI tools and technologies will create.

This proportion looks high given many of the problems which these organizations are currently struggling with, as the next two parts of this report illustrates. Building more solid foundations in data governance will be vital if this confidence is not to prove misplaced.

US organizations appear to be remarkably confident about their readiness for the data governance implications of AI

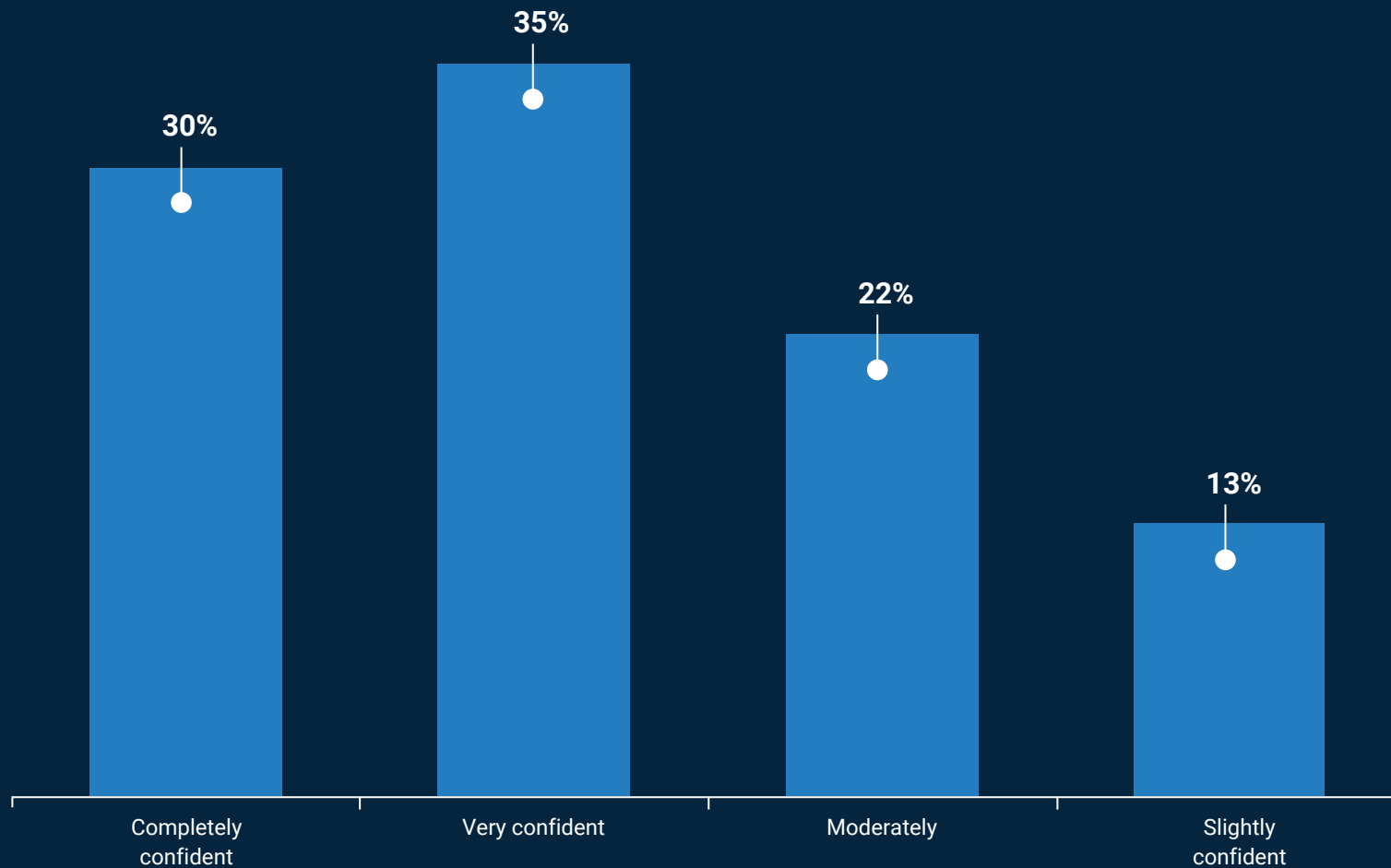


One trend that US businesses should note is the focus in many jurisdictions on outcomes, as well as technical compliance.

FIGURE 02

Are US businesses over-confident about AI risk?

? How confident are you that your organization is prepared for the data governance and risk implications of AI?
(% of respondents)



75%

of Americans worry
healthcare providers
will move too fast
using AI



Global Data Privacy Experts

Part 2

Towards more effective
privacy governance

Strength through privacy

INTRODUCTION

Effective privacy governance, with appropriate structures and frameworks, is the key to ensuring organizations have proper oversight over their use of personal data.

Our research suggests that while many US businesses have made good progress here – particularly those in regulated sectors of the market such as financial services and healthcare – there is significant room for improvement; closing the gap will help organizations secure the benefits and manage the risks outlined in Part 1 of this report.





Relatively few organizations feel the need to take external advice on how to achieve effective privacy governance.

The building blocks for privacy are in place

The good news from this survey is that many organizations now have the building blocks in place for effective privacy governance (Figure 3).

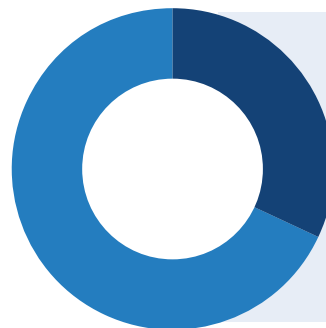
Seven in ten (70%) have a data privacy policy in place, meaning a formalized approach to how the organization deals with privacy management. The majority have appointed a data protection officer and have a governance or audit committee that considers privacy issues as part of its terms of reference.

There are causes for concern, though. Relatively few organizations feel the need to take external advice on how to achieve effective privacy governance from a specialist privacy consulting firm or a law firm with

expertise in this area. Clearly, most organizations feel equipped to manage privacy governance for themselves.

Given the pace of change facing these organizations – both in terms of customer and employee demands, and formal regulation – the worry is that this represents complacency or overreach.

The maturity required to deliver a holistic governance program is significant. But organizations outside regulated sectors, and with less exposure to international markets, will have very limited experience in this area. Privately owned businesses not required to meet such exacting standards in other areas of governance may find this issue particularly challenging.



Almost one in three organizations report having no DPO in place.

