

State of Privacy 2026



CONTENTS

4	Executive Summary
	4 / Key Findings
4	Survey Methodology
5	Staffing
	7 / Open Positions and Hiring
	9 / Skill Gaps
	10 / Retention
11	Privacy Operations
	11 / Accountability and Board Support
	13 / Monitoring Privacy Programs
	14 / Obstacles
	15 / AI and Privacy
16	Budgets
19	Privacy Awareness Training
21	Privacy Breaches
22	Privacy by Design
24	Conclusion
25	Acknowledgments

ABSTRACT

State of Privacy 2026 reports the results of the ISACA global State of Privacy survey conducted late in the third quarter of 2025. This report focuses on privacy staffing, operations, and budgets; privacy awareness training; privacy breaches; and privacy by design. *State of Privacy 2026* also explores how privacy professionals are adopting artificial intelligence (AI) and criteria that make it easier to adopt AI for privacy tasks. Many of the survey findings are consistent with last year's survey results, but this year's results show that challenges related to budget cuts and staffing have worsened.

Executive Summary

State of Privacy 2026 explores trends in privacy staffing, operations, budgets, and breaches; privacy awareness training; and privacy by design. This report also explores the ways in which privacy professionals are using artificial intelligence (AI) tools as well as some factors that may facilitate the adoption of AI technologies. These results are based on the sixth annual ISACA global State of Privacy survey that was conducted in September 2025.

Many regions and sectors have privacy laws and regulations with which enterprises must comply. With the proliferation of Internet of Things (IoT) devices and AI-powered devices, privacy is a key concern for many consumers—these technologies can collect and use massive amounts of personal data. Privacy teams play a vital role in protecting personal data and establishing their enterprises as trustworthy to current and potential customers.

Key Findings

This year's survey results have important insights for privacy professionals:

- Privacy teams are shrinking. The median privacy staff size of survey respondents is five, down from eight last year.
- Understaffing findings are consistent with last year's findings. Technical privacy roles are more understaffed than legal/compliance roles, similar to previous years' results.
- Technical privacy roles are slightly more likely to have increased demand in the next year compared to legal/compliance roles.

- Many privacy professionals feel that their roles are more stressful now compared to five years ago. The rapid evolution of technology is cited as the number one stressor, up eight percentage points from last year.
- Although the majority of survey respondents regularly practice privacy by design when building new applications or services, the percentage of respondents who always or frequently practice privacy by design is down slightly from last year.
- Expert-level privacy professionals are the most challenging to hire, followed by practitioners, then entry-level/foundational privacy professionals.
- Organizational fit is the most important factor in determining a candidate's qualification for a privacy role, followed by prior hands-on experience in a privacy role and adaptability. (Organizational fit and adaptability were new options included in this year's survey.)
- Fewer than half of survey respondents are very or completely confident in their privacy team's ability to achieve compliance with new privacy laws and regulations.
- Survey respondents identify lack of training or poor training as the most common privacy failure (51%, compared to 47% last year). The second most common failure is not practicing privacy by design, followed by data breaches/leakage.
- Budget optimism has waned. Less than a quarter of respondents expect their privacy budgets to increase in the next year, while half of respondents anticipate a decrease in their privacy budgets in the next 12 months.

Survey Methodology

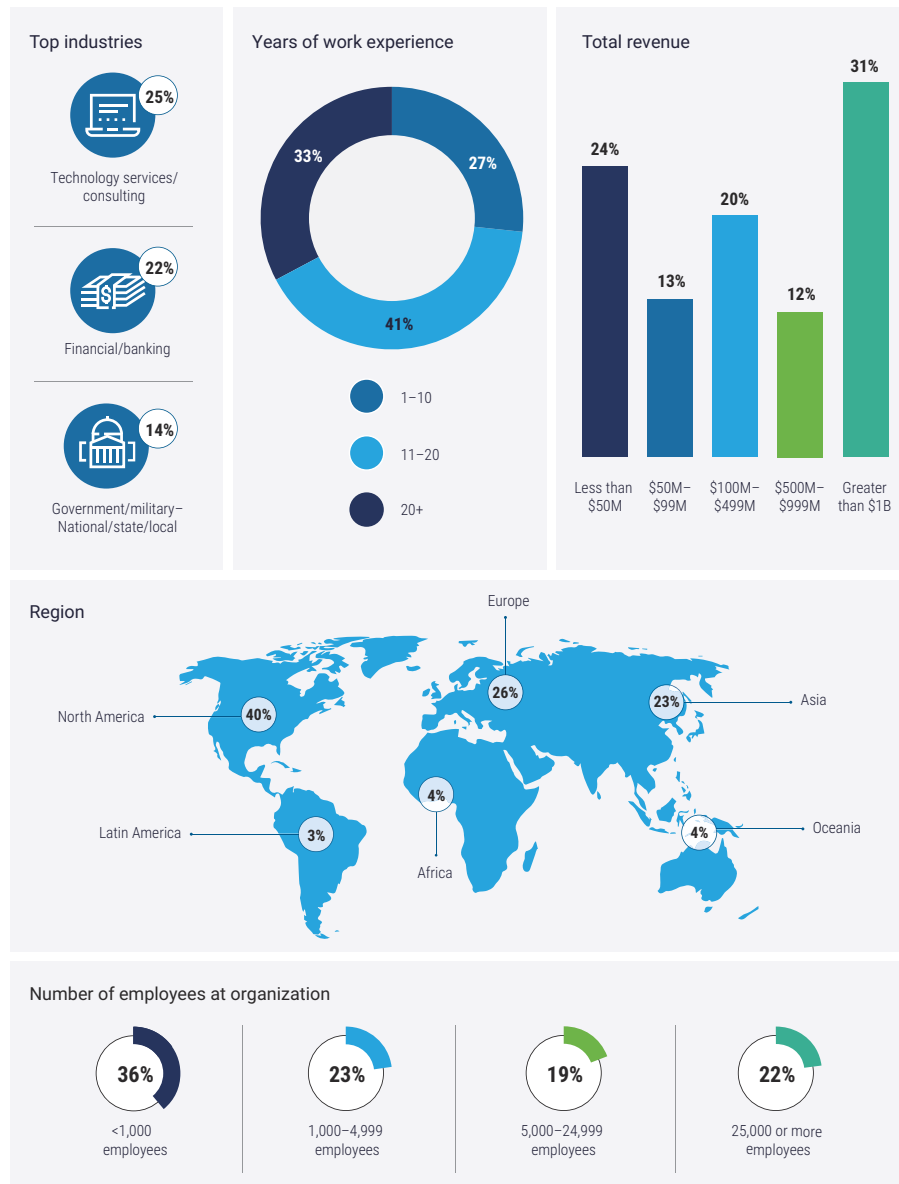
In September 2025, ISACA sent survey invitations to approximately 47,600 ISACA constituents who held the Certified Data Privacy Solutions Engineer™ (CDPSE™) designation and/or the ISACA Certified Information

Security Manager® (CISM®) designation or had "privacy" or "data protection" in their job titles. More than 1,800 people completed the survey.

Respondents held a variety of roles: 39% were in management roles, 28% were in senior leadership roles, 22% were individual contributors, and 11% were in executive leadership positions. Thirty-five percent of

survey respondents were IT practitioners, 11% were data privacy officers (DPOs), and 9% were legal/compliance practitioners. **Figure 1** shows additional demographic information about survey respondents.

FIGURE 1: Respondent Demographics



Staffing

The median privacy staff size declined considerably from last year. In 2025, the median privacy staff size was eight; this year, that number fell to five. Eleven percent of

total respondents said that only one full-time equivalent individual works on privacy in their enterprise. There was some regional variation: 22% of respondents in

Oceania, 19% of respondents in Latin America, and 15% of respondents in Europe only have one full-time privacy employee in their enterprise.

Figure 2 shows the adequacy of staffing for legal/compliance privacy teams, and **figure 3** shows the adequacy of staffing for technical privacy teams. Legal/compliance professionals have training in the law

and the ability to understand an organization's legal obligations. Technical privacy professionals have the technical knowledge to implement controls that can help achieve compliance requirements or other privacy objectives.

Perceptions of understaffing were similar to last year's survey results.

FIGURE 2: Legal/Compliance Privacy Staffing

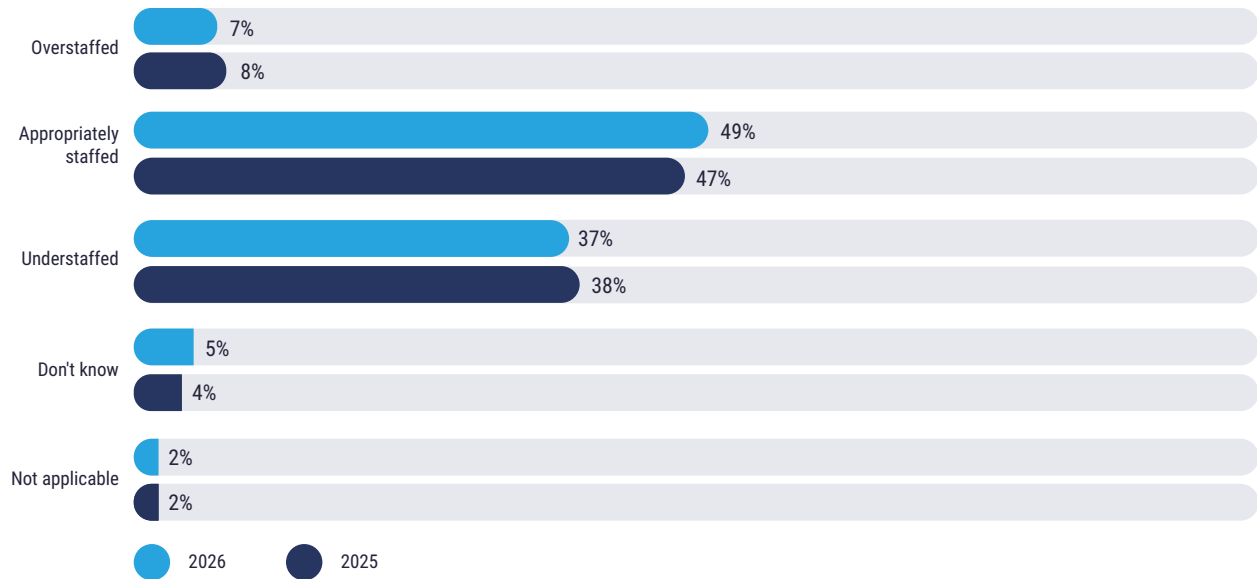
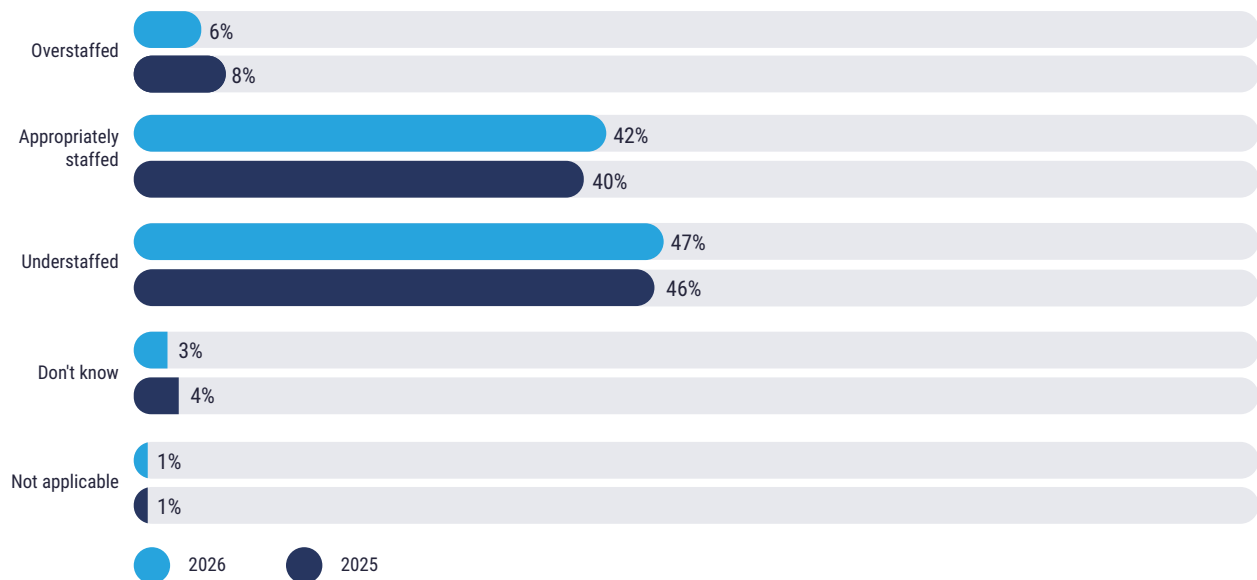


