ISACA

State of Privacy 2025

Privacy

CONTENTS

ABSTRACT

State of Privacy 2025 reports the results of the ISACA global State of Privacy survey conducted late in the third quarter of 2024. This report focuses on privacy staffing and operations, privacy budgets, compliance, the use of AI in privacy, privacy awareness training, privacy breaches, and the role of privacy by design. The survey findings overall are consistent with last year's results but hint at shrinking privacy teams and budget cuts.

Executive Summary

State of Privacy 2025 explores trends in privacy staffing and operations, board prioritization of privacy, privacy compliance, the use of artificial intelligence (AI) in privacy, privacy awareness training, privacy breaches, and the role of privacy by design. These results are based on the fifth annual ISACA global State of Privacy survey conducted in September 2024.

Customers value privacy, and the consequences of a privacy breach can result in significant fines, reputational damage, and loss of trust with data subjects, so the role of privacy professionals is vital. Enterprises that prioritize privacy and ensure it has adequate resources can empower their privacy teams to better support privacy objectives.

Key Findings

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

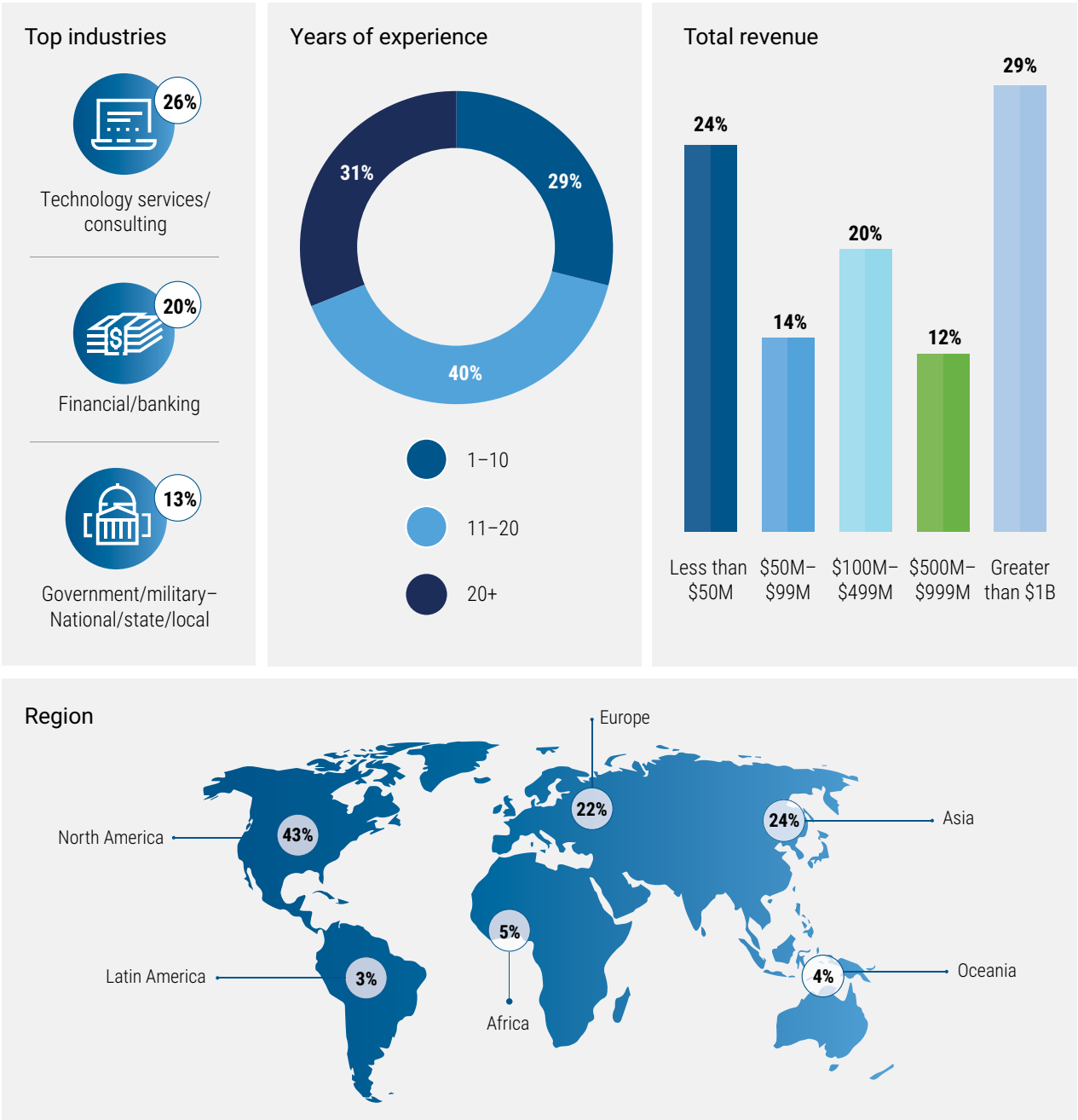
- While privacy staffing shortages remained a challenge, fewer respondents felt their privacy team was understaffed compared to last year, despite the median privacy staff size decreasing.
- Perceptions of privacy funding were consistent with last year.
- More than half of respondents believed their board of directors had adequately prioritized privacy.
- Demand for technical privacy roles is considerably more likely to increase in the next year compared to legal/compliance roles.
- The most common obstacles privacy programs encounter are a complex international legal and regulatory landscape, a lack of competent resources, and challenges with managing the risk associated with new technologies.
- Respondents identified the chief privacy officer as the person most likely to be accountable for privacy operations.
- More respondents reported using AI for privacy-related tasks this year compared to last year.
- The percentage of respondents who said they experienced a material privacy breach this year is comparable to last year's findings.
- Based on survey responses, enterprises that always practice privacy by design are more likely to:
  - Have more employees in privacy roles
  - Strongly believe their board of directors prioritizes privacy adequately
  - Have a privacy strategy aligned with organizational objectives
  - Regard their privacy budget as appropriately funded

Survey Methodology

In September of 2024, ISACA sent survey invitations to approximately 48,900 ISACA constituents who held the Certified Data Privacy Solutions Engineer™ (CDPSE™) designation or had "privacy" in their job title. Invitations were also sent to those who held the ISACA CSX Cybersecurity Practitioner Certification™ (CSX-P™) or Certified Information Security Manager® (CISM®) designation. More than 1,600 people completed the survey.

Respondents held a variety of roles: 38% were in management roles, 29% were senior leadership, 20% were individual contributors, and 12% were executive leadership. **Figure 1** shows additional demographic information about survey respondents.

FIGURE 1: Respondent Demographics



Privacy Staffing and Operations

Privacy teams are comprised of individuals with varying skills and competencies. Technical privacy professionals are those who work in privacy with the expertise to evaluate and apply controls that support privacy objectives, while legal/compliance privacy professionals have a background in law and can understand regulatory requirements and obligations. Technical professionals and legal/compliance professionals must work together to understand their obligations and meet compliance-related requirements. The survey examined staffing trends for both technical privacy professionals and legal/compliance privacy professionals.

Although the median privacy staff size declined from last year (eight this year compared to nine last year), understaffing was not as widespread as last year. Thirty-eight percent of respondents believed their legal/compliance privacy team was understaffed, while 46% of respondents felt their technical privacy team was understaffed. **Figures 2** and **3** compare this year's staffing perceptions to last year's.

There are a number of reasons respondents may not have felt understaffing was as challenging this year as it was last year, despite smaller staff sizes. For example, more respondents were using AI for privacy-related tasks. Last year, only 18% of respondents said they were increasingly relying on AI or automation to address privacy skill gaps, while this year, that number jumped to 24%.

While the demand for privacy professionals remains high, it is lower than last year. Fifty-one percent of respondents believed the demand for legal/compliance privacy roles would increase in the next year, while 57% of respondents believed the demand for technical privacy roles would increase. In 2024, 55% of respondents believed the demand for legal/compliance privacy roles would increase in the next year, and 62% of respondents said the demand for technical privacy roles would increase. The finding that demand for technical privacy roles was greater than for legal/compliance roles is consistent with last year's results.