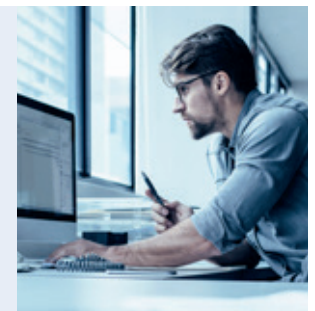
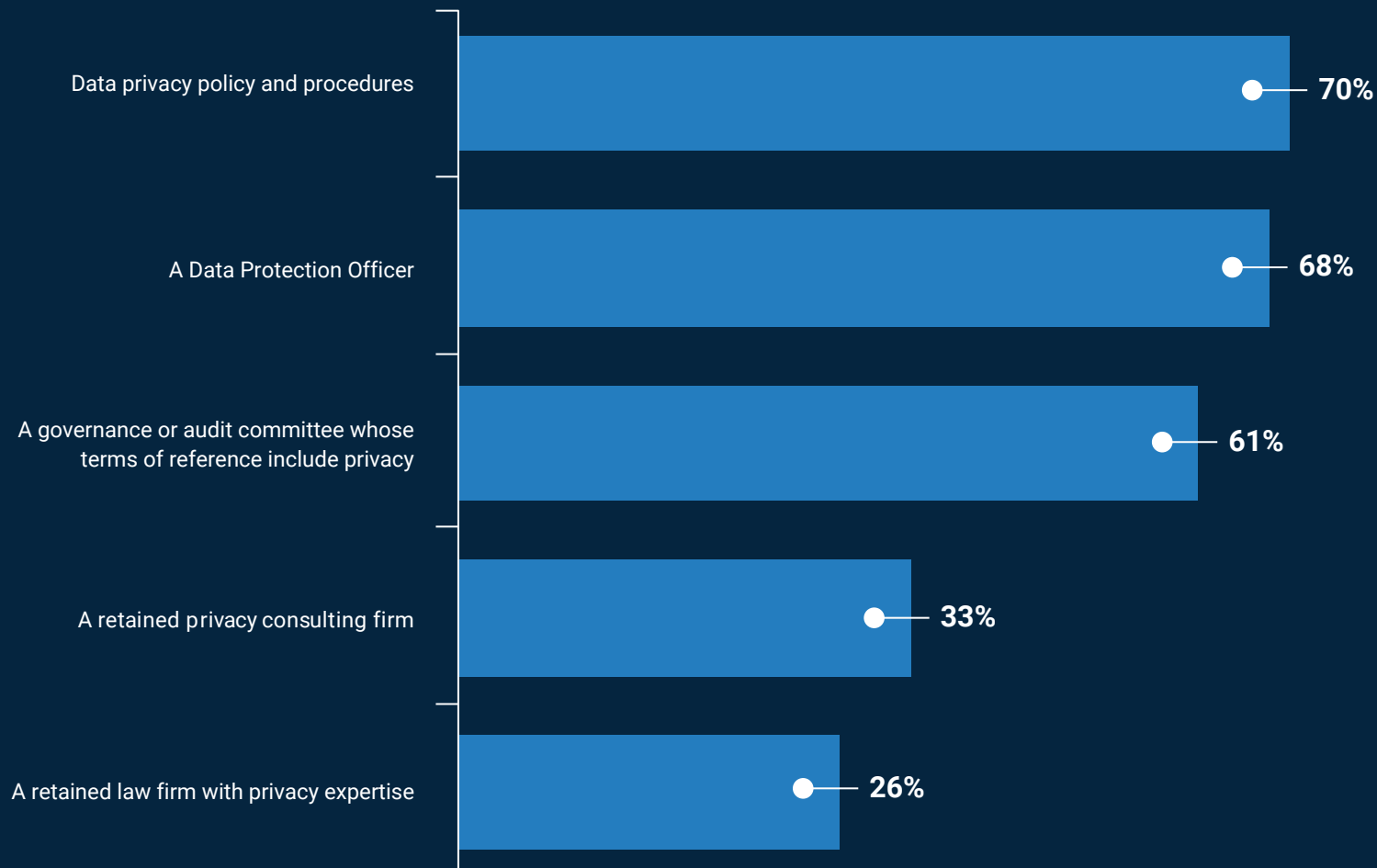


FIGURE 03

Starting with the basics

? Which of the following organizational measures does your organization have in place to govern privacy?
(% of respondents)



30%

of organizations have
no formalized data
privacy policy on
how the organization
deals with privacy
management

Privacy frameworks offer piecemeal solutions to specific challenges rather than an over-arching vision of what good governance looks like.

Many have turned to the privacy frameworks developed by official bodies and agencies for guidance. These frameworks are typically voluntary but set out a standardized approach to identifying and managing privacy risk (Figure 4).

Most commonly, more than eight in ten respondents to this research (83%) say they have adopted the NIST Privacy Framework; almost three-quarters (73%) have adopted the NIST AI Risk Management Framework.

This is welcome as these are robust frameworks that can play a key role in helping organizations to build out effective privacy management governance infrastructure.

But they are only a starting point. They offer piecemeal solutions to specific challenges rather than an over-arching vision of what good governance looks like. Critically, they do not provide organizations with an integrated and holistic data operating model – a single structure, with clear KPIs that boards can use to interrogate the organization's performance on privacy management. And they don't lay out a full continuum of capabilities across the organization, ensuring that every function is playing its part in delivering high-quality privacy management.

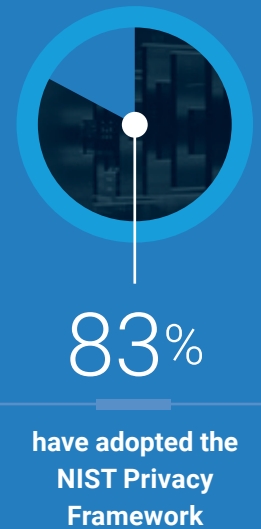
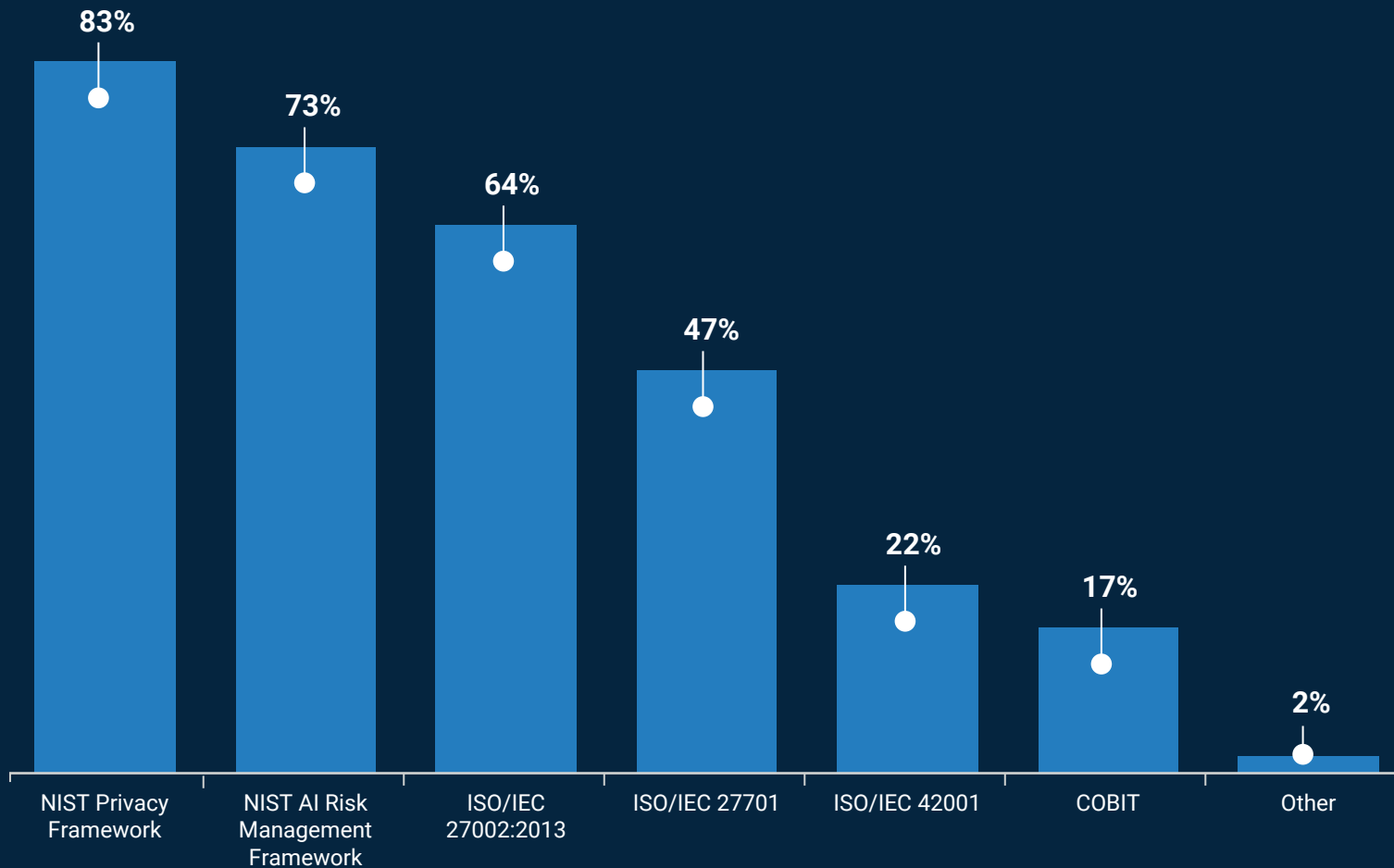
Many have turned to the privacy frameworks developed by official bodies and agencies for guidance.



FIGURE 04

A framework for privacy governance?