FIGURE 3: Technical Privacy Staffing



Open Positions and Hiring

This year, 19% of survey respondents said they had open legal/compliance privacy positions (which is a decrease from 22% last year), and 26% said they had unfilled technical privacy positions (down from 29% in 2025).

Seventeen percent of respondents said it took more than six months to fill open legal/compliance privacy positions, compared to 19% in 2025, while 18% said it took more than six months to fill open technical privacy positions (also compared to 19% last year).

Survey respondents reported that the speed of filling open privacy roles remains unchanged from last year. This year, 16% of respondents indicated the speed to fill open

legal/compliance privacy roles increased in the past year, which is identical to the 2025 findings. Thirty-nine percent of respondents said that the speed stayed the same (compared to 35% last year), while 9% felt that the speed decreased (compared to 12% last year). For technical privacy roles, 18% of respondents in 2026 indicated that the speed of filling these roles increased, which is also identical to last year's findings. Thirty-nine percent of respondents said that the speed stayed the same (up from 36% last year). Finally, 10% of respondents felt that the speed of filling technical privacy roles decreased, compared to 11% in 2025's survey.

Figures 4 and 5 show the percentage of candidates who were qualified for the positions to which they applied.

FIGURE 4: Legal/Compliance Privacy Candidates' Qualification

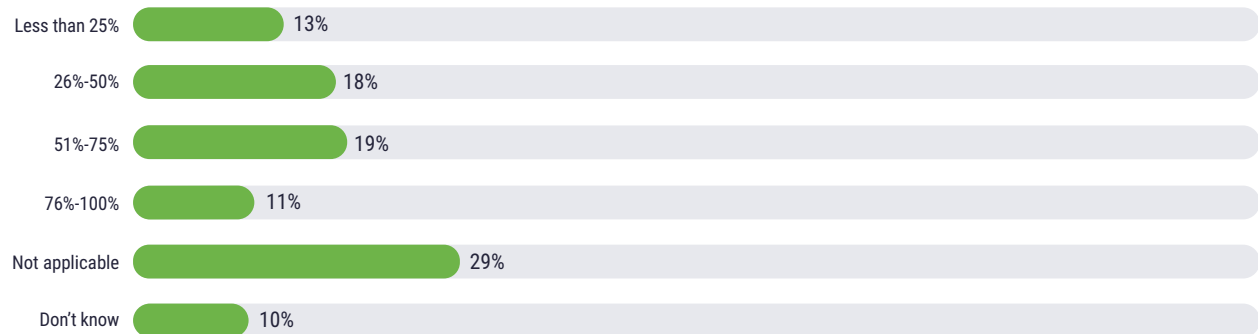


FIGURE 5: Technical Privacy Candidates' Qualification



Survey respondents identified the following factors as very important in determining if a privacy candidate was qualified:

- Organizational fit, e.g., culture (59%)
- Prior hands-on experience in privacy role (57%)
- Adaptability (56%)
- Compliance/legal experience (51%)
- Technical experience (48%)
- Credentials held (35%)
- Completion of hands-on training courses in privacy (35%)
- University degree (24%)
- Recommendation from previous employer (19%)
- Networking (19%)

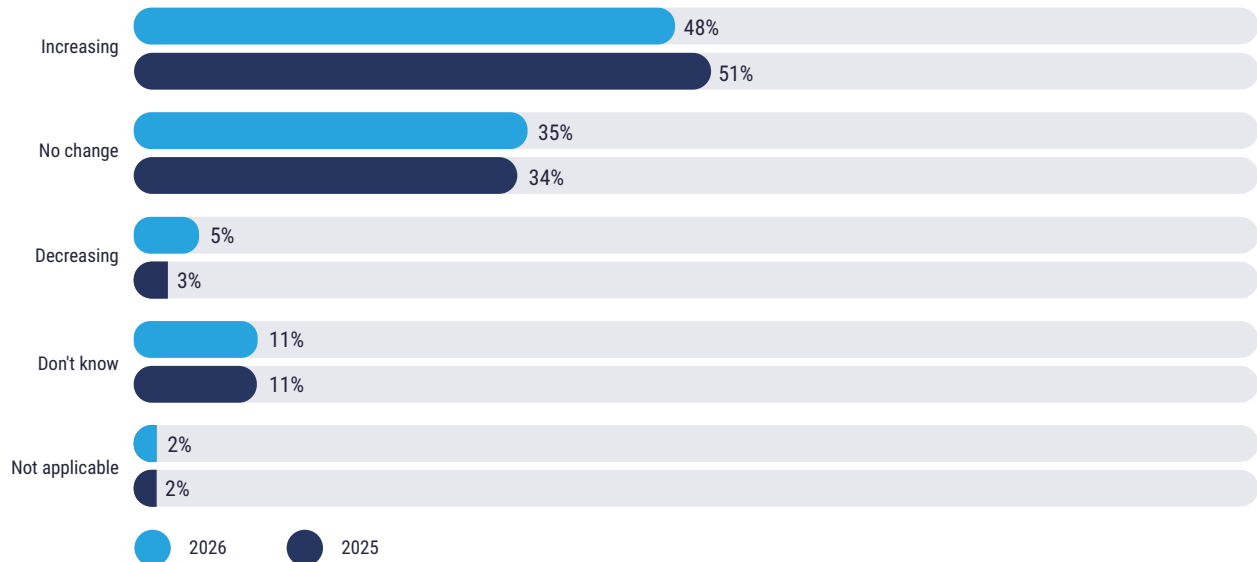
Organizational fit, a new factor added to this year's survey, surpassed last year's top factor: prior hands-on experience in a privacy role. Adaptability, also new this year, was the third most selected factor identified as being very important.

Given the high value of prior hands-on expertise, it is not surprising that a majority of respondents found it challenging to hire experienced privacy professionals. Fifty-seven percent of respondents said that expert-level privacy practitioners were most difficult to hire, followed by practitioners (25%) and entry-level/foundational personnel (4%).¹

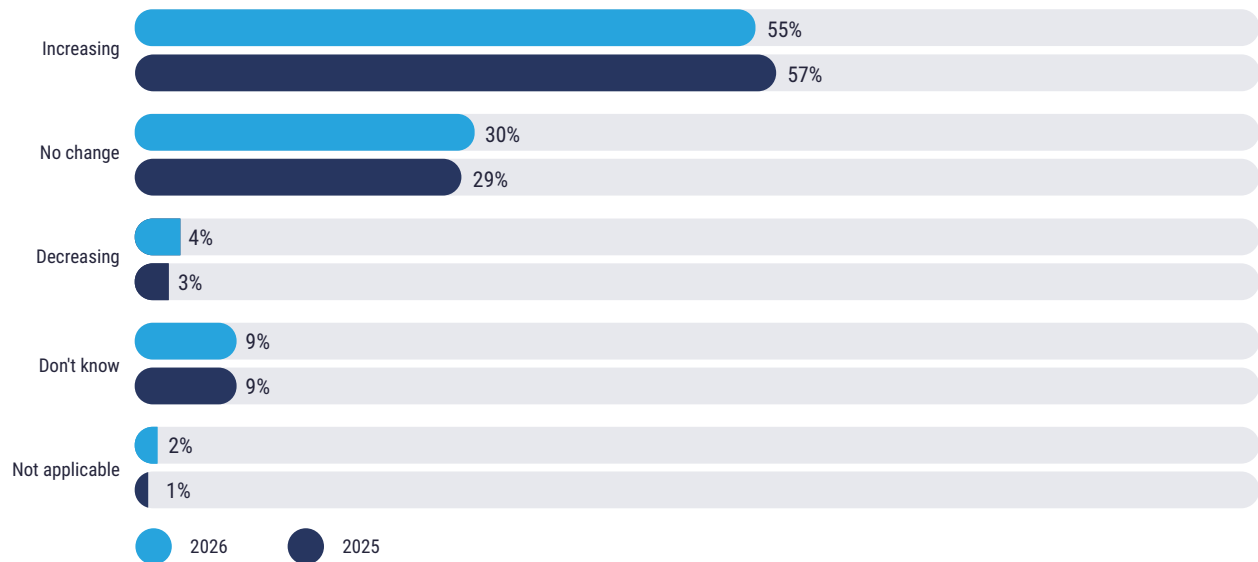
Given the high value of prior hands-on expertise, it is not surprising that a majority of respondents found it challenging to hire experienced privacy professionals.