FIGURE 2: Legal/Compliance Staffing

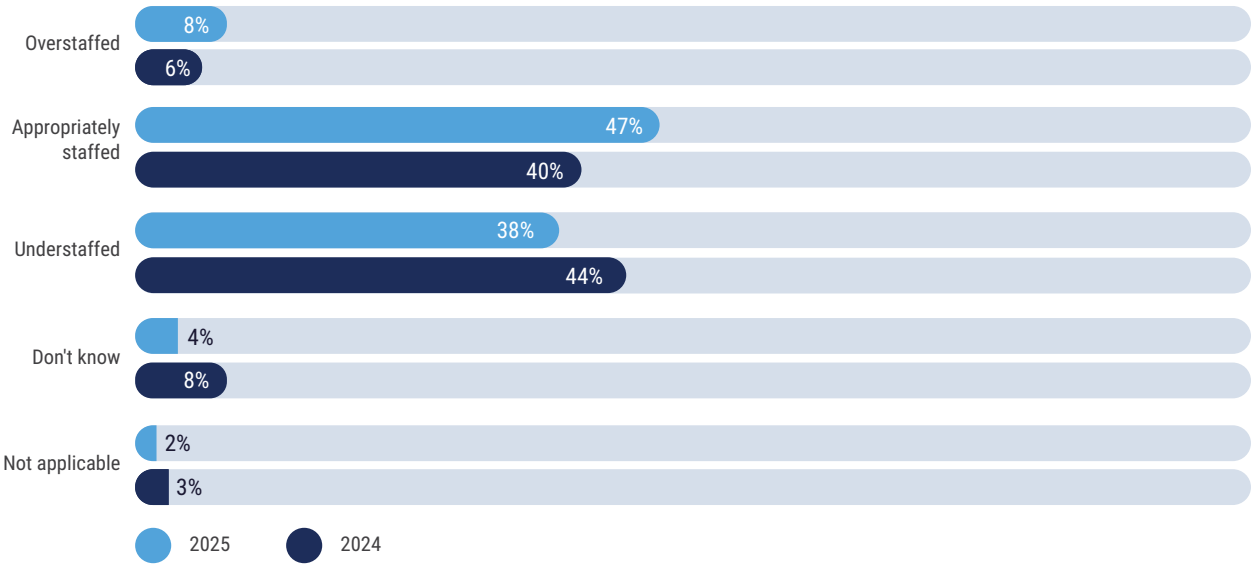
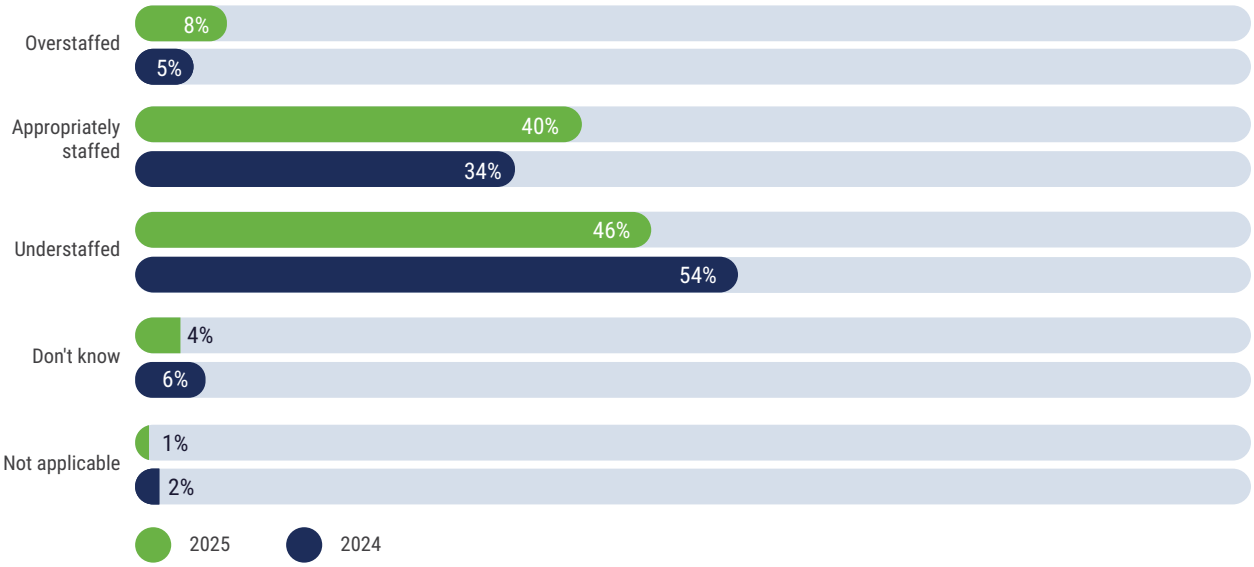


FIGURE 3: Technical Privacy Staffing



Open Privacy Positions

Twenty-two percent of respondents indicated their organization had open legal/compliance practitioner roles, and 29% indicated there were open technical privacy positions. This is a decrease from last year when a quarter of respondents indicated open legal/compliance roles and 31% indicated open technical privacy roles. Given that fewer of this year's respondents believed their organization was understaffed, it stands to reason that there would be fewer open privacy positions.

The decrease in open privacy roles may be attributed to the Big Stay—a recent trend of employees staying in current roles for longer amounts of time. Job markets vary by region, and in a competitive job market, people may be more inclined to stay in their current roles. For example, only 30% of respondents in North America said they experienced difficulties in retaining privacy professionals compared to 60% of respondents in Latin America who said they experienced challenges with employee retention.

Figures 4 and **5** show how long it took to fill open privacy positions compared to last year.

The decline in respondents indicating it took more than six months to fill open privacy roles (for both legal/compliance and technical privacy roles) could also support why understaffing appears to have decreased in the last year. Sixteen percent of respondents indicated that the speed of filling open legal/compliance privacy roles increased, while 18% indicated the speed of filling technical privacy roles increased.

In part, the time to fill open roles may have decreased because more job applicants were qualified for the roles to which they applied. Twenty-nine percent of respondents indicated that more than half of legal/compliance privacy applicants were well qualified for the role, while 28% said more than half of technical privacy applicants were well qualified for the role. This is a notable improvement compared to 2024, when only 21% of respondents said more than half of legal/compliance and technical privacy applicants were well qualified for the roles to which they applied.