? Which of the following frameworks, if any, does your organization use to manage privacy and/or AI compliance?
(% of respondents)





More than half of organizations struggle to communicate privacy risks and challenges.

Tracking risks and liabilities

Despite the absence of a holistic approach to privacy governance in most organizations, the confidence of US businesses in their abilities to manage risk and regulation is very high (Figure 5).

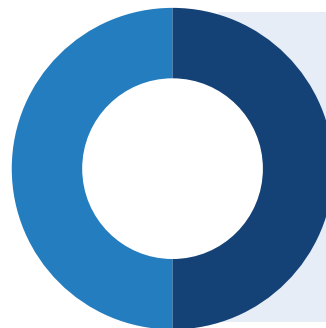
More than half (56%) describe themselves as very or completely confident that they can identify privacy risk. Almost as many (50%) say the same of their understanding of privacy laws across multiple jurisdictions.

Respondents even report a high level of confidence about the compliance challenges posed by AI, despite the nascent state of regulation in this rapidly evolving area.

Almost one in four organizations (23%) are completely confident they understand the risk and compliance implications of AI, with a further 26% very confident.

Still, there are some areas where confidence is more limited. More than half are struggling to communicate privacy risks and challenges within their organizations, hinting at their lack of integrated and overarching governance. There is also a significant talent shortage, with many businesses reporting difficulties in recruiting sufficient numbers of suitably trained privacy compliance specialists.

These concerns undermine organizations' claims of confidence in other areas. They also raise the question of why organizations seem so reluctant to bring in external support for privacy governance and management, as seen in Figure 3 on page 19. If they are unable to integrate governance for themselves, or to recruit the skills they need, they will need to draw on specialist expertise from third-party advisors.



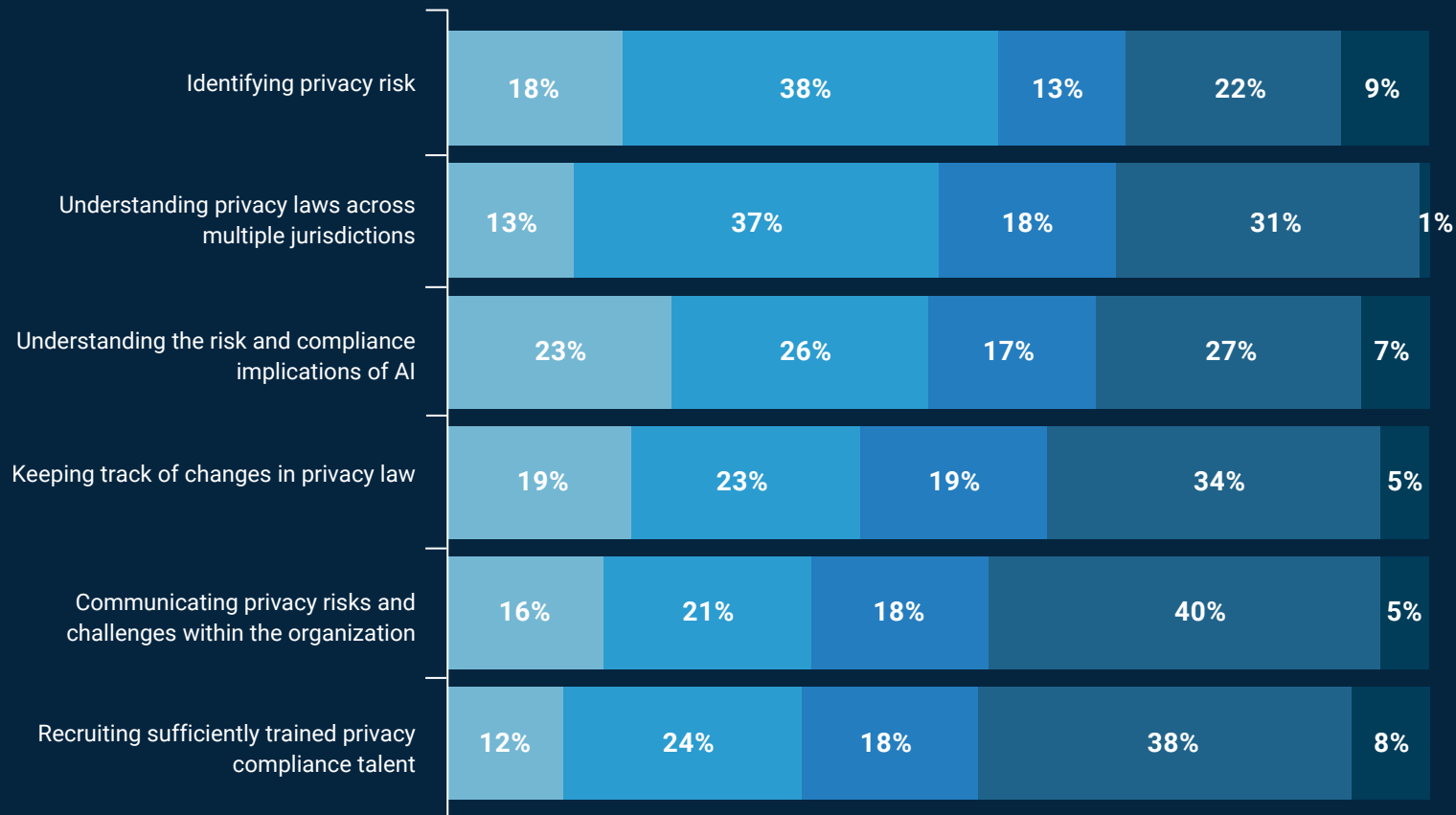
Only half of the organizations polled report being completely confident or very confident in understanding privacy laws across multiple jurisdictions.



FIGURE 05

No shortage of confidence

? Which of the following are your organization's greatest challenges when it comes to identifying its privacy compliance obligations and risks?
(% of respondents)



■ Completely confident ■ Very confident ■ Moderately confident ■ Slightly confident ■ Not at all confident



56%

describe themselves
as very or completely
confident that they can
identify privacy risk



The case for stronger oversight

Alarm bells should also sound over the way many organizations are building accountability and reporting lines. Some have appointed clearly designated and qualified leaders such as chief privacy officers, but in many cases, responsibility for privacy is owned by executives, such as the CIO, the CFO, or the general counsel, who are unlikely to have the required expertise. These leaders may also face conflicting priorities in balancing privacy concerns with their core activities (Figure 6).

Similarly, nearly six out of ten respondents (58%) say that privacy governance in their organizations is overseen by the executive who is also responsible for its delivery. This is at odds with generally accepted approaches to governance in other areas, including finance and ESG governance.

Across much of the rest of the world, there is a regulatory requirement for a separation of duties usually accomplished by the appointment of a Data Protection Officer who is accountable for ensuring the organization's privacy compliance, reporting to the most senior level of management in the organization and prevented by a statutory bar of conflict in interest in taking part in decision making regarding personal data processing.

The aim should be to build joint ventures for governance. Certainly, the gravity of privacy management requires C-level oversight – the CEO is ultimately responsible for the organization's most fundamental ethical pillars – and reporting to either the board or a specialist committee on ethics. But the structure below this oversight needs to reflect the inherent opportunities and the risks; it makes sense for functions such as marketing and business development to work together with risk.

Otherwise, organizations tend to delegate privacy to particular functions – to legal, for example, or to IT. That makes it much harder to secure the holistic approach that the organization needs to deliver the accountability that the C-suite and the board should be demanding.