Figures 6 and 7 show the anticipated demand for privacy roles. Although many respondents believed that the demand for privacy roles will increase in the next year, the percentage that anticipate an uptick in demand decreased slightly from 2025.

FIGURE 6: Demand for Legal/Compliance Privacy Roles



¹ Fourteen percent of respondents said that they were not sure which level was the most difficult to hire.

FIGURE 7: Demand for Technical Privacy Roles

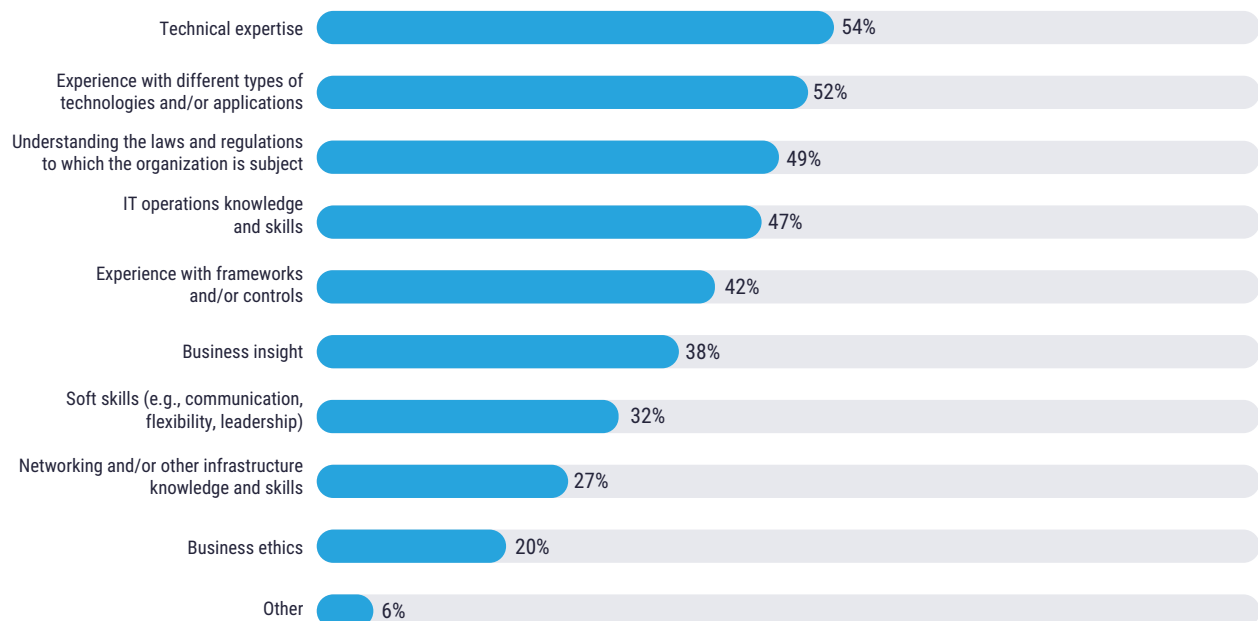
Skill Gaps

More than half (53%) of survey respondents said they were aware of skill gaps in today's privacy professionals.

Figure 8 shows the areas in which respondents saw the biggest skill gaps.

The top three strategies to combat these skill gaps include:

- Training to allow nonprivacy staff, who are interested, to move into privacy roles (48%)
- Increased usage of contract employees or outside consultants (36%)
- Increased reliance on AI or automation (34%)

FIGURE 8: Skill Gaps

Retention

Only 35% of respondents indicated that they had challenges retaining qualified privacy professionals, but this percentage varied based on region. Forty-five percent of respondents in Latin America and 50% of respondents in Asia said they had challenges retaining qualified privacy professionals. Note that only 3% of survey respondents were in Latin America, but retention challenges were also identified by Latin American respondents to ISACA's 2025 State of Cybersecurity survey,² suggesting that this region's job market may make retention more challenging.

Enterprises whose privacy strategies are not aligned with broader enterprise goals may have more retention challenges. Nearly half (49%) of respondents who said that their enterprise privacy strategy did not align with other organizational objectives said that they had retention issues. And those who are not so confident or not at all confident in their privacy team's ability to achieve compliance with new privacy laws and regulations had similar challenges—50% said their organizations struggled to retain qualified privacy professionals.

Retention challenges also increased (to 51%) for those who experienced a material privacy breach in the past 12 months. Of those respondents who said their enterprises

did not experience a privacy breach in the past 12 months, only 33% had retention challenges. Responding to a privacy breach and navigating its consequences, e.g., fines and reputational damage, can be challenging for privacy teams. Therefore, it is not surprising that enterprises that have experienced privacy breaches have had retention problems.

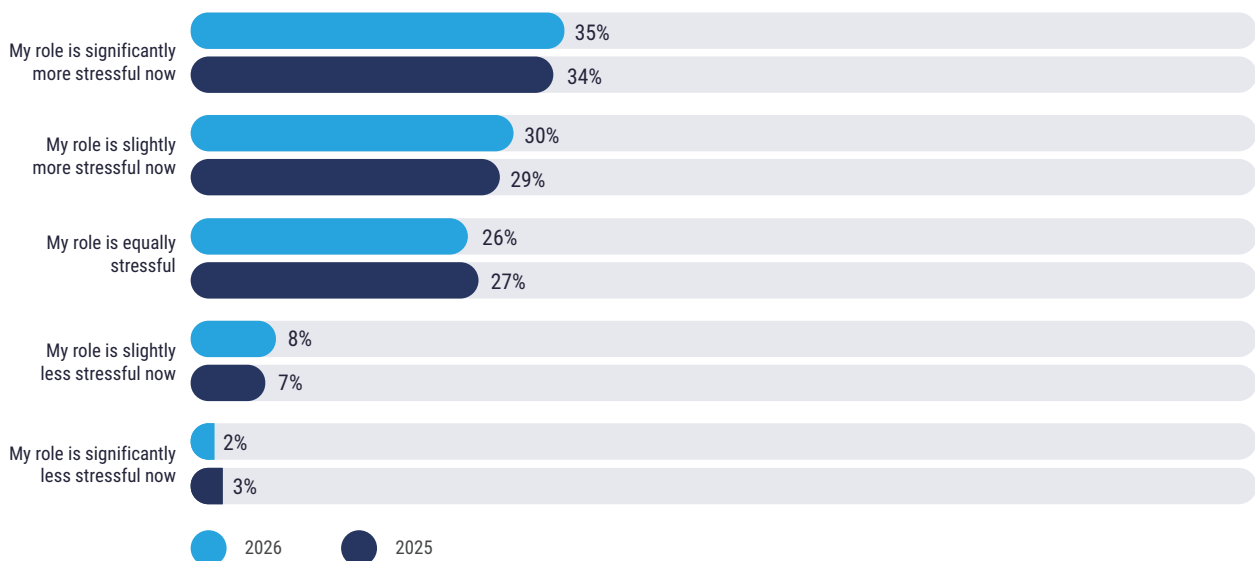
Stress

A majority of respondents said they find their roles more stressful now than five years ago, which is slightly higher than in 2025. **Figure 9** compares this year's findings to last year's. Of respondents in enterprises with significantly or somewhat underfunded privacy budgets, 46% said their role is significantly more stressful now, which suggests a correlation between resources and on-the-job stress.

Survey respondents said that their roles were more stressful due to the following reasons:

- Technology's rapid evolution (71%, up from 63% in 2025)
- Compliance challenges (62%, up from 61% in 2025)
- Resource shortages (61%, up from 59% in 2025)
- Competing priorities (56%, up from 50% in 2025)

FIGURE 9: Job Stress



² ISACA, *State of Cybersecurity 2025*, 29 September 2025, www.isaca.org/resources/reports/state-of-cybersecurity-2025

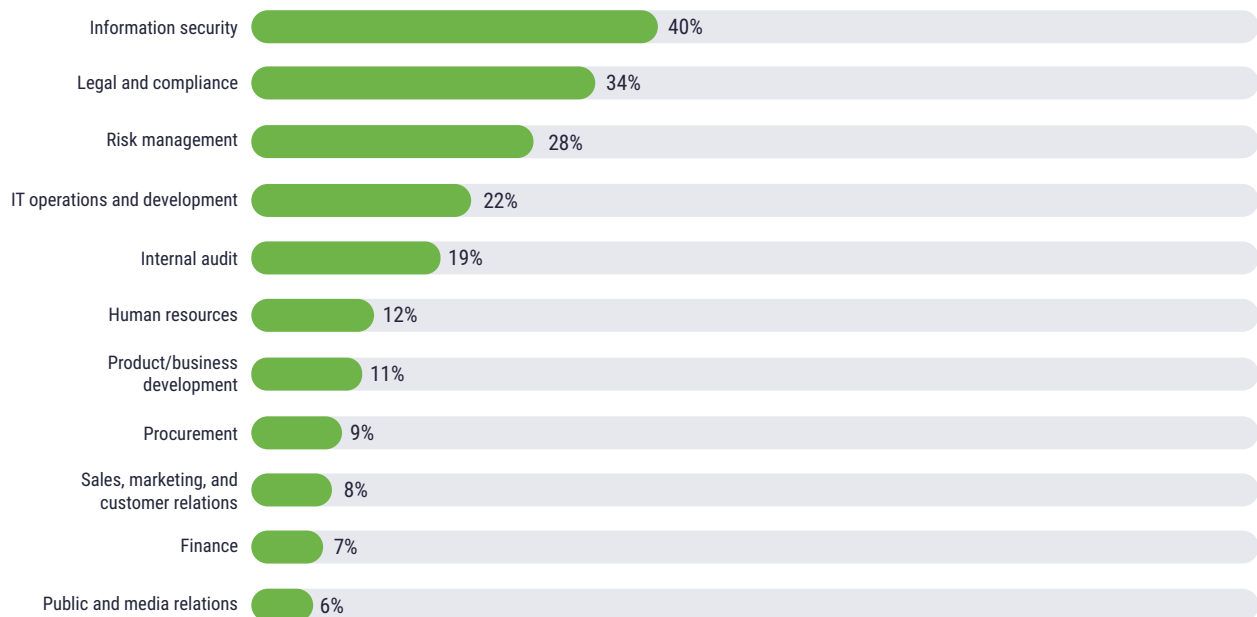
Privacy Operations

Cross-functional collaboration and buy-in for privacy activities are essential to achieving privacy-related goals and compliance requirements. **Figure 10** shows the percentage of respondents who indicated that their privacy office always works with other departments.