FIGURE 4: Time to Fill Legal/Compliance Privacy Roles

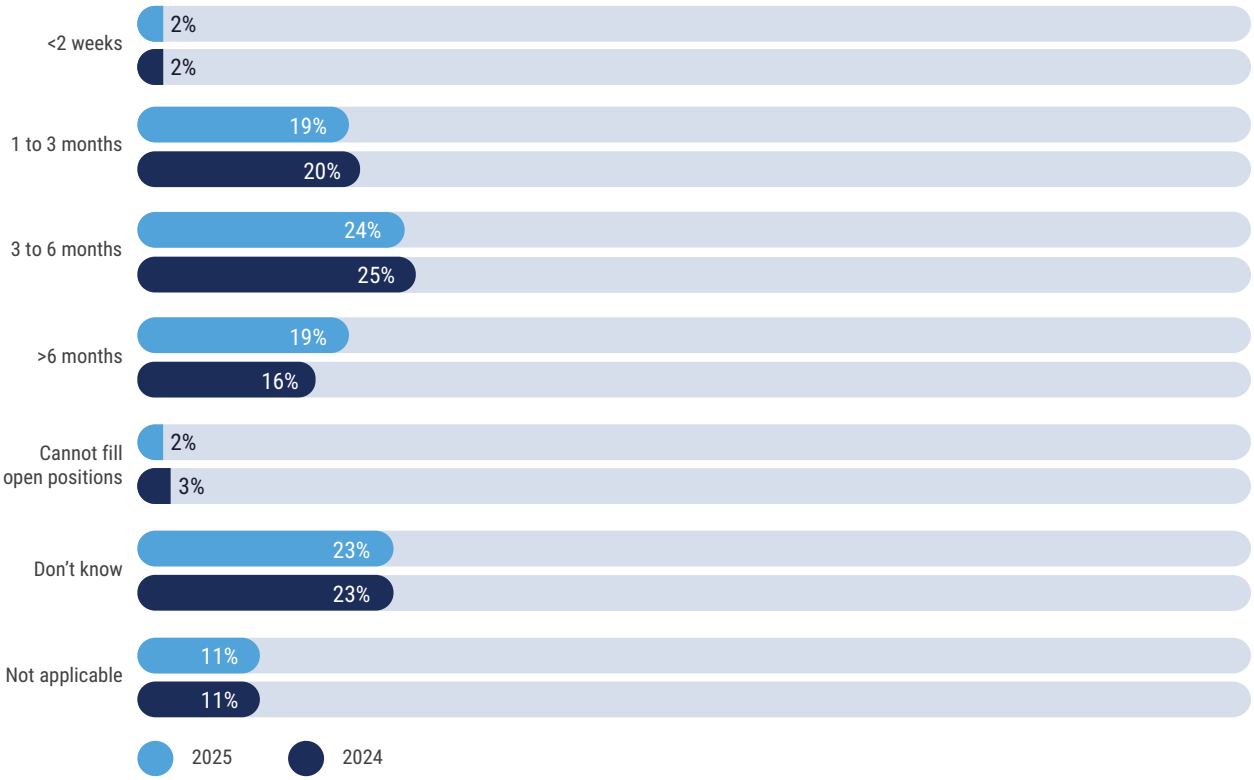
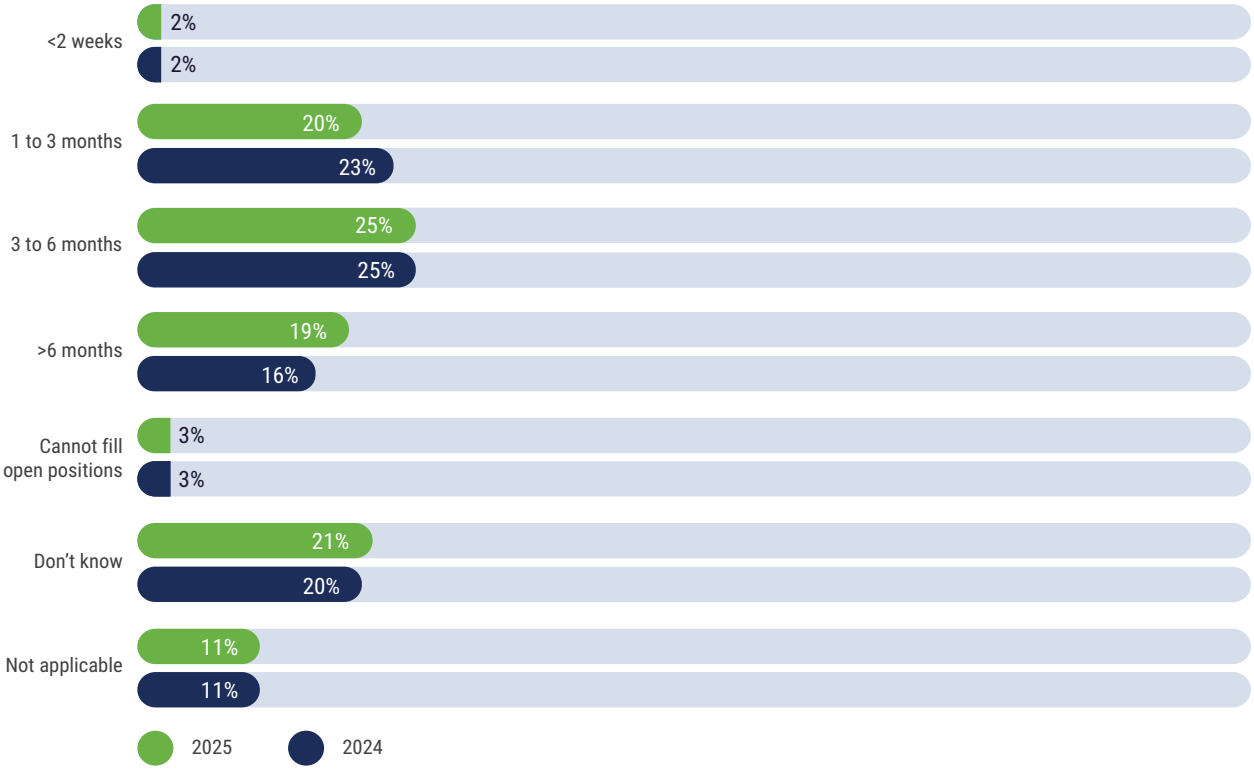


FIGURE 5: Time to Fill Technical Privacy Roles



Experienced privacy professionals are highly desired. The following factors were identified as important in determining if a privacy candidate was qualified for a role, and their importance is comparable to last year's findings:

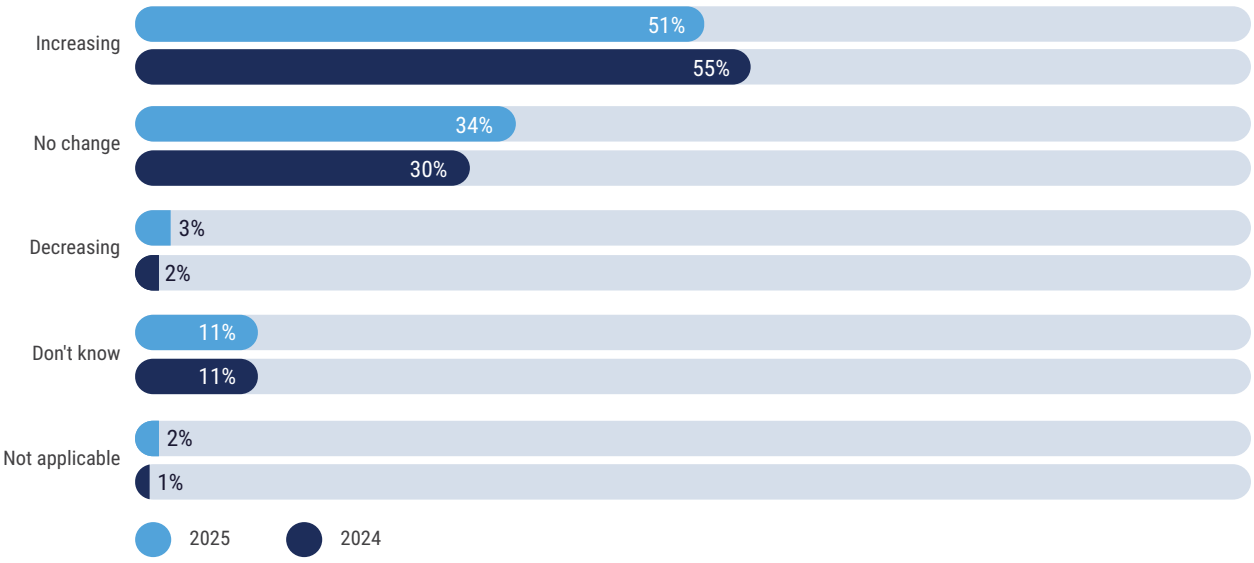
- Compliance/legal experience (96%)
- Prior hands-on experience in a privacy role (94%)
- Technical experience (93%)
- Credentials held (93%)
- Completion of hands-on training courses in privacy (84%)
- University degree (70%)
- Recommendation from previous employer (69%)

It is likely difficult to find a candidate with extensive technical experience as well as compliance/legal experience, which further emphasizes the importance of technical privacy professionals collaborating closely with legal/compliance privacy professionals.

Finding seasoned privacy professionals remains a challenge. Seventy-three percent of respondents said expert-level privacy professionals were the most difficult to hire, 47% said practitioners were most difficult to hire, and 15% said entry level/foundational professionals were most difficult to hire.