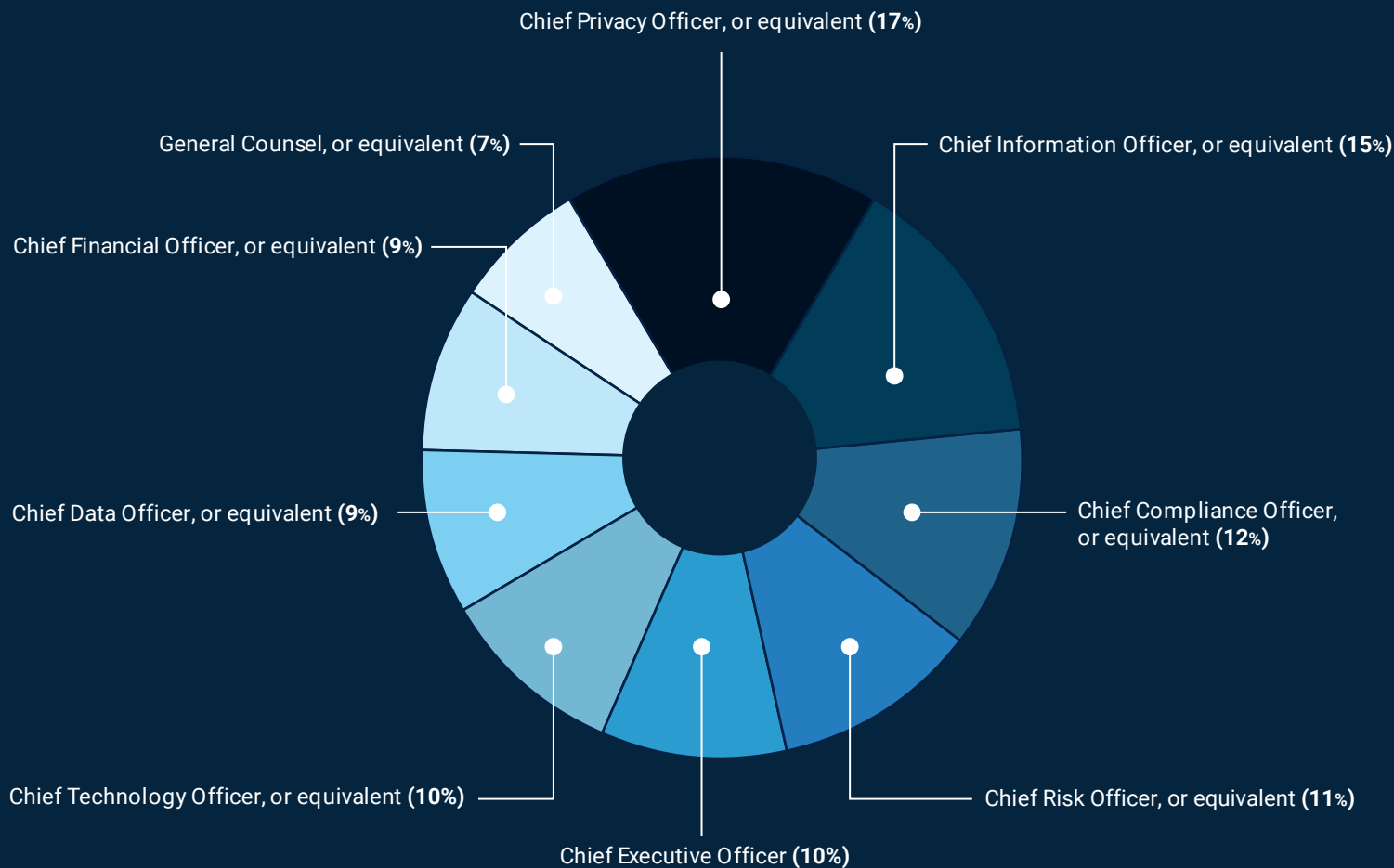
A related danger is the growing tendency of organizations to add responsibility for AI compliance to the job description of privacy and data protection roles. AI governance requires particular skills that data protection professionals may not have, especially if they come from a legal background.

The gravity of privacy management requires C-level oversight.

FIGURE 06

Where responsibility for privacy currently lies

? In your organization, who is the most senior executive with explicit responsibility for and active involvement in privacy?
(% of respondents)



51%

indicated that they were either not at all, slightly or moderately confident that they understood the risk implications of AI.

Part 3

Transforming privacy operations

INTRODUCTION

If organizations can rise to the challenge of implementing more robust privacy governance structures, they will be in a stronger position to manage privacy operations effectively.

They will be able to handle data in a way that achieves compliance and builds trust with customers, employees, and other key stakeholder groups. Our research highlights several areas where US businesses have opportunities to make operational improvements.





Building for success

While many businesses have adopted frameworks such as those developed by NIST, there is still an appetite for more structure and guidance on privacy operations (Figure 7).

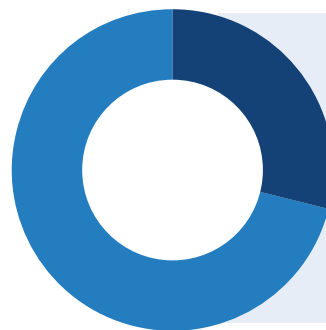
The most commonly cited operational challenge by US businesses seeking to improve the effectiveness of their privacy management is the lack of privacy and information security policy frameworks.

As discussed in Part 2, each framework provides support for particular aspects of privacy governance and operations but falls short of the necessary holistic approach. Clearly, many organizations are beginning to recognize this issue.

Similarly, almost a third of US businesses (32%) are concerned they lack guidance on privacy operations. Effective privacy management requires organizations to deliver operational excellence as well as strong governance, but many feel poorly equipped and advised to achieve the former.

Other issues highlighted in Figure 7 point to specific areas where many organizations now need to do more work. More than a quarter (29%) acknowledge the need to adapt for the impact of AI developments. Almost as many (27%) say they now need to focus on resolving the issue of data silos in their businesses, and 26% say they lack the tools and technologies necessary to do better.

A third of US businesses are concerned they lack guidance on privacy operations.



Almost one in three organizations experience difficulty in making the business case for investments in privacy.

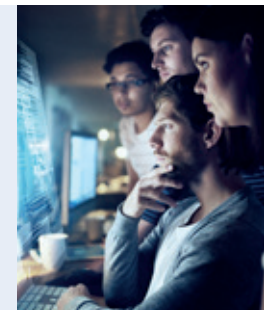
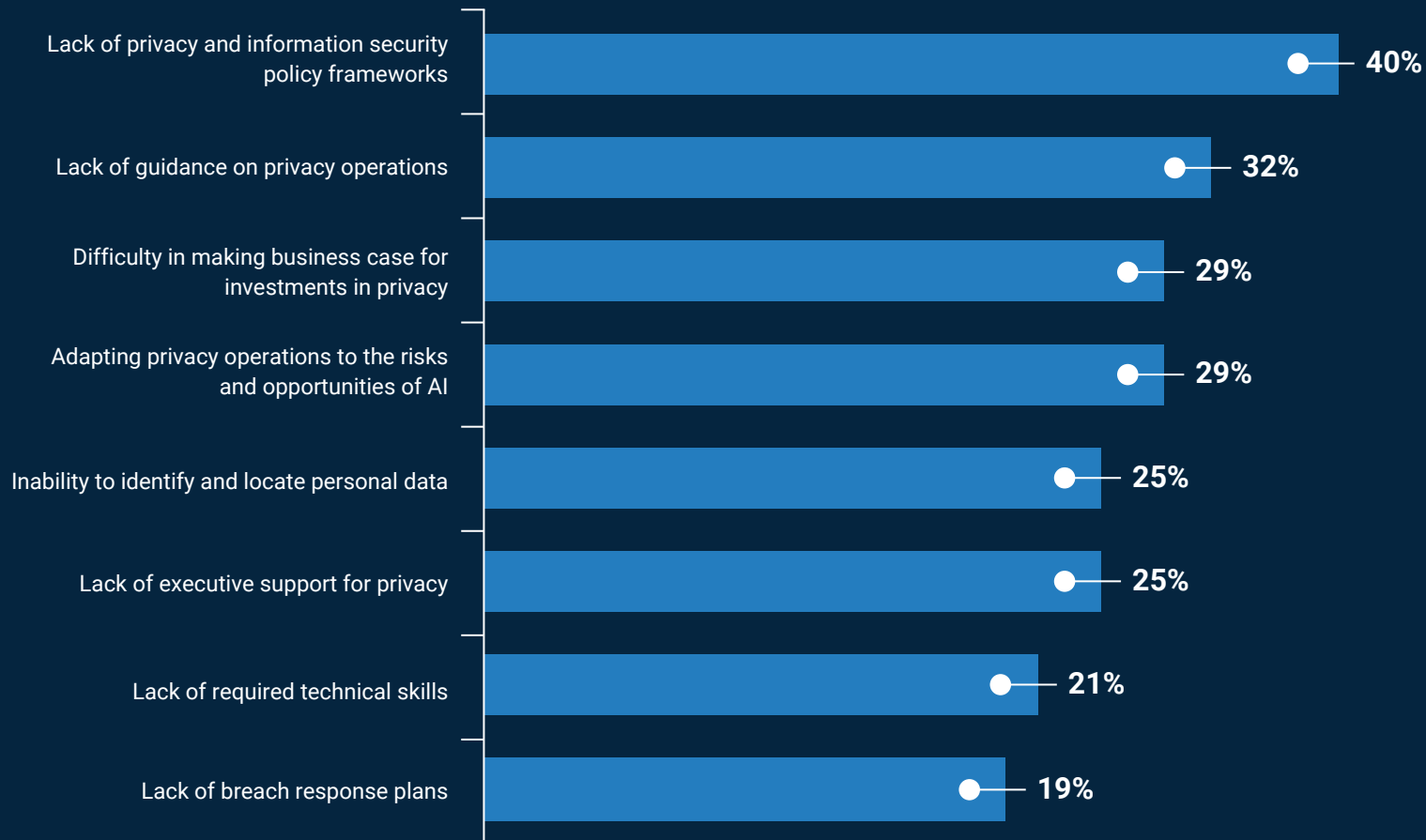