Technical privacy professionals and legal/compliance privacy professionals must work closely to ensure the enterprise is compliant with applicable laws

and regulations. Eight percent of respondents said that technical privacy and legal/compliance privacy professionals meet weekly, 17% said they meet monthly, 28% said they meet quarterly, and 23% said they meet one-to-two times per year. Concerningly, 7% said that they never meet. The remaining 16% said that technical privacy and legal/compliance privacy professionals meet when new privacy laws or regulations go into effect.

FIGURE 10: Privacy Department Collaboration



Accountability and Board Support

This year, the role most likely to be accountable for privacy within enterprises was the chief privacy officer (CPO). Twenty-two percent of respondents said the CPO was accountable for privacy, 14% said the chief information officer (CIO) was accountable, and 13% said that an executive-level security officer was accountable. But some enterprises do not have a CPO; organizations with smaller staff sizes were less likely to have a CPO —only 12% of respondents at organizations with fewer

than 250 employees said a CPO was accountable for privacy. This percentage jumps to 36% for respondents at organizations with more than 25,000 employees.

A CPO is an important role that can advocate for privacy teams and initiatives. Respondents whose organizations had a CPO accountable for privacy were more likely to feel that their board of directors adequately prioritized privacy and more likely to feel that the privacy strategy aligned with organizational objectives. Respondents with a CPO were also more likely to feel completely or very confident in their organization's ability to ensure data compliance.

A majority of respondents (56%) said their board of directors adequately prioritized privacy. Board support for privacy is imperative to the success of privacy operations and is positively correlated with:

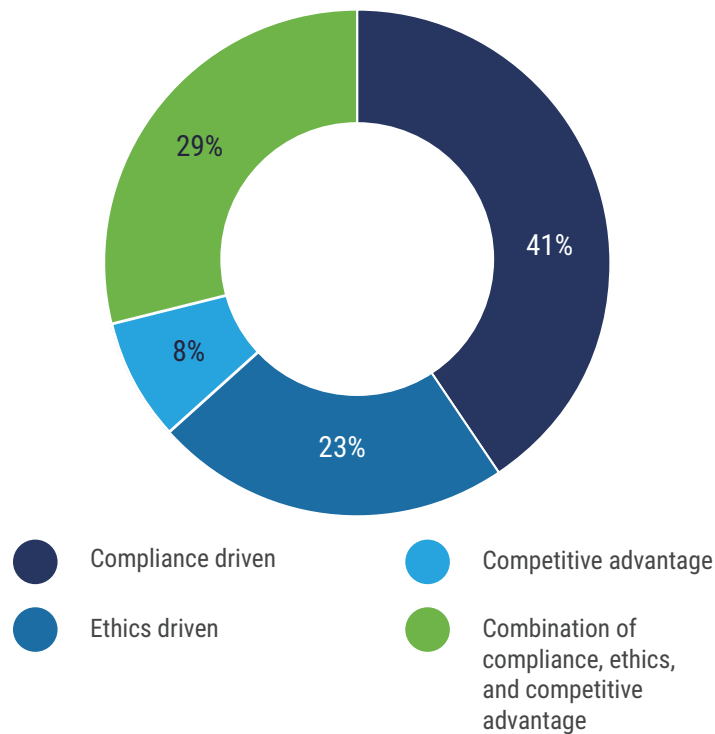
- Frequently practicing privacy by design
- Confidence in ensuring privacy and compliance objectives
- Adequate privacy budget funding

Figure 11 shows the ways boards of directors view privacy programs. Although privacy compliance requirements are top-of-mind for many enterprises, a pure compliance approach to privacy is correlated with numerous challenges. Of respondents who said their privacy strategy is not aligned with enterprise objectives, 67% said their boards view privacy programs as compliance driven. Compliance requirements are rapidly shifting and are not necessarily meant to align with enterprise objectives; therefore, a compliance-driven approach to privacy can present challenges for privacy teams whose objectives are at odds with broader organizational priorities.

Paradoxically, respondents in enterprises with a purely compliance-driven approach to privacy were less likely to feel confident in privacy compliance—59% of respondents who were not so confident or not at all confident in their privacy team's ability to achieve compliance with new privacy laws and regulations said that their board views privacy programs as compliance driven.

Enterprises with boards that are primarily compliance focused were also less likely to adopt new technology. Of respondents whose organizations have no plans to use AI for privacy tasks, 52% had a board that views privacy programs as predominantly compliance driven. This lower adoption of AI for privacy at these organizations makes sense because laws and regulations likely guide many of the enterprise activities, and AI regulations are still fairly limited and not prescriptive for internal AI use. Therefore, these enterprises likely do not know how to responsibly adopt this technology.

FIGURE 11: Board View of Privacy Programs



Nearly three-quarters (74%) of respondents said their enterprise's privacy strategy is aligned with organizational objectives. This alignment is imperative because it can facilitate enterprisewide buy-in for privacy initiatives and is correlated with more resources. When privacy objectives align with other objectives, any cuts to privacy teams will have widespread ramifications, which may protect these teams from budget cuts.

When privacy objectives align with other objectives, any cuts to privacy teams will have widespread ramifications, which may protect these teams from budget cuts.

Eighty-two percent of respondents said that they used a framework or law/regulation to manage privacy in their organization. The most common laws/regulations and frameworks were:

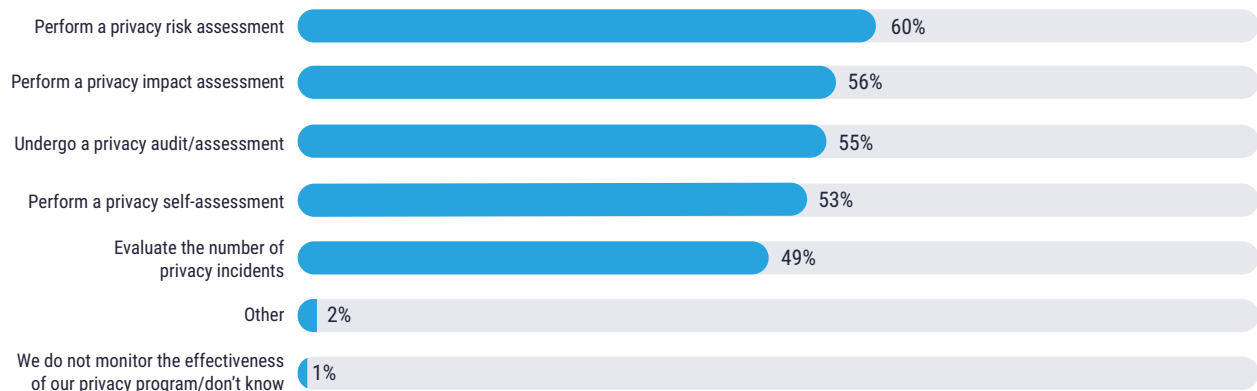
- General Data Protection Regulation (GDPR) 2016/679 (51%)
- US National Institute of Standards and Technology (NIST) Privacy Framework (45%)

- ISO/IEC 27002:2013 *Information technology — Security techniques — Code of practice for information security controls* (33%)
- ISO/IEC 27001:2022 *Information security, cybersecurity and privacy protection — Information security management systems — Requirements* (32%)

Monitoring Privacy Programs

One in five respondents said they do not monitor their privacy programs, which is concerning, as these respondents do not have a way to evaluate their privacy program's progress or identify areas for improvement. Almost half (48%) of respondents who said their board of directors does not adequately prioritize privacy also said that they do not monitor their privacy program, hinting at a lack of oversight or a lack of incentive to monitor privacy programs. **Figure 12** shows the ways in which respondents monitor their privacy programs.

FIGURE 12: Monitoring Privacy Program Effectiveness



Almost one-third (31%) of respondents said their organization finds it easy or very easy to identify and understand its privacy obligations, whereas one-fifth (20%) said it is difficult or very difficult. Forty-six percent of respondents said they are completely or very confident in their privacy team's ability to achieve compliance with new privacy laws and regulations. Forty percent of respondents were somewhat confident, while 10% were not so confident or not at all confident.³

Under certain privacy laws, data subjects have the right to make requests about their data, e.g., deletion and rectification. Thirty-five percent of respondents said the number of data subject requests increased in the past year, 31% said it stayed the same, and only 4% said the number decreased.⁴

³ Five percent of respondents selected "Don't know/prefer not to answer."

⁴ Thirty percent of respondents selected "Don't know."

Obstacles

Almost half (44%) of respondents said their privacy program faced obstacles (figure 13).

Not practicing privacy by design was the second most common privacy failure, with a nine percentage-point increase from last year.

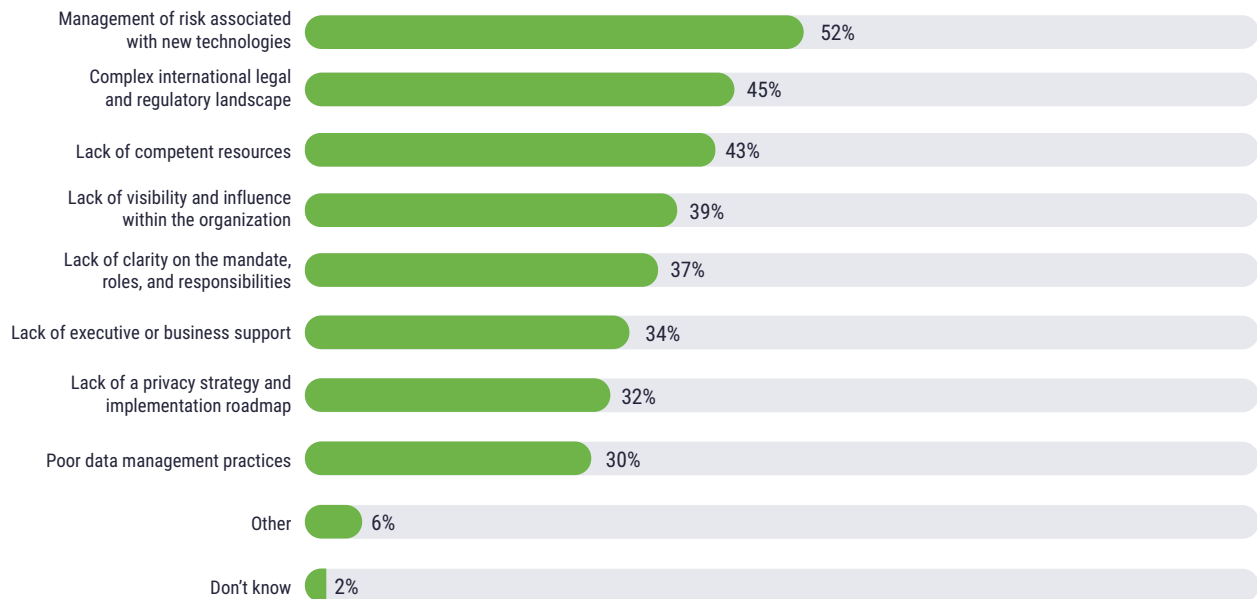
It is possible that, this year, more respondents experienced the consequences of not practicing privacy by design, especially related to AI. Some privacy rights advocates said that AI is at odds with privacy,⁵ but generative AI is the fastest-adopted technology in history.⁶ This rapid adoption, with little or no prioritization of privacy, may have exacerbated the effects of not practicing privacy by design.