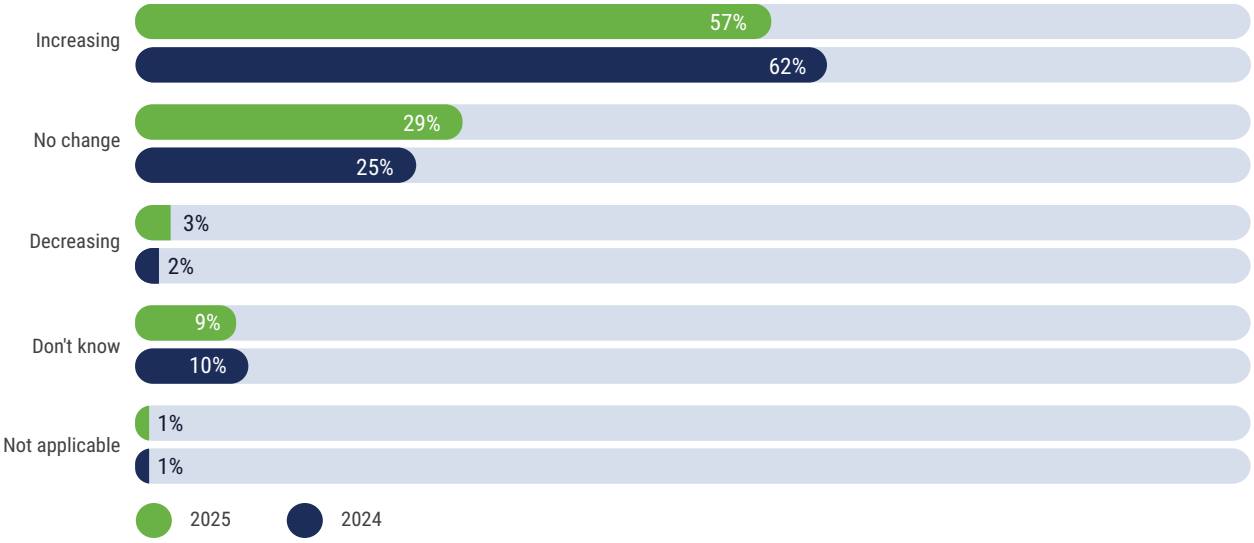
Given the impact of high-profile privacy breaches and consumer demand for privacy,[1] the demand for privacy professionals is expected to increase (**figures 6** and **7**).

FIGURE 6: Demand for Legal/Compliance Privacy Professionals



1 Szczesny, M.; "Data Privacy Matters to Your Customers — Show Them It's a Priority for You, Too. Here's How.," Entrepreneur, 13 February 2024, https://www.entrepreneur.com/science-technology/consumers-demand-more-data-protection-can-you-deliver/468944

FIGURE 7: Demand for Technical Privacy Professionals



Skill Gaps

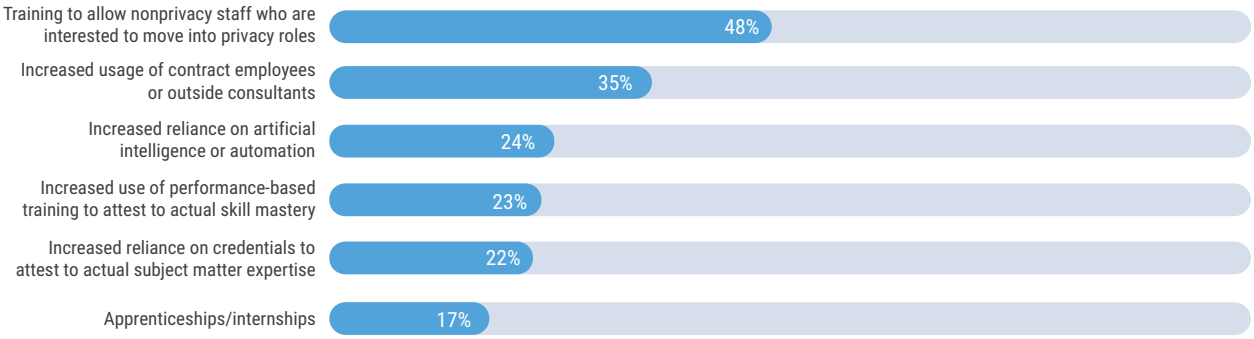
There are certain qualifications that are still lacking among many privacy professionals. The top three skill gaps reported are:

1. Experience with different types of technologies and/or applications (61%)
2. Experience with frameworks and/or controls (49%)
3. Technical expertise (48%)

Other skill gaps include IT operations knowledge and skills (43%), understanding the laws and regulations to which the organization is subject (42%), business insight (35%), networking and/or other infrastructure knowledge and skills (32%), soft skills (29%), and business ethics (18%). **Figure 8** shows the strategies enterprises have been taking to decrease these skill gaps.

FIGURE 8: Addressing Privacy Skill Gaps

Which, if any, of the following has your organization undertaken to help decrease this privacy skills gap?



Retention

Thirty-eight percent of respondents said their organization experienced difficulties retaining qualified privacy professionals. In part, this may be a result of job stress. Sixty-three percent of respondents believed their role was more stressful than it was five years ago, with 34% indicating their role was significantly more stressful.

There are many potential reasons privacy roles may feel more stressful than five years ago. Many enterprises have rushed to adopt new technology—for example, generative AI—without adequate consideration for the associated privacy risk. This may result in privacy professionals having to react to risk rather than be proactive, and it can lead to the perception that privacy teams seek to stifle innovation.

The complex privacy regulatory landscape is also a significant challenge for privacy professionals. There are myriad privacy laws and regulations, and countries, states, and industries may have their own unique privacy laws and associated challenges. Understanding the applicable regulatory requirements and remaining compliant with multiple laws and regulations is a challenging task for privacy professionals.

The reasons survey respondents said roles were more stressful include:

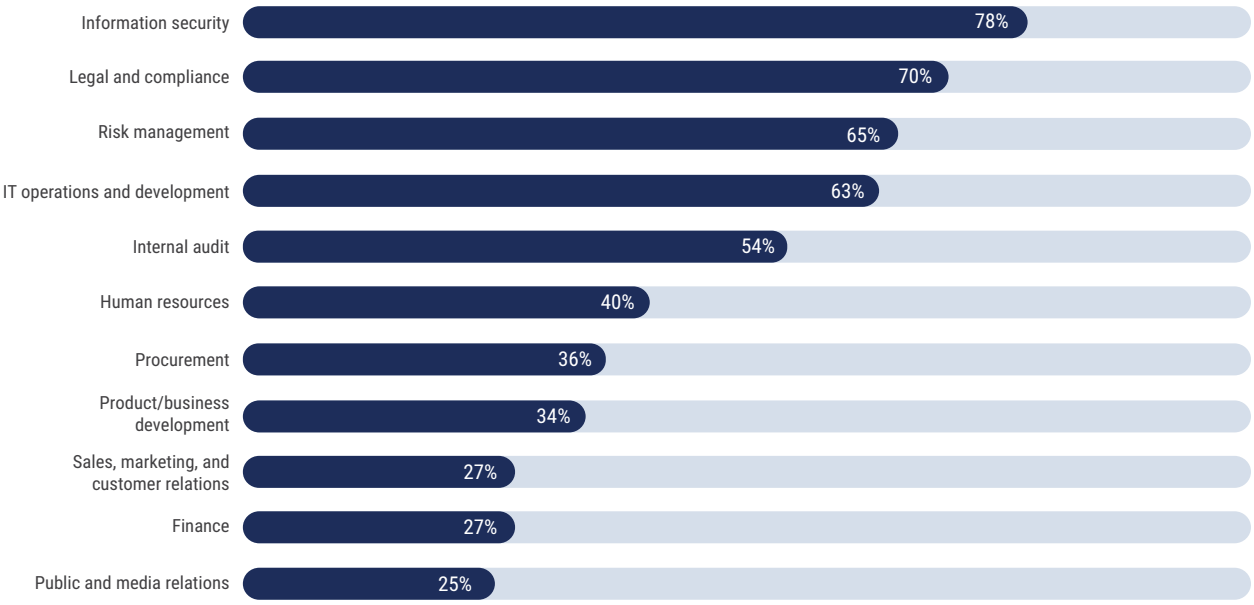
- Technology's rapid evolution (63%)
- Compliance challenges (61%)
- Resource shortages (59%)
- Competing priorities (50%)

Collaboration

Many departments beyond the privacy team have a role in supporting privacy-related objectives. Audit, risk, security, and marketing teams can all facilitate privacy professionals and embed privacy into their work. Privacy professionals work cross-functionally to ensure privacy is embedded throughout the organization. **Figure 9** shows the departments that privacy professionals interact with most frequently.

FIGURE 9: Privacy Interaction With Other Areas

How frequently do the privacy office/privacy professionals in your organization interact with the following areas?