FIGURE 07

Obstacles to effective privacy management operations

? Which of the following are the greatest operational challenges to effective privacy management at your organization?
(% rank 1/2/3)



40%

of US businesses lack
privacy and information
policy frameworks

There is a need to do more to manage data risk across the supply chain – US businesses routinely share data with vendors, suppliers, and other partners.

Stepping up best practice

It is also the case that many organizations now need to step up their privacy management. Too few businesses are on top of key operational and governance controls – delivered either in-house or through outsourced providers – that drive greater effectiveness.

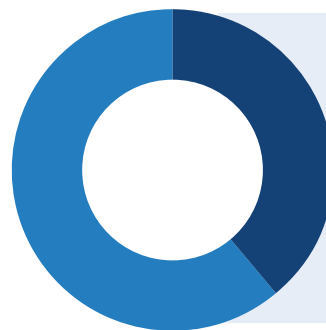
For example, only just over half of respondents to our survey (56%) regularly benchmark their privacy practices against those of other organizations. The same number have the capability to manage privacy rights requests; and only a slightly higher proportion (61%) carry out privacy audits.

There is also a need to do more to manage data risk across the supply chain. US businesses routinely share data with vendors, suppliers, and other partners; each of these organizations potentially poses a risk from a privacy perspective, but it is not clear whether

this danger is being identified or mitigated. A more systematic approach to supply chain risk could also help many businesses build more streamlined and effective partner ecosystems.

Where organizations lack the capacity to carry out these operational tasks in-house, outsourcing the work makes sense. This is clearly happening to some extent, with US businesses using outsourced providers in areas such as benchmarking, privacy rights requests, and horizon scanning, our research suggests a widespread reluctance to embrace external support for their operations.

For every operational privacy capability covered in this study, fewer than half of respondents currently use outsourcing (Figure 9). Many say they would consider doing so, but that does not appear to be translating into practice.



More than one in three organizations report not carrying out privacy audits.

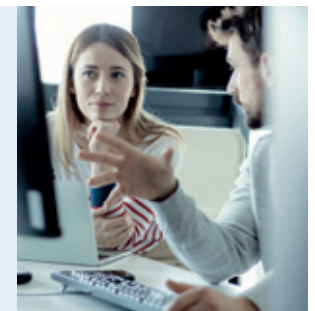


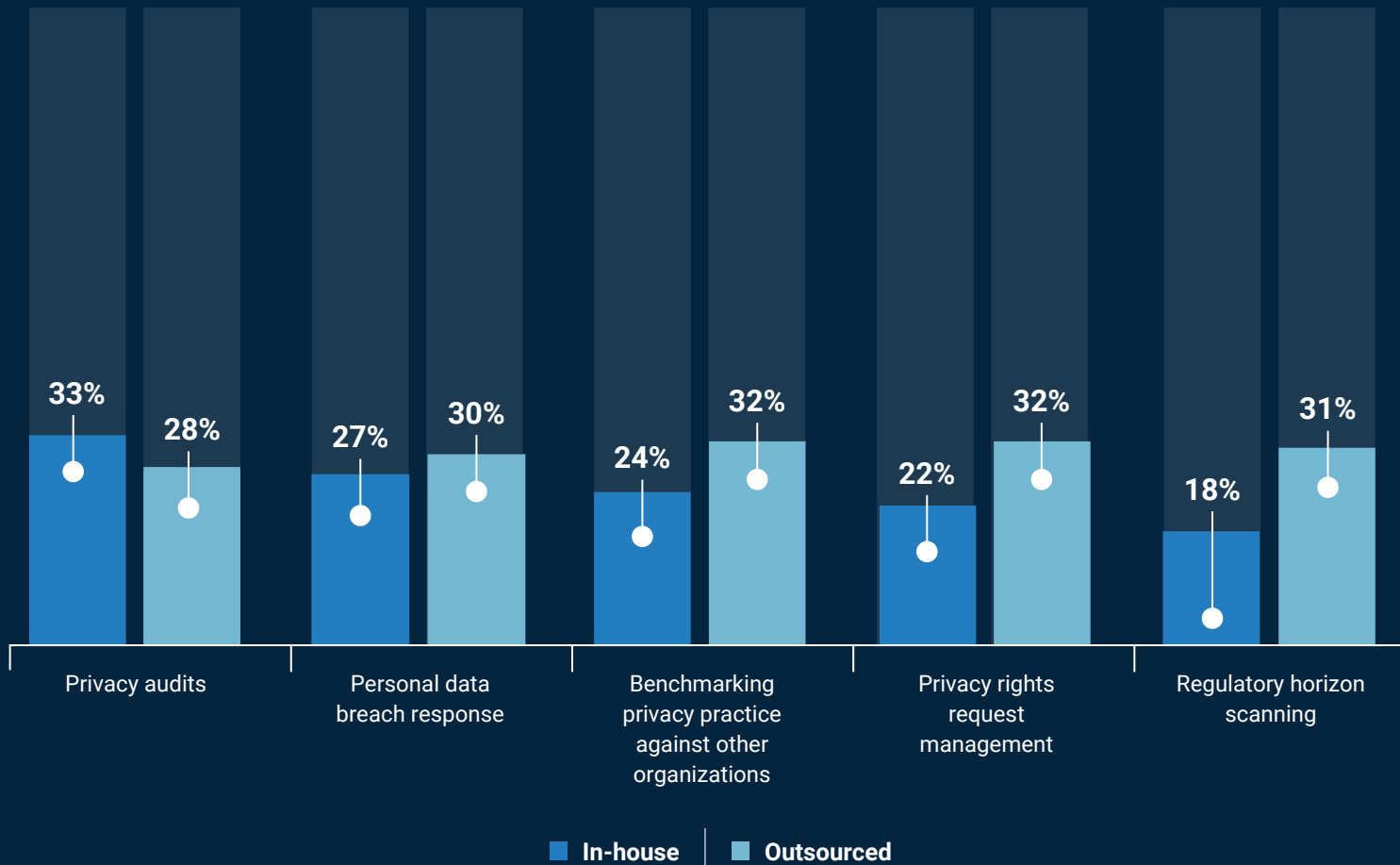
FIGURE 08

The need to do more



Which of the following privacy management measures or capabilities does your organization have in-house? Does your organization currently use outsourced capabilities for each of the following functions?

(% of respondents)



44%

do not regularly benchmark their privacy practices against those of other organizations



Many organizations report skills shortages and difficulties with recruitment.