It is possible that, this year, more respondents experienced the consequences of not practicing privacy by design, especially related to AI. Some privacy rights advocates said that AI is at odds with privacy, but generative AI is the fastest-adopted technology in history. This rapid adoption, with little or no prioritization of privacy, may have exacerbated the effects of not practicing privacy by design.

Ethical decision making, although lower on the list of common privacy failures, increased five percentage points from last year. This increase may be explained by the growing trend of ethical considerations falling within the purview of privacy departments.⁷

Figure 14 shows the most common privacy failures identified by survey respondents.

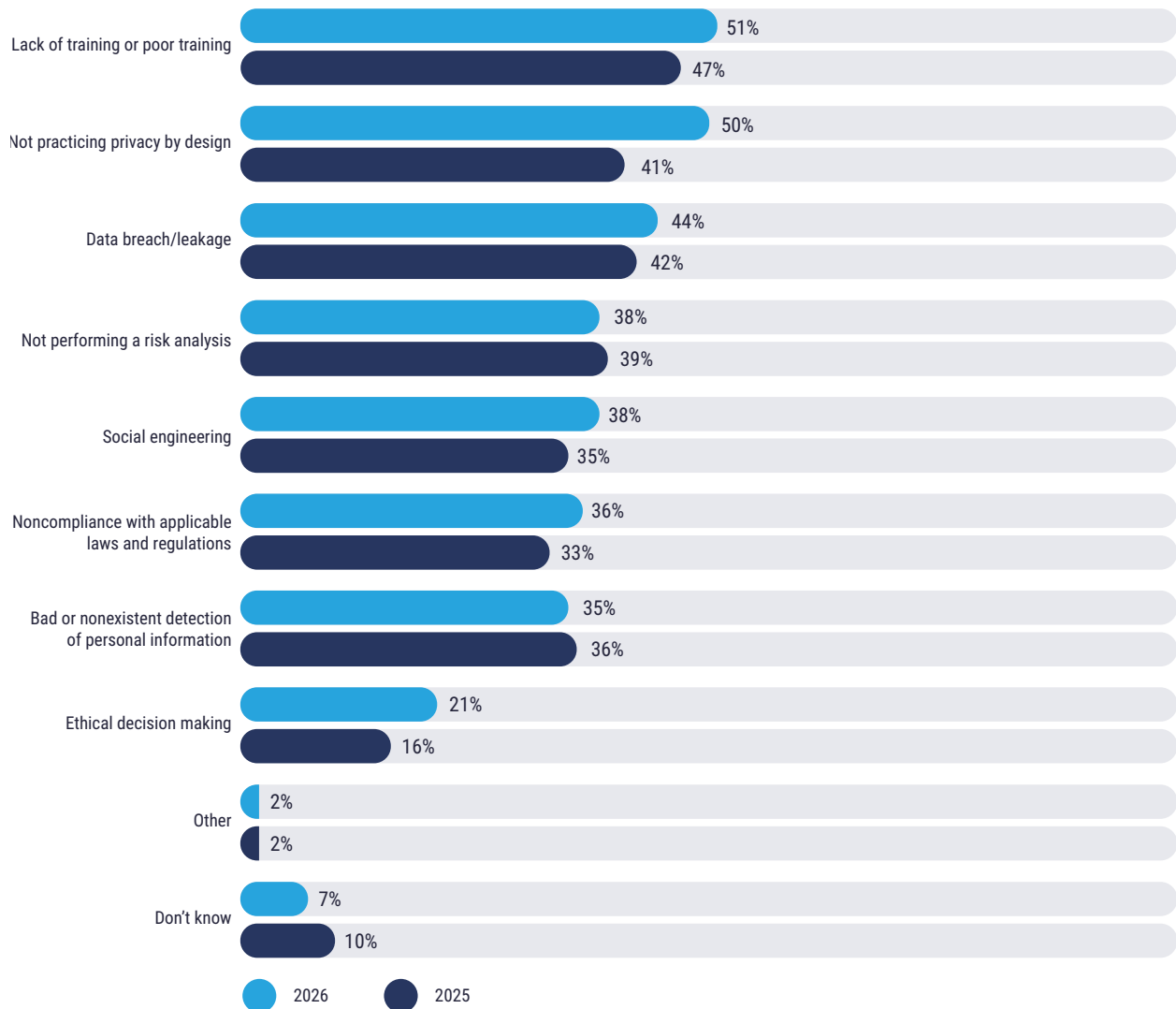
FIGURE 13: Privacy Programs Obstacles



5 Caltrider, J.; "AI is killing privacy. We can't let that happen," Fast Company, 16 November 2025, www.fastcompany.com/91435189/ai-privacy-openai-tracking-apps

6 Wagener, T.; "2025 Survey of Product Impact in the Connected Economy: Artificial Intelligence," CCIA, 18 November 2025, <https://ccianet.org/research/reports/2025-survey-of-product-impact-in-the-connected-economy-artificial-intelligence/>

7 Kazi, S.; "The Evolving Role of the Privacy Professional," ISACA, 21 February 2025, www.isaca.org/resources/news-and-trends/industry-news/2025/the-evolving-role-of-the-privacy-professional

FIGURE 14: Common Privacy Failures

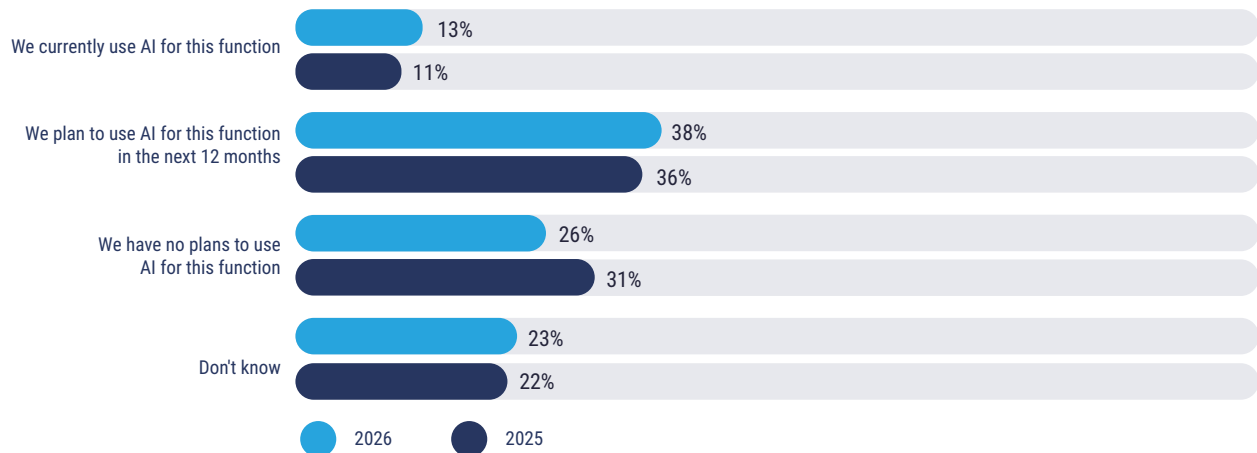
AI and Privacy

Figure 15 shows respondents' plans to use AI for privacy-related tasks. The use of AI may appear low, but some enterprises may have instances of shadow AI⁸ that may not be reflected in the survey results. Additionally, survey respondents may not have considered AI features that have been added to existing products or services.

Mature enterprises with more resources tend to be more likely to adopt AI. Adoption is lower at enterprises with fewer resources and less support for privacy programs:

- Eighteen percent of those whose boards prioritized privacy said they currently use AI for privacy, compared to just 8% of those whose boards do not prioritize privacy.
- Twenty-two percent of respondents who always practice privacy by design said they used AI for privacy-related tasks, compared to just 5% who rarely practice privacy by design and 3% who never practice privacy by design.
- Eighteen percent of respondents working at enterprises with more than US\$1 billion in revenue said they currently use AI for privacy-related tasks, compared to just 10% who work for enterprises with less than US\$50 million in revenue.

8 Maher, S.; "What Is Shadow AI And What Can IT Do About It?," Forbes, 31 October 2023, www.forbes.com/sites/delltechnologies/2023/10/31/what-is-shadow-ai-and-what-can-it-do-about-it/

FIGURE 15: Using AI for Privacy Tasks

These findings suggest that many enterprises understand that AI tools are not without risk and that insufficient resources or prioritization of privacy can be problematic. These correlations also underscore that AI tools, although helpful, are not a panacea for challenges with prioritization or resource shortages.

These findings suggest that many enterprises understand that AI tools are not without risk and that insufficient resources or prioritization of privacy can be problematic. These correlations also underscore that AI tools, although helpful, are not a panacea for challenges with prioritization or resource shortages.

AI adoption appears higher among survey respondents who hold higher-level positions. Sixteen percent of survey respondents in executive leadership positions said they currently use AI, compared to 14% for senior leadership positions and 13% for management roles. Eleven percent of individual contributors currently use AI for privacy-related tasks.