Obstacles

Competitive enterprises have myriad goals, objectives, and priorities, and privacy is just one small facet of their key considerations. Privacy teams may encounter a variety of obstacles. Survey respondents indicated the most common obstacles were:

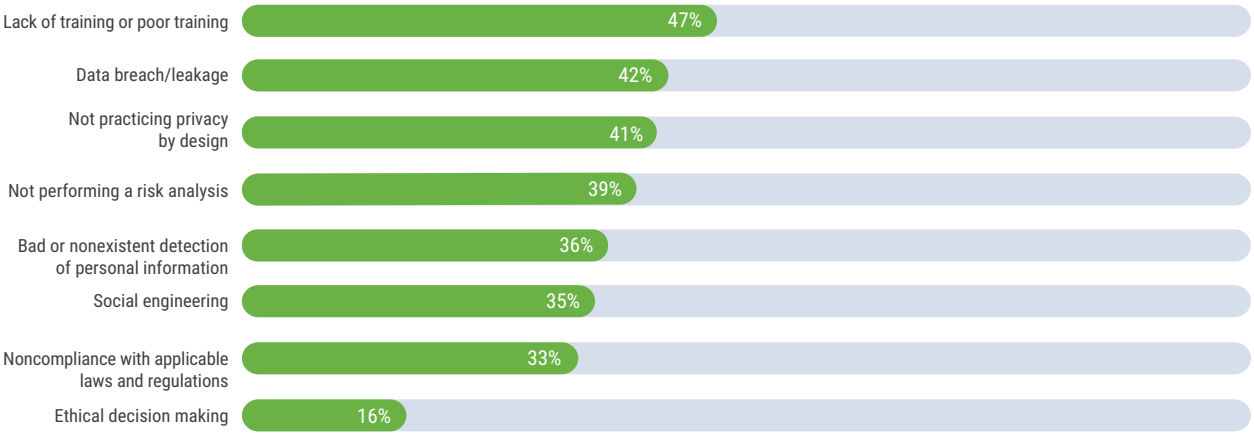
- Complex international legal and regulatory landscape (38%)
- Lack of competent resources (37%)
- Management of risk associated with new technologies (36%)
- Lack of clarity on the mandate, roles, and responsibilities (35%)
- Lack of executive or business support (33%)
- Lack of visibility and influence within the organization (33%)
- Poor data management practices (27%)
- Lack of a privacy strategy and implementation roadmap (26%)

Survey results, once again, indicate that experienced privacy professionals—with prior expertise in privacy roles or with laws and regulations—are critical to the effective functioning of a privacy program.

Given privacy teams' wide scope of responsibility, there are numerous reasons privacy failures may occur. **Figure 10** shows the most common privacy failures in organizations.

FIGURE 10: Most Common Privacy Failures

In your opinion, which of the following are the most common privacy failures in an organization?



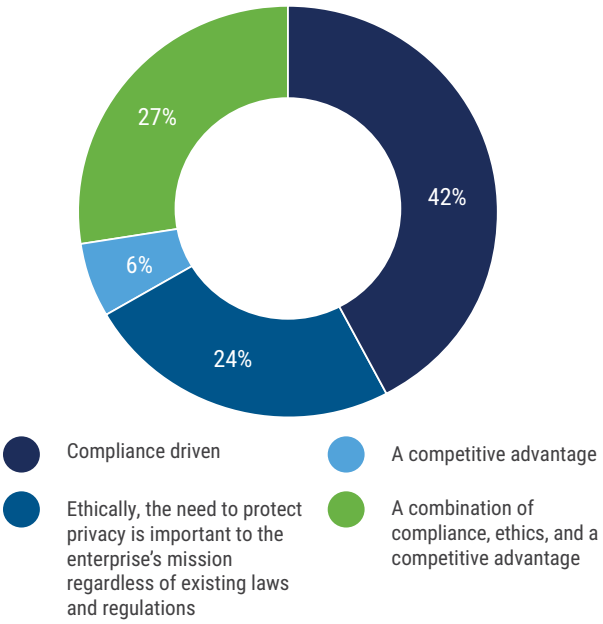
Privacy Prioritization

Boards of directors properly prioritizing privacy can help ensure that privacy teams have the resources and support needed to complete their objectives and ensure privacy compliance. Just over half of respondents (57%) believed their board of directors adequately prioritized privacy. Nearly three-quarters of respondents (74%) said their organization's privacy strategy was aligned with organizational objectives. **Figure 11** shows the way boards view privacy programs.

Enterprises should have one individual who is primarily accountable for privacy. This individual can be an advocate for privacy and ensure privacy teams have the necessary resources. Twenty-one percent of respondents said the chief privacy officer was primarily accountable for privacy, 14% said the chief information officer was accountable, 14% said an executive-level security officer was accountable, 11% said the chief executive officer was accountable, and 11% said general counsel/the chief legal officer was primarily accountable for privacy.

FIGURE 11: Board Views of Privacy Programs

Do you think your board of directors views your enterprise's privacy program as:



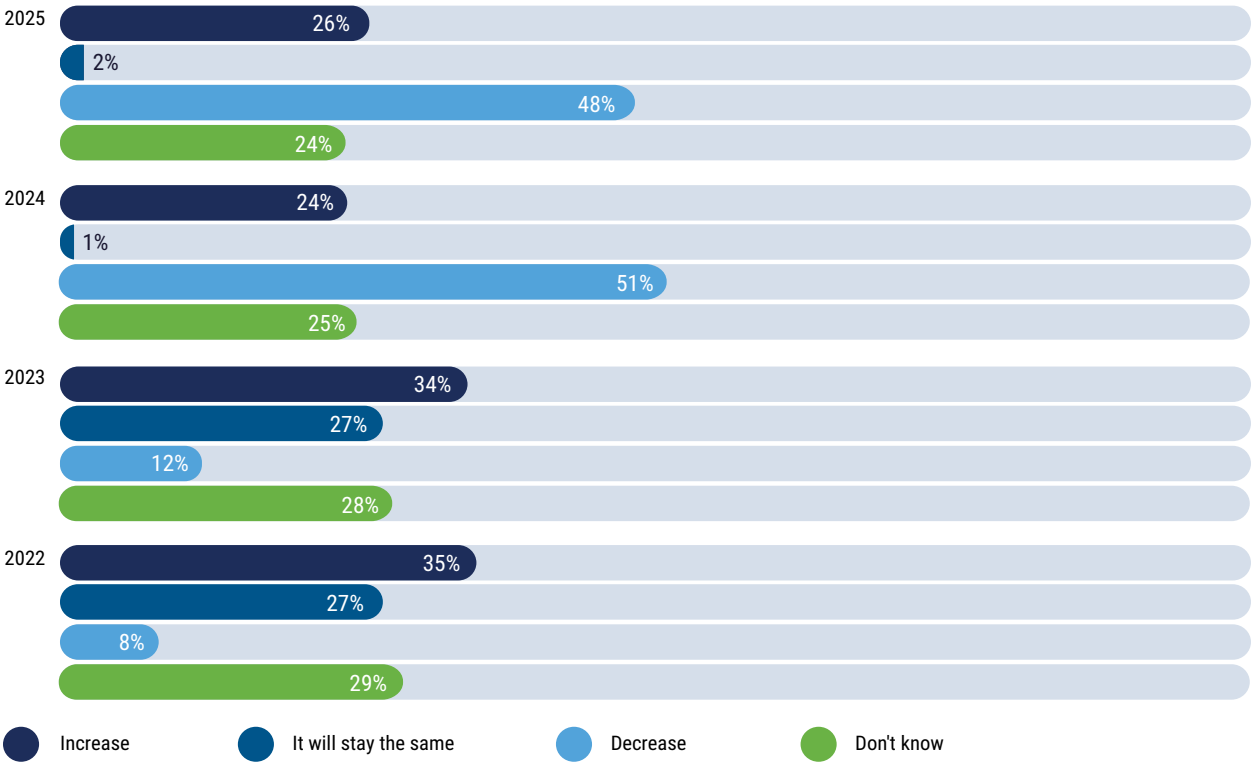
Some of these roles may, at times, be at odds with privacy. For example, some security-related measures could conflict with privacy objectives; pursuing nonrepudiation may put privacy at risk. Additionally, the general counsel/chief legal officer is primarily concerned with protecting the enterprise, while privacy professionals typically prioritize protecting data subjects, so the goals of privacy professionals may contradict the goals of the general counsel/chief legal officer.