Stepping up best practice (continued)

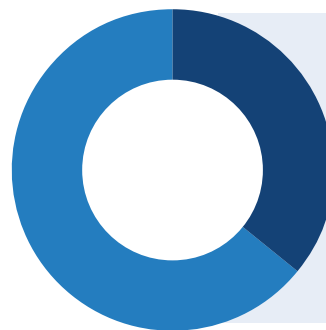
Outsourcing is more common for certain practices. For example, 43% of respondents say they use a third party for guidance on their multi-jurisdictional privacy responsibilities; 38% have sought external support on privacy awareness training. But in other areas, outsourcing is rare – just 28% of US businesses use a third-party provider to help with privacy audits.

The contradiction here is that while so many organizations report skills shortages and difficulties with recruitment, the most common reasons given for not outsourcing are that they have all the expertise they need in-house (64% of respondents say this) or that they want to develop their in-house expertise (57%).

It's also a concern that almost half of respondents (47%) say they are choosing not to make greater use of outsourcing because previous experiences with third-party providers have proved disappointing.

While in other areas of compliance, it is common for a Chief Risk Officer to understand their responsibilities as beginning with risk identification and to seek outside input that highlights these unchecked risks, the relative immaturity of privacy as a compliance activity sometimes means that a Chief Privacy Officer sees themselves as directly responsible for the risks that they manage and therefore uncomfortable in the face of external scrutiny.

Third-party advisors and consultants often present the challenge, rather than provide an out-of-the-box solution. Privacy teams in many organizations are not yet at a stage where that feels like a constructive process.



One in three organizations report lacking the expertise they need in-house.

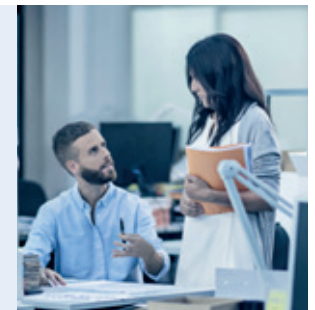
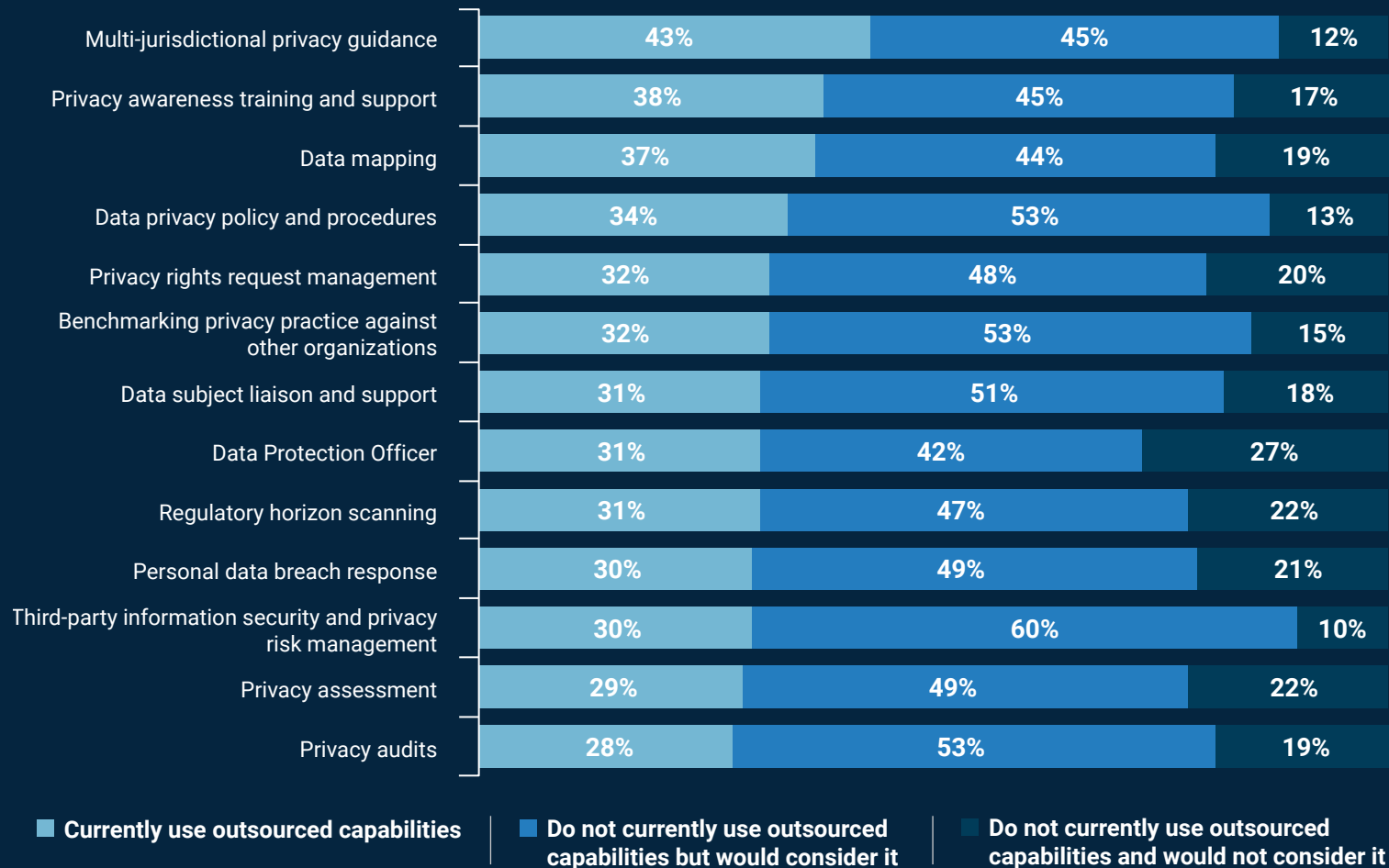


FIGURE 09

The role of outsourced providers remains limited

? Does your organization currently use outsourced capabilities for each of the following functions? If not, would you consider using outsourced capabilities in future?
(% of respondents)



60%

of US organizations
do not use outsourced
capabilities for third
party information
security and risk
management



US businesses stress the importance of minimizing risk but fail to set out opportunities such as securing competitive differentiation.

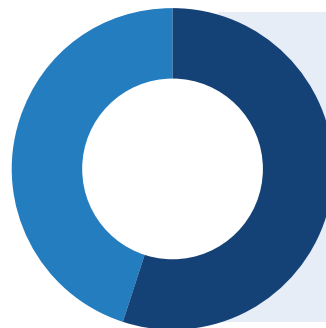
Building the business case

Another explanation for the relatively low penetration of outsourcing in privacy management is a lack of resources. More than half of respondents (55%) say they lack the budget for outsourcing privacy support.

This emphasizes a broader problem. As Figure 7 shows, making the business case for investment in privacy can be difficult: 29% of respondents cited this as a barrier to progress, the third most common obstacle cited. Almost as many (25%) warned that a lack of executive support for privacy was holding them back.


Privacy leaders will need to confront this challenge head on if they are to win backing and approval for the investments in operational improvements that are now required. The key is to set out a broader case for investment.

As we saw earlier, US businesses see a wide range of potential benefits from more effective privacy management. But too few of them are building all these benefits into their business cases – they stress the importance of minimizing risk but fail to set out opportunities such as securing competitive differentiation, increasing the value extracted from data, and achieving their ESG goals. Making that case more clearly will help privacy leaders secure resources and executive support.



Just over half of organizations polled report lacking the budget for outsourcing privacy support.



A woman with blonde hair, wearing glasses and a blue button-down shirt with a pearl necklace, is seated at a desk. She is holding a tablet and looking at it intently. In the background, another person is partially visible, and the office environment is softly blurred. The overall lighting is cool and professional.

Better privacy management increases competitive advantage, reduces risk and builds trust.

Recommendations

Our research sets out both a challenge and an opportunity for US businesses to focus on privacy governance and operations.

Amid increasing risk, the continuing evolution of regulation, and the rapid advance of AI, there is now an urgent need to improve the maturity of privacy management. In some cases, that will require organizations to reconsider their current high levels of confidence in their privacy capabilities.