Budgets

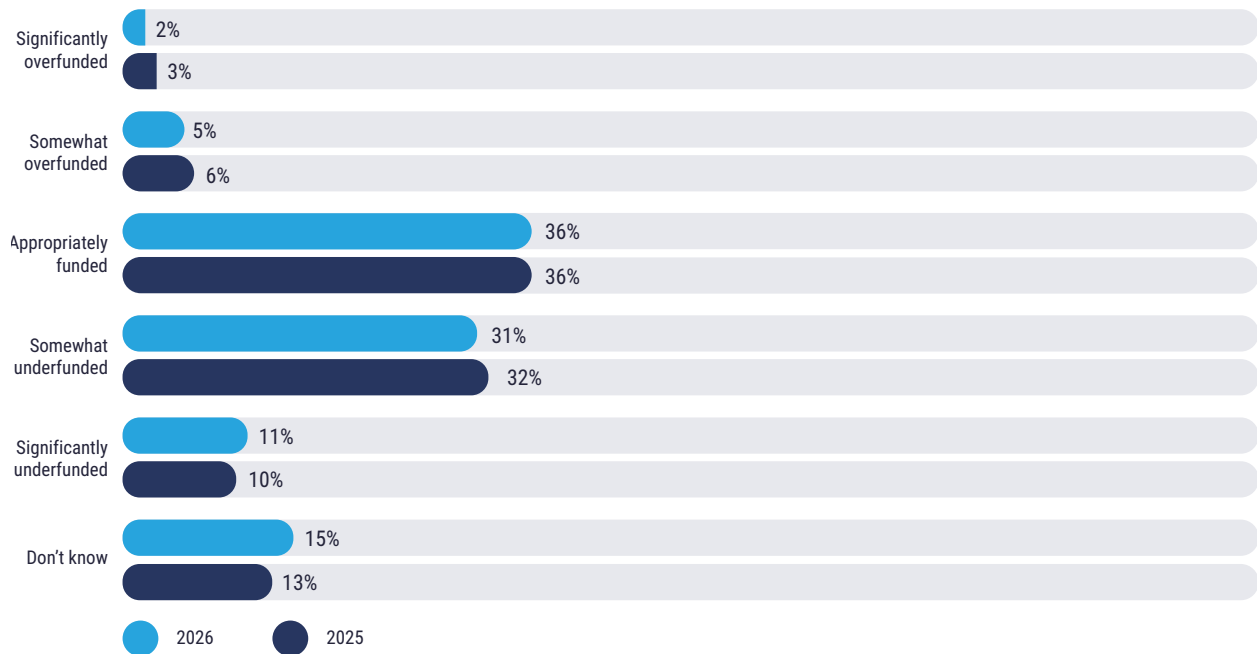
Figure 16 shows respondents' privacy budget perceptions, which are comparable to last year.

In recent years, the State of Privacy survey results related to budget forecasts have been concerning.

Beginning in 2024, there was a sharp increase in respondents who anticipated budget cuts, which was reinforced in 2025 and 2026 (**figure 17**).

The findings in **figure 17** are especially concerning for privacy teams that already feel underfunded. Of survey respondents who said their privacy budget was significantly or somewhat underfunded, 61% said they anticipate their privacy budget to decrease in the next 12 months, indicating that many teams that are currently struggling may face even more budget challenges in the next year.

FIGURE 16: Privacy Budget Perceptions



Consistent with last year, the percentage of respondents whose privacy budget decreased was far lower than those who anticipated a decrease in the previous year. In 2025, 42% of respondents believed that their budget would somewhat decrease in the next year, and 6% believed that it would significantly decrease. In the 2026 survey, only 9% of respondents said their privacy budget somewhat decreased, and 3% said it significantly decreased. Anxiety regarding privacy budget cuts has been high for a few years, but these fears have not yet come to fruition.

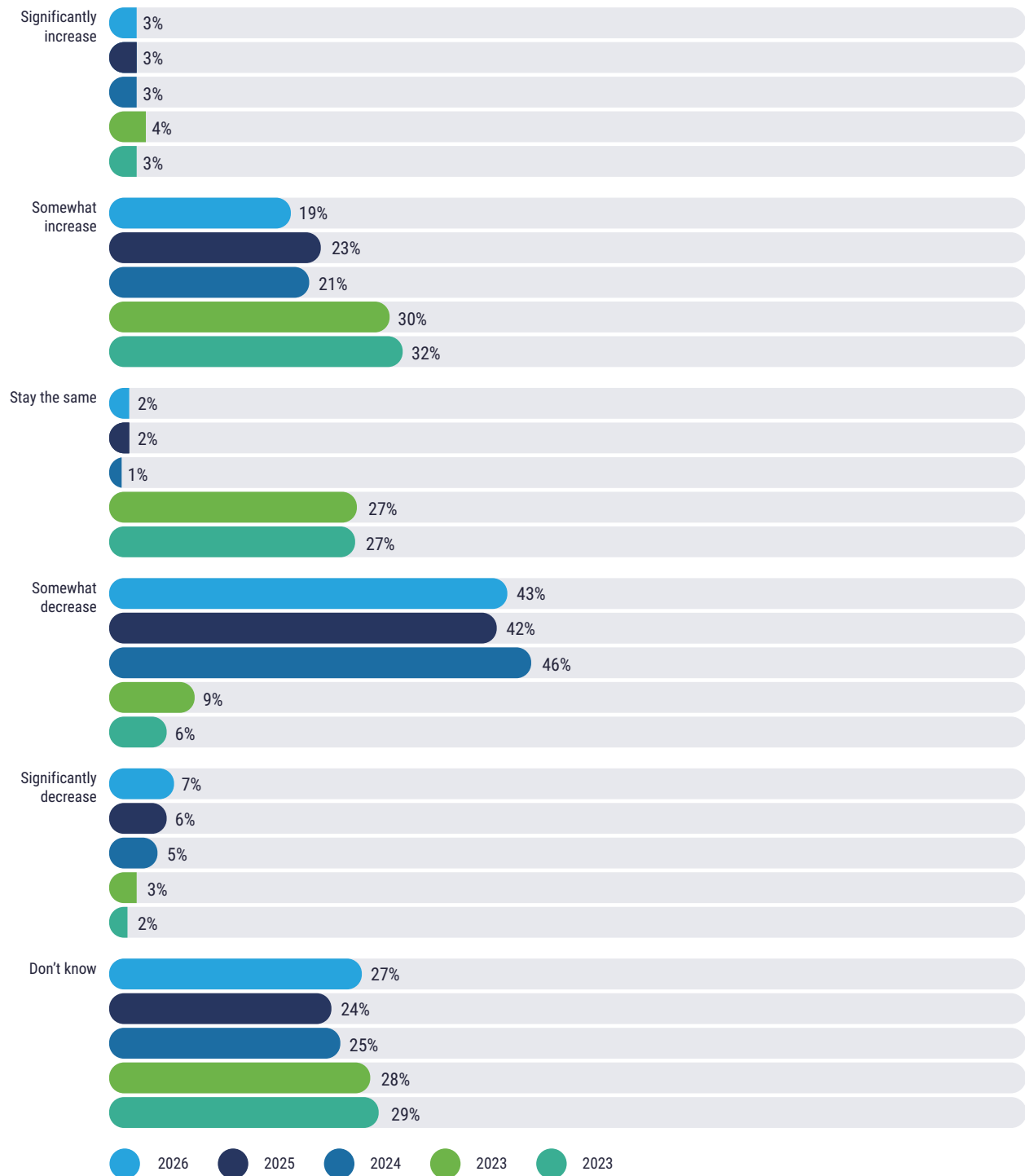
Budget cuts can have serious ramifications for the ability of privacy teams to ensure privacy, which is demonstrated by a correlation between forecasts for budget cuts and confidence in ensuring privacy. Sixty-one percent of respondents who were not so confident or not at all confident in their organization's ability to ensure the privacy of sensitive data believed that their privacy budget will decrease in the next 12 months.

Budget cuts can have serious ramifications for the ability of privacy teams to ensure privacy, which is demonstrated by a correlation between forecasts for budget cuts and confidence in ensuring privacy.

Board support for privacy and privacy alignment with other enterprise goals are correlated with budget increases. Twenty-nine percent of respondents who said their board adequately prioritized privacy said that the privacy budget would increase in the next 12 months, compared to just 14% whose boards did not prioritize privacy.

Of respondents who said their privacy strategy aligned with other enterprise objectives, 26% anticipated an increase in their privacy budget, compared to just 13% of those who said their privacy strategy did not align with organizational objectives. This correlation suggests that privacy alignment with other enterprise objectives may shield these budgets from being cut.

FIGURE 17: Budget Forecasts



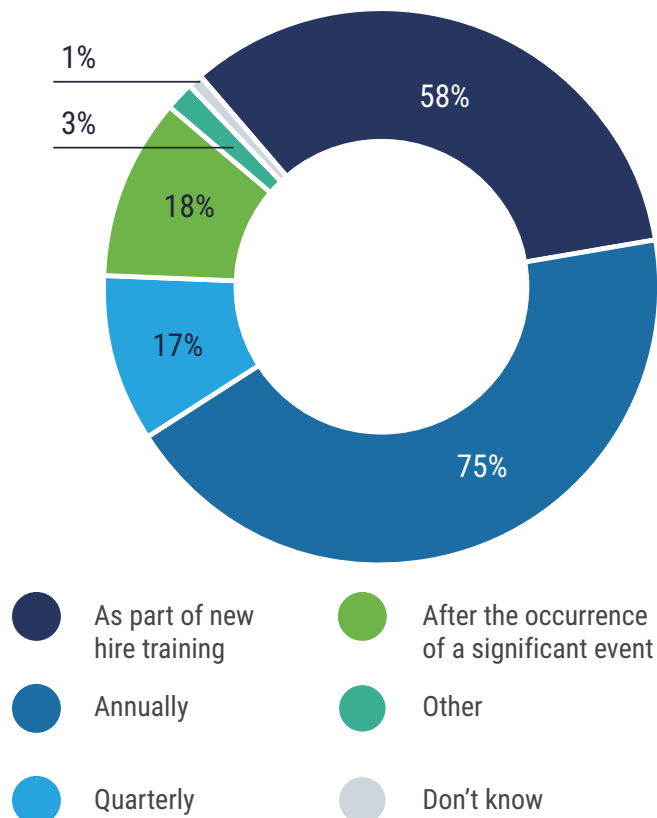
Privacy Awareness Training

Seventy-nine percent of respondents said their organization provides privacy awareness training. **Figure 18** shows when privacy awareness training is provided.

To ensure that training content is up to date and provides value to staff, privacy teams must periodically review privacy awareness training and revise it as appropriate. Twenty-four percent of respondents said they revise training when new laws and regulations go into effect, 66% revise training annually, 8% revise it every two-to-five years, and 2% said they do not revise their privacy awareness training.