Budgets

The perception of privacy budget funding this year was consistent with last year. Forty-three percent of respondents believed their privacy budget was underfunded and 36% of respondents felt their privacy budget was appropriately funded, which is identical to last year's findings. **Figure 12** shows how privacy budgets are expected to change over the next 12 months and compares it with previous survey findings.

FIGURE 12: Privacy Budget Changes

How will your organization's privacy budget change in the next 12 months?



While the percentage of respondents who believed their privacy budget would decrease in the next 12 months is consistent with last year's findings, both the 2024 and 2025 perceptions of budget decreases were considerably higher than in previous years. Fortunately, it does not appear that 2024 fears about decreases came to fruition: Only 10% of respondents saw a decrease in their privacy budget in the past 12 months.

Although many departments may have concerns about budget cuts, privacy appears to be disproportionately affected. In ISACA's 2024 State of Cybersecurity survey, only 13% of respondents believed their cybersecurity budget would decrease in the next 12 months.[2] The State of Privacy survey findings could be concerning for cybersecurity professionals: With potential cuts to privacy, cybersecurity practitioners may be expected to take on some privacy-related responsibilities as well. Some senior leadership teams may struggle to understand the difference between security and privacy and why both are fundamental to gaining and maintaining trust with consumers.

Compliance

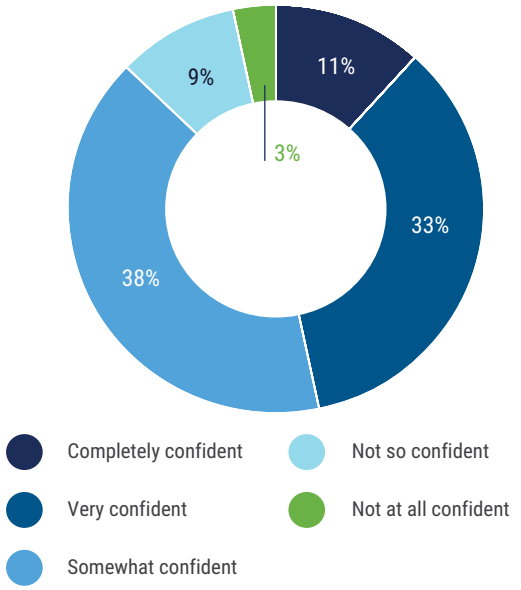
Regulatory requirements may heavily shape an enterprise's privacy program. Eighty-two percent of respondents use a framework or law/regulation to manage privacy in their organization. Given the myriad privacy laws and regulations enterprises may need to comply with, working closely with legal/compliance professionals is critical to ensure compliance. Twenty-eight percent of respondents meet with legal/compliance professionals quarterly, 24% meet with them once or twice a year, 18% meet with them monthly, 16% meet with them as new privacy laws/regulations go into effect, 8% meet with them weekly, and 7% never meet with them.

Meeting regularly with legal/compliance professionals is critical given that only one-third of respondents found it easy or very easy to identify/understand privacy obligations. Twenty-three percent of respondents said it was difficult or very difficult, and 39% said it was neither easy nor difficult. This is unsurprising, considering the multitude of existing privacy laws and potentially conflicting regulatory requirements.

Despite challenges associated with identifying and understanding privacy obligations, most survey respondents felt confident in the ability of their organization's privacy team to ensure data privacy and achieve compliance (**figure 13**).

FIGURE 13: Confidence in Ensuring Data Privacy and Achieving Compliance

How confident are you in your organization's privacy team's ability to ensure data privacy and achieve compliance with new privacy laws and regulations?



2 ISACA, *State of Cybersecurity 2024*, 1 October 2024, https://www.isaca.org/resources/reports/state-of-cybersecurity-2024

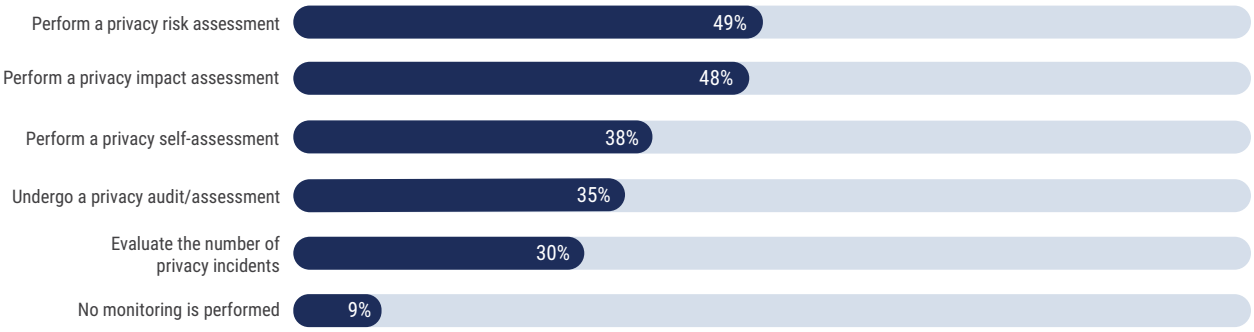
The majority (68%) of respondents said that addressing privacy with documented privacy policies, procedures, and standards was mandatory. But among respondents who believed their board adequately prioritized privacy, that number jumped to 80%, indicating that this documentation may facilitate buy-in and support for privacy or that boards supporting privacy expect formalized privacy policies and procedures.

Enterprises that wish to improve their privacy programs must first monitor and evaluate them. **Figure 14** shows the methods used to monitor the effectiveness of privacy programs. Ideally, enterprises would combine several methods to obtain a comprehensive view into the efficacy of their privacy program.

Some privacy laws and regulations allow data subjects to make requests about their data—for example, deletion or transfer to another system. Thirty-five percent of respondents said the number of data subject requests they received increased in the past year, 32% said it stayed the same, and only 5% said it decreased.

FIGURE 14: How Enterprises Monitor Privacy Programs

How does your organization monitor the effectiveness of its privacy program?



Using AI for Privacy

AI may be used to aid the work of privacy professionals, and it has the potential to address skill gaps and staffing issues. AI can also help enterprises better manage the massive amounts of data they collect, assisting with data classification and identifying personal information. It is important to note that the use of AI is not without risk, and enterprises must determine if the use of AI for privacy-related work aligns with their risk appetite. **Figure 15** shows respondents' use of AI for privacy-related tasks.

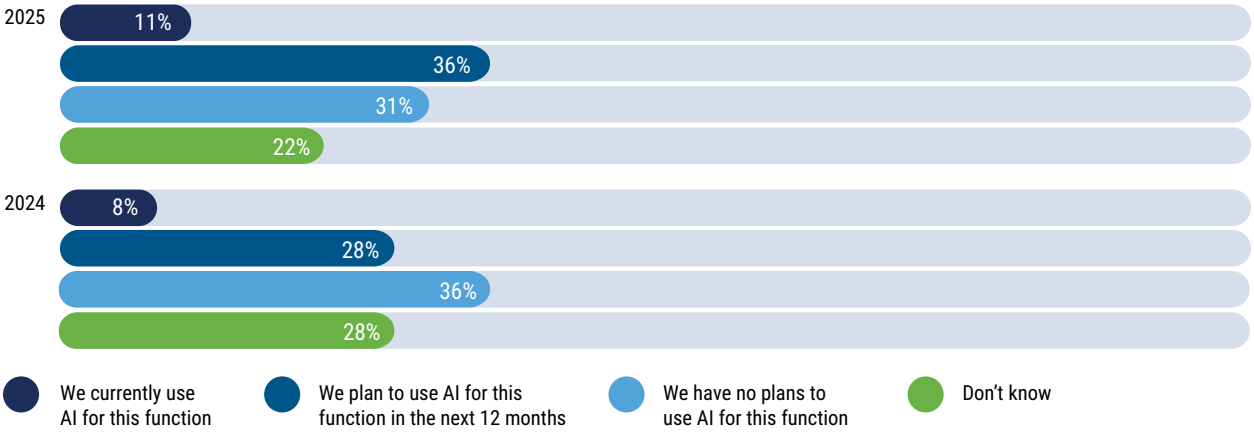
More respondents used AI this year compared to last year. Additionally, fewer respondents said they had no plans to use AI for privacy, which may indicate that some fears around the use of AI are gradually being addressed.