The prize for taking action is considerable. Businesses that successfully improve their privacy management can look forward to unlocking benefits including increased competitive advantage, reduced risk, and enhanced trust with key stakeholders.

Our research suggests US businesses now need to:

01

Focus on holistic privacy management

Build governance structures with executive-level accountability and cross-functional input. Don't make the mistake of leaving privacy management and compliance to a single function, such as risk management or IT.

**02**

Expand privacy operations to secure compliance and trust

Use exercises such as privacy audits and benchmarking exercises to identify operational shortcomings; close the gaps to ensure the business meets the demands of regulators in its key jurisdictions and to win the trust of customers and employees.

**03**

Benchmark your privacy program

Understand where you sit against best practice to identify areas for future improvement. Seek outside input to ensure you set your privacy program in a global context.



04

Eliminate vulnerabilities in the supply chain

Minimize privacy risks in the supply chain by regularly reviewing existing suppliers' governance measures, and with careful due diligence and onboarding for new providers. This is especially important with suppliers that move customer and other data across jurisdictions.



05

Develop a future-ready approach to data

Improve data protection by looking again at how the whole organization uses data – what is required to minimize risk, maximize customer appeal, and drive efficiency and innovation? Look at data through the prism of AI initiatives to come.



06

Build the business case for investment

Identify the benefits that your organization stands to gain from investment in privacy management, including both value drivers, such as improved consumer relationships and employee engagement, and the reduction of cyber and legal risk. Secure executive support for a more mature approach to privacy.



07

Embrace outsourcing and specialist support

Use expert advisors to help you to close the gaps in specialist areas such as third-party risk management, managing international transfers of data and privacy rights management. Consider where to find specialist support to overcome in-house skills shortages and recruitment challenges.



About Securys

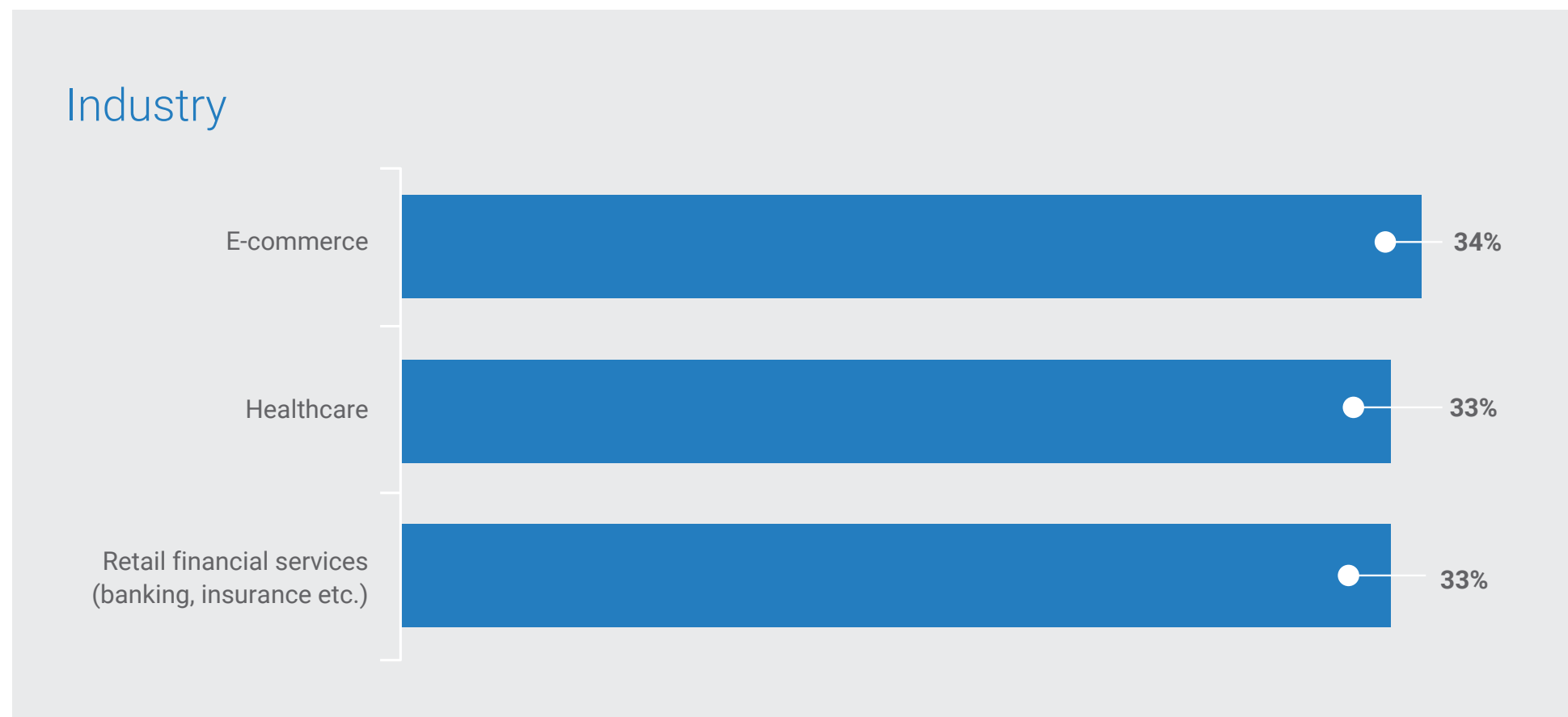
As a market-leading firm, with a large and diverse team of privacy and AI professionals working from multiple offices around the world, Securys brings more than a decade of successful delivery of data governance programs to enterprise clients.

Working across borders and in complex ecosystems with multiple data-sharing partners means we have the knowledge, experience, and toolsets to help US companies navigate both the domestic and international privacy landscape, responding to current challenges and preparing for the future evolution of regulation and technology.