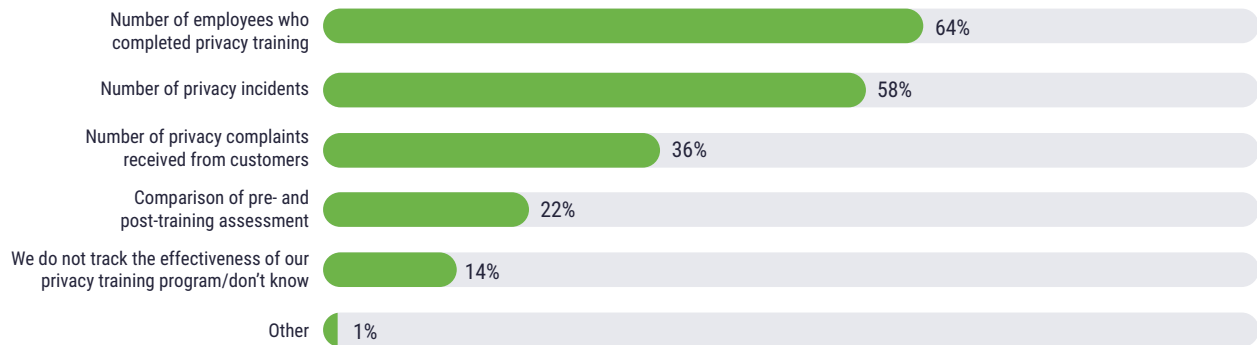
More than two-thirds (68%) of respondents said that privacy awareness training is separate from security awareness training. If security and privacy training are not separate, it is essential to ensure that security training incorporates privacy-specific concepts. Security and privacy are not interchangeable concepts. Security is a privacy prerequisite, but it does not guarantee privacy.

FIGURE 18: Privacy Awareness Training



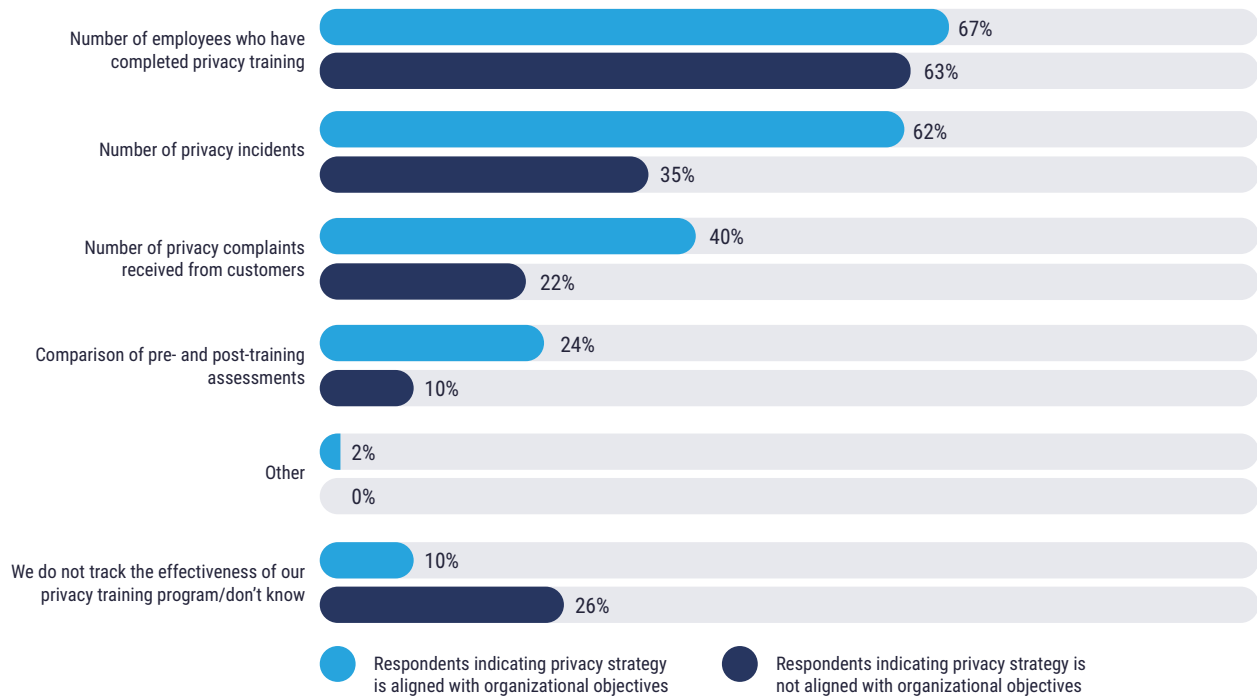
The most common privacy failure identified by survey respondents was a lack of training or poor training. Identifying bad privacy awareness training requires

monitoring and measuring its efficacy. **Figure 19** shows the metrics that respondents tracked to assess privacy training program effectiveness.

FIGURE 19: Evaluating Privacy Awareness Training Effectiveness

Note that using the number of privacy incidents as a measure of training effectiveness can be challenging. If staff are properly educated about what constitutes a privacy incident, the number of privacy incidents can increase, signaling that staff are self-reporting incidents.

Respondents who identified alignment between privacy strategy and other organizational objectives were more likely to use multiple metrics to evaluate the effectiveness of privacy awareness training (**figure 20**), suggesting that having multiple factors is important.

FIGURE 20: Evaluating Privacy Training and Strategy Alignments

Most survey respondents said that privacy awareness training has a positive impact on employee privacy awareness. Twenty-eight percent said that training has a strong positive impact, 54% said it had some positive

impact, 13% said it had little positive impact, 1% said it had no positive impact, and 5% did not know or preferred not to answer.

Privacy Breaches

Figure 21 shows breach trends. Of note are a nine-percentage-point drop in the respondents who said they did not experience a privacy breach in the last 12 months and a two-percentage-point increase in the respondents who indicated their organization experienced a breach.

Six percent of respondents said they are experiencing more breaches as compared to a year ago, 16% said they are experiencing fewer breaches, and 23% said they are experiencing the same number of breaches.⁹ **Figure 22** shows the likelihood of experiencing a privacy breach in the next year.

FIGURE 21: Privacy Breaches

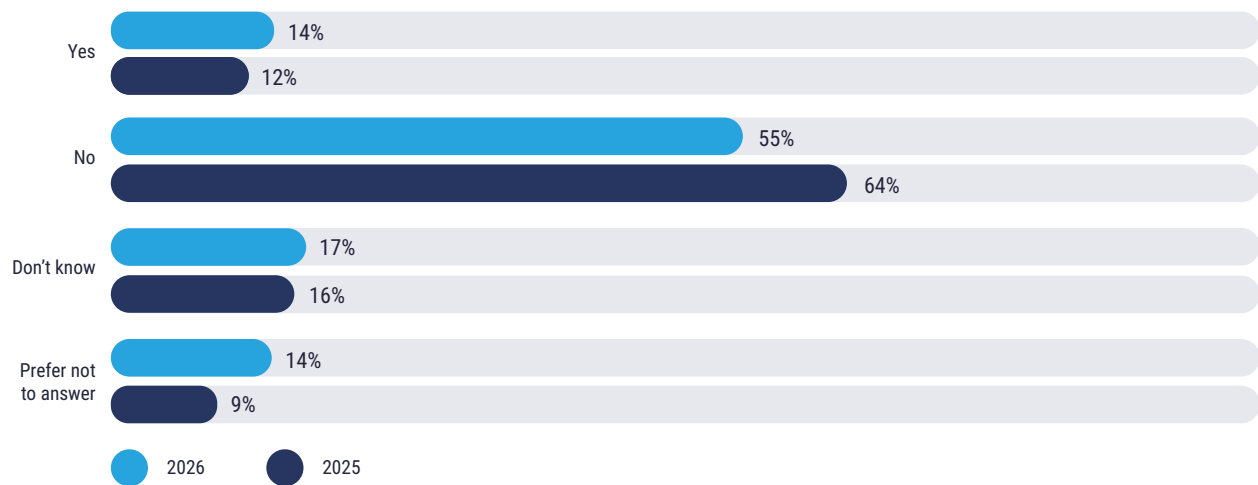
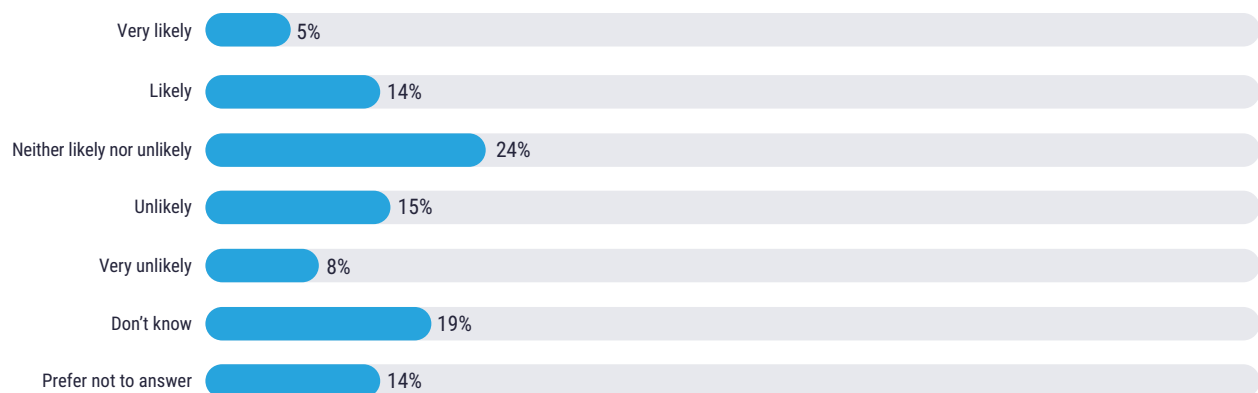


FIGURE 22: Likelihood of a Privacy Breach Next Year



⁹ Thirty-two percent of respondents preferred to not answer, and 23% did not know.

Board prioritization of privacy and privacy strategy alignment with organizational objectives are correlated with the likelihood of experiencing a privacy breach. Of the respondents who said their board of directors does not prioritize privacy, 11% said a breach in the next 12 months is very likely. Of those who said their privacy strategy did not align with organizational objectives, 14% said a breach in the next 12 months is very likely.

Only 9% of respondents said they were not so confident or not at all confident in their organization's ability to ensure the privacy of its sensitive data. Nine percent said

they were completely confident in this ability, and 34% were very confident. Thirty-nine percent of respondents were somewhat confident, and 10% did not know or preferred not to answer. But confidence does not translate to immunity from breaches: 38% of respondents who experienced a privacy breach in the past 12 months were completely or very confident in their ability to ensure privacy.