Of note, the use of AI for privacy-related tasks was higher in enterprises that were not purely compliance driven. Only 9% of respondents in enterprises whose boards viewed privacy programs as purely compliance driven reported currently using AI for privacy, while 14% of those in enterprises with boards that viewed privacy ethically or as a competitive advantage said they currently used AI for privacy-related work. This finding further illustrates that relying solely on compliance to drive privacy programs will leave enterprises behind; enterprises must develop their own standards and ethical guidelines around the use of emerging technology. Laws and regulations cannot keep pace with rapidly evolving technologies, so to adopt them safely, enterprises must think beyond mere compliance.

The current use of AI was also higher among enterprises that regularly practiced privacy by design. Of respondents who said they always practiced privacy by design, 18% reported currently using AI for privacy-related tasks. This is encouraging, hinting at the use of privacy by design in AI applications, which can make their use safer and more privacy preserving. It may also allude to enterprises that leverage AI solutions understanding the importance of data protection and taking steps to better prioritize privacy.

FIGURE 15: Plans to Use AI

What are your organization's plans to use AI (bots or machine learning) to perform any privacy-related tasks?



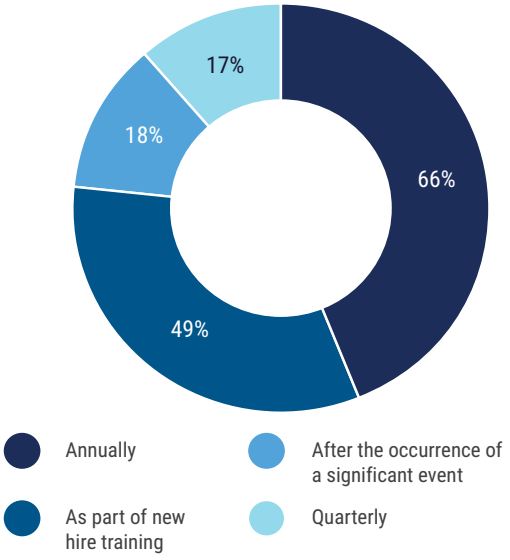
Privacy Awareness Training

Privacy awareness training can help privacy professionals empower staff to act with privacy in mind, reducing the likelihood of privacy incidents. The vast majority of respondents (87%) said their organization provided privacy awareness training for employees. **Figure 16** shows the frequency with which privacy awareness training was provided.

To ensure that privacy awareness training provides valuable, relevant content, it needs to be updated with some frequency. New laws and regulations, enforcement actions, and organizational changes may impact the content that needs to be shared in privacy training. Fifty-nine percent of respondents updated privacy awareness training annually, 24% updated it when new laws/regulations went into effect, 9% updated it every two to five years, and 3% of respondents said they did not revise their privacy training.

FIGURE 16: Frequency of Privacy Awareness Training

When does your organization provide privacy training?



Privacy teams may need to update privacy training if it is determined not to be effective. To know this, it is critical to have metrics to evaluate training effectiveness. **Figure 17** shows the ways respondents evaluated their privacy awareness program's effectiveness.

Solely looking at the number of privacy incidents as a measure of privacy training efficacy is concerning for a few reasons. It is a reactive measure; if a privacy incident has occurred, data subjects may have already experienced some kind of harm. This can result in the enterprise not knowing its training program needs improvement until it has to pay a lofty fine or customer trust is damaged.

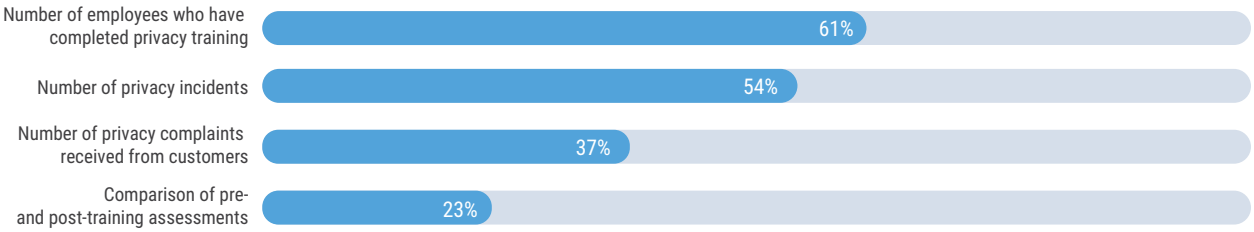
Additionally, the number of privacy incidents could increase as a result of effective privacy awareness training: Employees may be better versed in what constitutes a privacy incident and report more incidents because of this knowledge. The process of tracking privacy incidents should be granular—for example, measuring privacy incidents reported by staff vs. privacy incidents reported by customers. An increase in staff reporting privacy incidents could indicate privacy awareness training is working, while an increase in externally reported incidents could indicate room for improvement.

The majority of respondents (61%) said privacy awareness training was separate from security training. It is possible to provide security and privacy training concurrently, but if they are combined, it is critical for the training to have sufficient privacy-specific content. Training focused entirely on security may leave crucial gaps pertaining to privacy—for example, neglecting the importance of data minimization. While it is not possible to have privacy without security, security objectives could be met without consideration for privacy.

Overall, privacy training and awareness programs were perceived to be beneficial. Eighty-six percent of respondents said privacy training and awareness programs had a positive impact on overall employee privacy awareness.

FIGURE 17: Metrics to Evaluate Privacy Training Programs

What metrics does your organization track to evaluate the privacy training program's effectiveness?



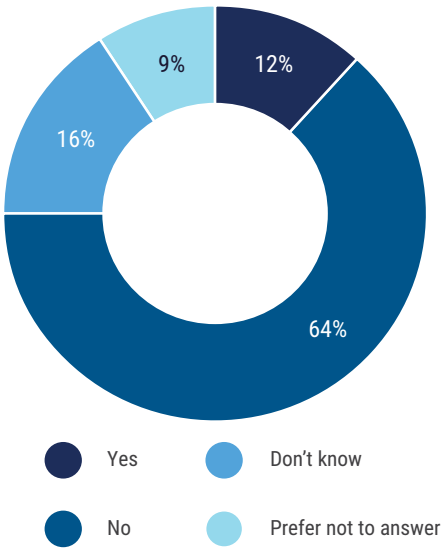
Privacy Breaches

Privacy breaches can lead to reputational harm, damage to trust with consumers, and regulatory consequences. **Figure 18** shows how many respondents' organizations experienced a material privacy breach in the past 12 months.

These findings are relatively consistent with last year's; in 2024, 11% of respondents had experienced a material privacy breach in the past 12 months, 63% had not, 18% didn't know, and 8% preferred not to answer.

FIGURE 18: Material Privacy Breaches

Has your organization experienced a material privacy breach in the past 12 months?



While the percentage of respondents who indicated they did not know if they had experienced a material privacy breach may seem high, it is likely that some enterprises are unsure if security breaches affected personal information. This may indicate a broader concern about data classification and breach response: Inaccurate classification of data makes breach response more challenging, making it harder to meet compliance-related obligations related to breaches, such as notification of supervisory authorities.

Most respondents did not believe they were experiencing more breaches this year compared to a year ago. Only 5% of respondents said they were experiencing more breaches, while 19% said they were experiencing fewer breaches, 22% said they were experiencing the same number of breaches, and 30% did not know. (Twenty-four percent of respondents preferred not to answer.)

There was a lot of uncertainty about the likelihood of a material privacy breach in the future. Fifteen percent of respondents said a material privacy breach in the next 12 months was likely, 23% said it was neither likely nor unlikely, 29% said it was unlikely, 22% did not know, and 11% preferred not to answer. The finding that over a fifth of respondents did not know about the likelihood of a material privacy breach in the next 12 months may indicate that privacy risk is not a mature discipline in many organizations.

Only 40% of respondents felt completely or very confident in their organization's ability to ensure the privacy of its sensitive data. This percentage jumps to 54% for respondents whose board adequately prioritized privacy and 68% for those who always practiced privacy by design. Eleven percent of respondents were not confident in their organization's ability to ensure privacy of sensitive data, while 7% did not know, and 6% preferred not to answer. Enterprise size is not necessarily correlated to confidence. While 46% of those in enterprises with more than 25,000 employees and 42% of respondents in enterprises with less than 250 employees felt confident in their organization's ability to ensure the privacy of its sensitive data, only 37% of respondents in organizations with 250-4,999 employees were confident in this ability.