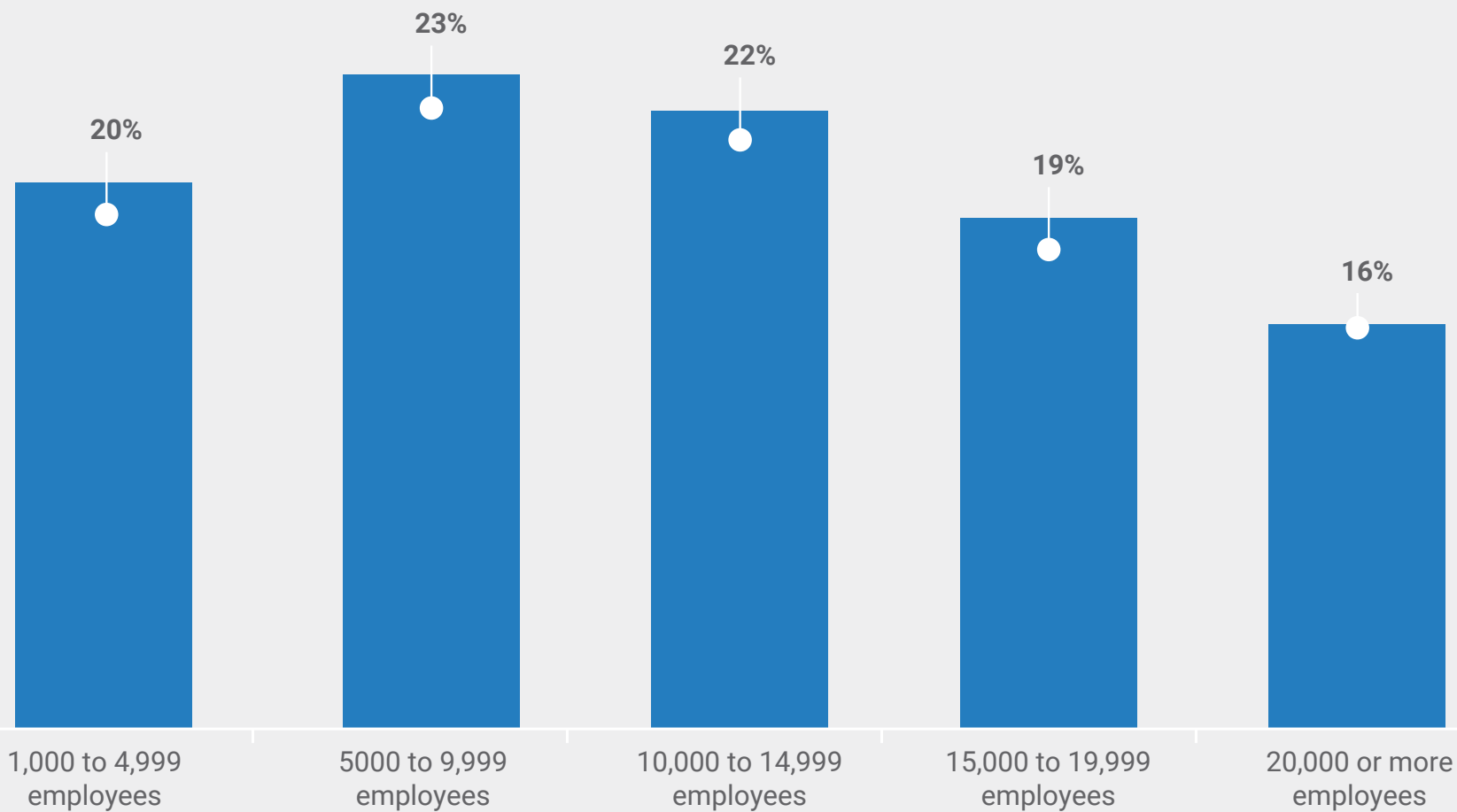


Methodology

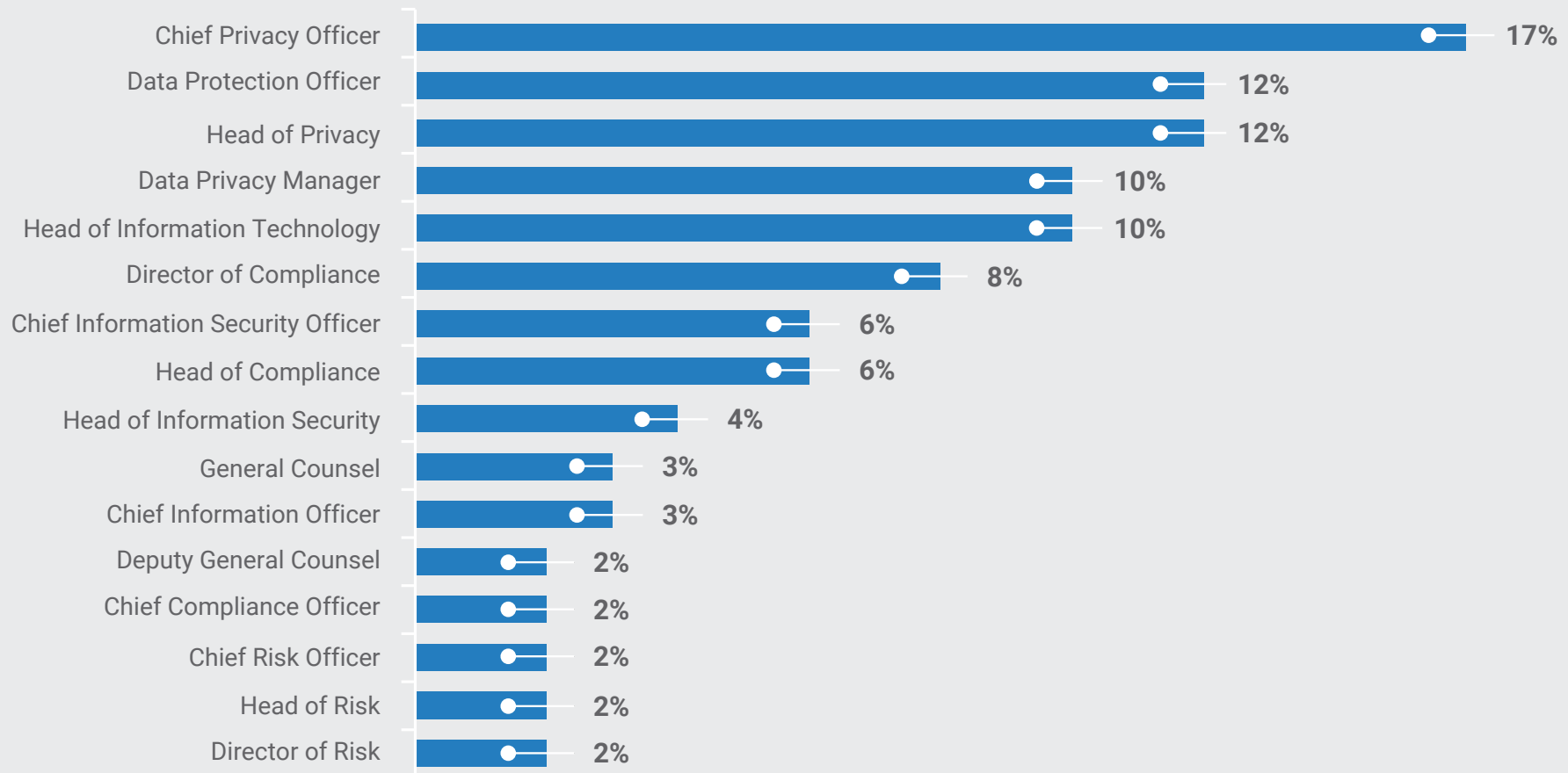
In September 2024, Securys interviewed 100 executives with responsibility for privacy compliance at US businesses. The profile of respondents is as follows:

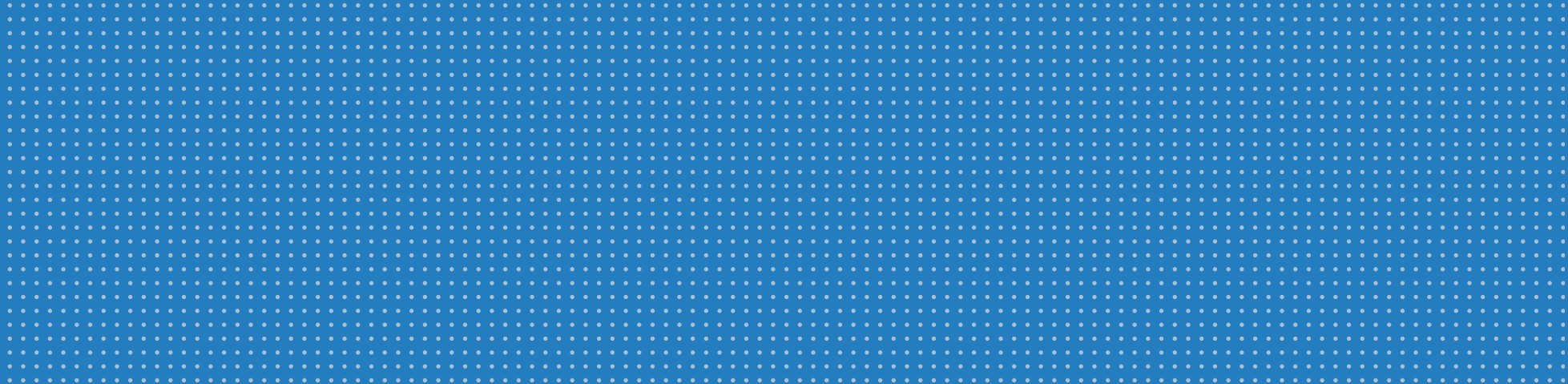


Company size



Job title





A global presence, locally delivered

Headquartered in London – with offices in Europe, the Caribbean and the US – we have practical on-the-ground experience in most of the world's privacy regimes with our team of international experts operating across dozens of jurisdictions.

United Kingdom

4th Floor
91 Goswell Road
London
EC1V 7EX

USA

Trust Center
1209 Orange Street
Wilmington
Delaware 19801
United States

Europe

28 Upper Fitzwilliam Street
Dublin 2
Ireland

Caribbean

Jamaica
9th Floor
Pan-Jam Building
60 Knutsford Boulevard
Kingston
Jamaica W1

Saint Lucia
20 Micoud Street
Castries
Saint Lucia, W.I.