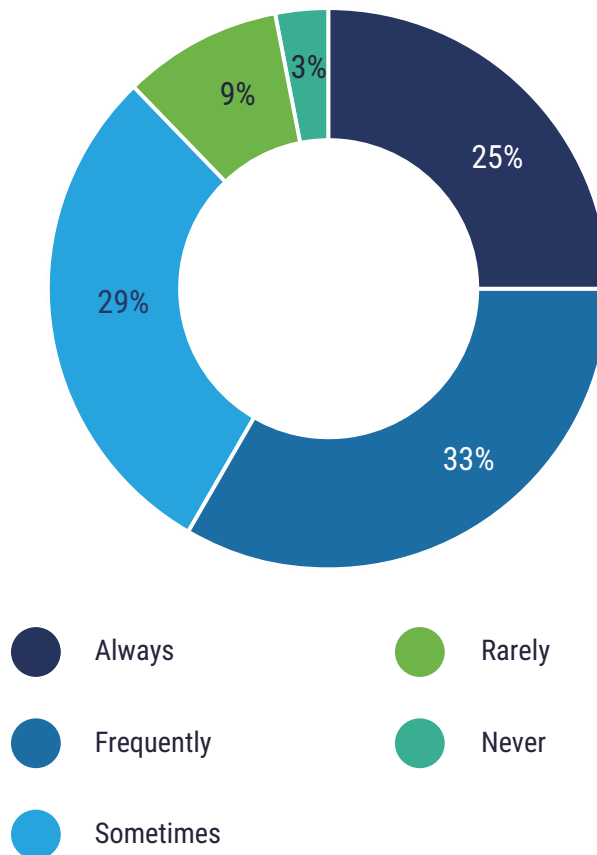
Privacy by Design

Privacy by design is the practice of integrating privacy into the entire engineering process. It is a valuable way to ensure data privacy and, in some cases, may

be required by applicable privacy laws and regulations.

Figure 23 shows how frequently survey respondents practiced privacy by design.

FIGURE 23: Privacy by Design Frequency



Enterprises are more likely to always practice privacy by design if boards prioritize privacy, privacy strategy is aligned with organizational objectives, and there is sufficient funding. Of those respondents whose boards adequately prioritized privacy, 35% always practiced privacy by design, compared to just 9% for respondents whose boards did not prioritize privacy. Thirty percent of respondents who said their privacy strategy aligned with organizational objectives always practiced privacy by design, in contrast to only 6% of respondents who said their privacy strategy did not align with enterprise objectives. Lastly, 32% of respondents who said their privacy budget was significantly/somewhat overfunded and 32% who said their privacy budget was appropriately funded always practiced privacy by design, compared to

just 17% who said their privacy budget was significantly/somewhat underfunded. These correlations indicate that adequate resources and support are key enablers for regularly practicing privacy design.

Of those who currently use AI for privacy tasks, 41% said they always practice privacy by design. This suggests that these AI projects may leverage privacy by design, which is essential for embracing the technology in a way that is privacy preserving.

Larger enterprises with more resources tend to always practice privacy by design, as shown in **figures 24** and **25**, further suggesting that more resources can facilitate privacy by design efforts.

FIGURE 24: Employee Size and Always Practicing Privacy by Design

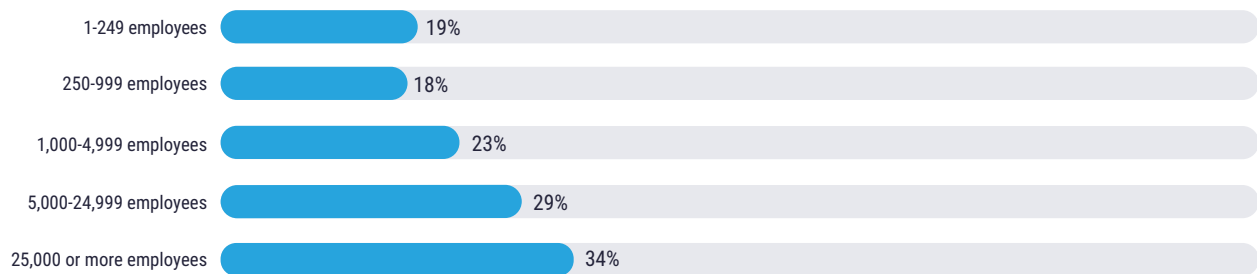
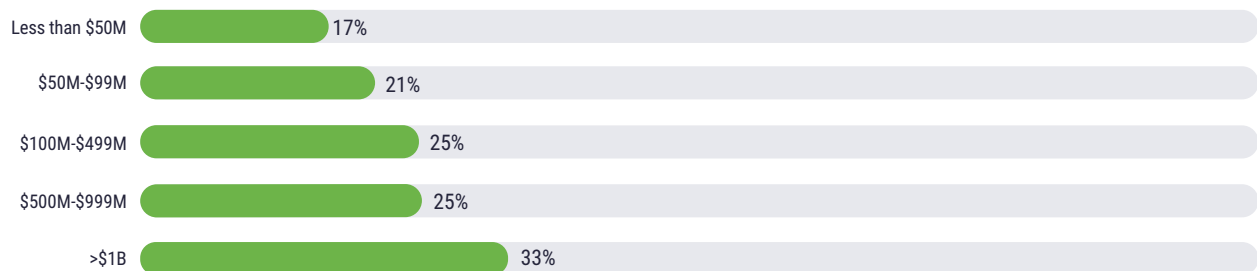


FIGURE 25: Revenue and Always Practicing Privacy by Design



Although practicing privacy by design is worthwhile, it does not correlate to a reduction in breaches. Twenty-four percent of respondents who experienced a breach in the

past 12 months always practiced privacy by design—the same percentage as respondents who did not experience a breach in the past 12 months.

Conclusion

As in previous years, the 2026 State of Privacy survey results highlight that privacy teams often lack sufficient resources. The median privacy staff size dropping by one-third this year is cause for concern, especially considering that half of survey respondents expected their privacy budgets to decrease in the next 12 months.

This year's survey findings also highlight the benefits associated with prioritizing privacy. For example, enterprises that have their privacy team report to a CPO can ensure they have an executive advocate for their privacy program. Enterprises with a CPO were more likely to have adequate board support, and those whose privacy teams reported to a CPO were more confident in their ability to ensure data privacy.

Enterprises with a CPO were more likely to have adequate board support, and those whose privacy teams reported to a CPO were more confident in their ability to ensure data privacy.

Privacy teams that are less impacted by resource limitations tend to have boards of directors that adequately prioritize privacy. Additionally, privacy strategy alignment with organizational objectives is correlated with less understaffing and more optimistic budget forecasts, likely because when privacy is a part of other enterprise

objectives, anything that harms the privacy team will have widespread impacts, incentivizing senior leadership to adequately fund and prioritize privacy programs.

Survey results underscore that AI will not compensate for resource shortages and budget concerns. Given that the adoption of AI for privacy-related tasks is strongly correlated with having a mature privacy program, it appears that privacy professionals understand that AI solutions come with risk and that AI will not be a silver bullet for improper prioritization of privacy.

AI will not compensate for resource shortages and budget concerns. Given that the adoption of AI for privacy-related tasks is strongly correlated with having a mature privacy program, it appears that privacy professionals understand that AI solutions come with risk and that AI will not be a silver bullet for improper prioritization of privacy.

Budget cuts, shrinking staff sizes, and an increasingly complex technology landscape make the work of privacy professionals incredibly challenging. Technology alone will not alleviate the challenges that privacy professionals are experiencing. Only when boards prioritize privacy and privacy objectives align with broader enterprise goals can privacy teams thrive.

Acknowledgments

Lead Developer

An ISACA Staff Publication

Board of Directors

John De Santis, Chair

Former Chairman and Chief Executive Officer, HyTrust, Inc., USA

Jamie Norton, Vice-Chair

CISA, CISM, CGEIT, CIPM, CISSP
Chief Information Security Officer,
Australian Securities and Investments
Commission, Australia

Stephen Gilfus

NACD.DC
General Partner, Oversight Ventures LLC,
Chairman, Gilfus Education Group, and
Founder, Blackboard Inc., USA

Niel Harper

CISA, CRISC, CDPSE, CISSP, NACD.DC
Global Chief Security Officer at JetBrains,
Germany

Gabriela Hernández-Cardoso

NACD.DC
Former President and Chief Executive
Officer, GE Mexico, Independent Board
Member, Mexico

Jason Lau

CISA, CISM, CGEIT, CRISC, CDPSE, CEH,
CIPM, CIPP/E, CIPT, CISSP, FIP, HCISPP
Chief Information Security Officer,
Crypto.com, Singapore

Massimo Migliuolo

Executive Chairman, Intuin, Founder and
Director of Cedro and Kibe, Malaysia

Maureen O'Connell

NACD.DC
Former Executive Vice President and
Chief Financial Officer, Scholastic
Corporation, USA

Erik Prusch

Chief Executive Officer, ISACA, USA

Tim Sattler

CISA, CISM, CGEIT, CRISC, CDPSE, CCSP,
CISSP, ISO 27000 LI/LA
Head of Corporate Information Security
and Chief Information Security Officer,
Jungheinrich AG, Germany

Asaf Weisberg

CISA, CISM, CGEIT, CRISC, CSX-P, CDPSE
Founder and Chief Executive Officer,
introSight Ltd., Israel

Pamela Nigro

ISACA Board Chair 2022-2023
CISA, CGEIT, CRISC, CDPSE, CRMA
Vice President, Security, Medecision, USA

Tracey Dedrick

ISACA Board Chair, 2020-2021
Board Member and Chair of the Risk
Committee, First Bank Puerto Rico and
Sterling FSB, USA

About ISACA

ISACA® (www.isaca.org) champions the global workforce advancing trust in technology. For more than 55 years, ISACA has empowered its community of 185,000+ members with the knowledge, credentials, training and network they need to thrive in fields like information security, governance, assurance, risk management, data privacy and emerging tech. With a presence in more than 190 countries and with nearly 230 chapters worldwide, ISACA offers resources tailored to every stage of members' careers—helping them to thrive in a rapidly changing digital landscape, drive trusted innovation and ensure a more secure digital world. Through the ISACA Foundation, ISACA also expands IT and education career pathways, fostering opportunities to grow the next generation of technology professionals.

DISCLAIMER

ISACA has designed and created *State of Privacy 2026* (the "Work") primarily as an educational resource for professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

RESERVATION OF RIGHTS

© 2026 ISACA. All Rights Reserved.



1700 E. Golf Road, Suite 400
Schaumburg, IL 60173, USA

Phone: +1.847.660.5505

Fax: +1.847.253.1755

Support: support.isaca.org

Website: www.isaca.org

Participate in the ISACA Online Forums:

<https://engage.isaca.org/onlineforums>

X: www.x.com/ISACANews

LinkedIn:
www.linkedin.com/company/isaca

Facebook:
www.facebook.com/ISACAGlobal

Instagram:
www.instagram.com/isacanews/