Privacy by Design

Privacy by design, which is the integration of privacy into the entire engineering process, is critical to ensuring that new products and services can support privacy objectives. Sixty-seven percent of respondents said their enterprise practiced privacy by design when building new applications and services. The use of this approach appears to be regular in many enterprises. **Figure 19** shows the frequency with which enterprises practiced privacy by design.

Privacy by design requires the consideration of privacy as a factor in every life cycle stage. Given that, it is surprising that only 36% of respondents always or frequently worked with procurement teams since they can help ensure that new tools and software align with privacy objectives. However, this number jumped to 52% among respondents who always practiced privacy by design.

Additionally, product/business development teams can ensure that product functionality supports privacy, but only 34% of respondents always or frequently worked with product/business development. But among respondents who always practiced privacy by design, this number increased to 49%. Not regularly collaborating with these key teams makes it difficult to practice privacy by design and ensure that privacy is properly embedded throughout the entire engineering process.

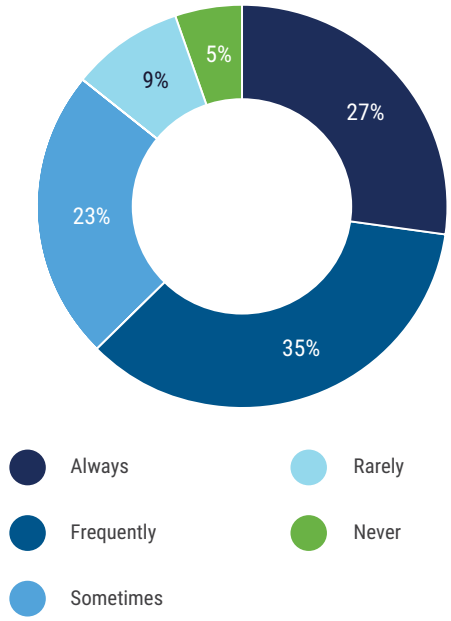
Forty-one percent of respondents said that not practicing privacy by design was a common privacy failure, yet only 27% of respondents report always practicing privacy by design. While privacy by design may be perceived as important, some enterprises may not have the resources and support needed to pursue it regularly.

The survey results indicate that teams that always practice privacy by design tend to have more support and more resources. Respondents who always practiced privacy by design were more likely to believe their board of directors had adequately prioritized privacy. Eighty percent of those in enterprises that always practiced privacy by design said their board adequately prioritized privacy, compared to just 57% for all respondents. Leadership that understands the importance of privacy teams and values them may be more likely to support budget increases that facilitate the work of privacy professionals.

Half of respondents in enterprises that always practiced privacy by design said their enterprise privacy budget was appropriately funded, compared to 36% of total

FIGURE 19: Privacy by Design Frequency

How often does your enterprise practice privacy by design?



respondents who said their privacy budget was appropriately funded. Only 6% of respondents who always practiced privacy by design said their privacy budget decreased in the last 12 months compared to 10% of total respondents. This may indicate that always pursuing privacy by design is considerably more challenging in the event of budget cuts.

The median staff size among enterprises that always practiced privacy by design was 11 compared to eight among enterprises overall. But this number is considerably lower than last year when the median staff size for enterprises that always practiced privacy by design was 15. Technical privacy understaffing appears to have eased among enterprises that always practiced privacy by design. Half of respondents in enterprises that always practiced privacy by design said their technical privacy team was appropriately staffed, and only 33% said it was understaffed, compared to 40% of total respondents who said technical privacy teams were appropriately staffed and 46% of total respondents who said technical privacy teams were understaffed.

Enterprises that always practiced privacy by design were less likely to have boards that were purely compliance driven (34% vs. 42% for all respondents). A purely compliance-based approach to privacy puts enterprises in a reactionary position. They must respond to regulatory requirements rather than be proactive, and being proactive is a key tenet of privacy by design. A risk-based approach to privacy is proactive, identifying potential risk to data subjects and allowing enterprises to address it as appropriate. It allows enterprises to maximize the benefits of their technology while minimizing the harm to consumers.

Those who always practiced privacy by design were also more likely to have a privacy strategy that aligned with organizational objectives. Ninety-one percent of those in enterprises that always practiced privacy by design said their privacy strategy aligned with organizational objectives, compared to 74% of total respondents. This alignment may explain why these privacy teams have access to more resources: Privacy strategy supports broader organizational objectives, which can lead to more leadership support and buy-in for investments in privacy.

The expectations around privacy may also account for why some enterprises always adhere to privacy by design. Eighty-nine percent of respondents in enterprises that always practiced privacy by design said addressing privacy with documented privacy policies, procedures, standards, etc., was mandatory compared to just 68% for total respondents. The existence of documented policies, procedures, and standards implies a level of maturity, as does mandating that privacy practices align with this documentation. The maturity of these organizations may also hint at why they always practice privacy by design.

Those who always practice privacy by design are more likely to be confident in their ability to ensure data privacy and achieve compliance with new privacy laws and regulations. Seventy-two percent of respondents in enterprises that always practiced privacy by design felt completely or very confident in this ability, compared to just 44% for total respondents. But practicing privacy by design does not mean immunity from privacy breaches. Ten percent of those who always practiced privacy by design experienced a material privacy breach in the past year, compared to 12% of total respondents.

Conclusion

Privacy remains a priority for many enterprises, but privacy teams are getting smaller, indicating that the roles of privacy professionals could become more challenging. Budgetary reductions have correlated with a slight increase (1% compared to last year) in material privacy breaches, raising concerns as to what may happen if anticipated reductions come to fruition in the next 12 months.

Enterprise privacy programs that have board-level support and adequate resources are more likely to practice privacy by design and feel more confident in ensuring data privacy. Regardless of executive support and despite staffing and skills shortages, privacy professionals have been resourceful in leveraging emerging technology and outside assistance to meet privacy-related objectives.

Acknowledgments

ISACA would like to recognize:

Board of Directors

John De Santis, Chair

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

Niel Harper, Vice-Chair

CISA, CRISC, CDPSE, CISSP, NACD.DC

Chief Information Security Officer and Data Protection Officer, Doodle, Former Chief Information Security Officer, United Nations Office for Project Services (UNOPS), Germany

Stephen Gilfus

Managing Director, Oversight Ventures LLC, Chairman, Gilfus Education Group and Founder, Blackboard Inc., USA

Gabriela Hernandez-Cardoso

NACD.DC

Former President and CEO, GE Mexico, Independent Board Member, Mexico

Jason Lau

CISA, CISM, CGEIT, CRISC, CDPSE, CIPM, CIPP/E, CIPT, CISSP, FIP, HCISPP

Chief Information Security Officer, Crypto.com, Singapore

Massimo Migliuolo

Independent Board Member, Malaysia

Jamie Norton

CISA, CISM, CGEIT, CIPM, CISSP

Partner, McGrathNicol, Australia

Maureen O'Connell

NACD.DC

Board Chair, Acacia Research (NASDAQ), Former Chief Financial Officer and Chief Administration Officer, Scholastic, Inc., USA

Erik Prusch

Chief Executive Officer, ISACA, USA

Asaf Weisberg

CISA, CISM, CGEIT, CRISC, CSX-P, CDPSE

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

Former Executive Vice President and Head of Enterprise Risk Management, Santander Holdings, USA

Brennan P. Baybeck

ISACA Board Chair, 2019-2020

CISA, CISM, CRISC, CISSP

Senior Vice President and Chief Information Security Officer for Customer Services, Oracle Corporation, USA

About ISACA

ISACA® (www.isaca.org) is a global community advancing individuals and organizations in their pursuit of digital trust. For more than 50 years, ISACA has equipped individuals and enterprises with the knowledge, credentials, education, training and community to progress their careers, transform their organizations, and build a more trusted and ethical digital world. ISACA is a global professional association and learning organization that leverages the expertise of its 180,000+ members who work in digital trust fields such as information security, governance, assurance, risk, privacy and quality. It has a presence in 188 countries, including 225 chapters worldwide. Through the ISACA Foundation, ISACA supports IT education and career pathways for underresourced and underrepresented populations.

DISCLAIMER

ISACA has designed and created *State of Privacy 2025* (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

ISACA
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/