ISACA

Privacy in Practice 2023

Privacy

CONTENTS

ABSTRACT

Privacy in Practice 2023 reports the results of the ISACA® global *State of Privacy Survey*, conducted in the fourth quarter of 2022. This report focuses on privacy staffing, budgets, program trends, awareness training and breaches, and privacy by design. Some survey findings are consistent with last year's survey results, while others indicate relief from some of the privacy challenges identified last year.

Executive Summary

Privacy in Practice 2023 explores trends in privacy staffing, budgets, programs, awareness training and privacy by design, based on the results of the ISACA global *State of Privacy Survey*, conducted in the fourth quarter of 2022.

Strong enterprise privacy practices are critical in a rapidly evolving privacy regulatory landscape. Privacy violations erode customer trust and increasingly result in enterprise reputation damage and significant fines. Enterprise privacy programs that aim to protect data subjects and gain their trust set their enterprises apart from competitors. This white paper explores the state of organizational privacy.

Key Findings

The following are key survey findings:

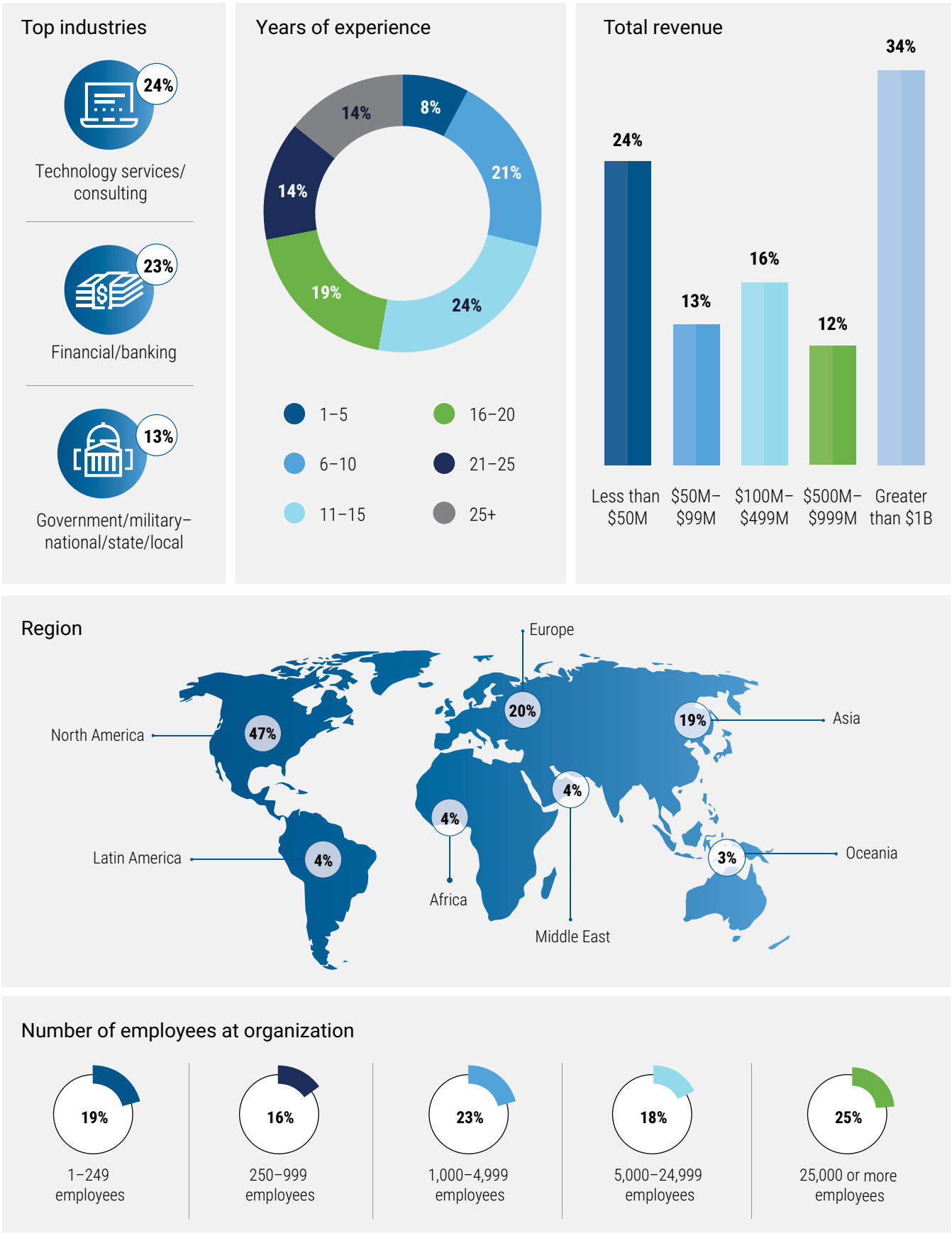
- Technical privacy roles are slightly more likely to be somewhat or significantly understaffed than legal/compliance privacy roles, although both types of roles are impacted by staff shortages.
- Technical privacy roles are significantly more likely than legal/compliance privacy roles to have increased demand in the next year.
- Experience is considered the most important factor in determining if a privacy-position candidate is qualified.
- The demand for privacy professionals is expected to increase over the next year for technical privacy professionals and legal/compliance privacy professionals.
- Privacy teams interact most frequently with information security, legal/compliance and risk management teams.
- Enterprises that practice privacy by design are more likely to:
  - Have adequately staffed privacy teams
  - Believe that their board of directors appropriately prioritizes enterprise privacy
  - Require documented privacy policies, procedures and standards
  - Use more privacy controls overall than are legally required
  - Feel their privacy budget is appropriately funded

Survey Methodology

In the fourth quarter of 2022, ISACA sent survey invitations globally to approximately 46,000 ISACA constituents who hold the ISACA CSX Cybersecurity Practitioner Certification™ (CSX-P™), Certified Information Security Manager® (CISM®) or Certified Data Privacy Solutions Engineer™ (CDPSE™) designation, or have "privacy" in their job title. Survey data were collected anonymously via Survey Monkey. A total of 1,890 respondents completed the survey; their responses are included in the results.

The most commonly held certification is the CISM certification: Seventy-five percent of respondents hold the CISM certification, 42 percent hold the Certified Information Systems Auditor® (CISA®) certification and 35 percent hold the CDPSE certification. Forty-three percent of respondents are in a management role, 26 percent are in senior leadership positions, 21 percent are individual contributors and 10 percent are in executive leadership positions. **Figure 1** shows additional information about survey respondents.

FIGURE 1: Respondent Demographics



Privacy Staffing

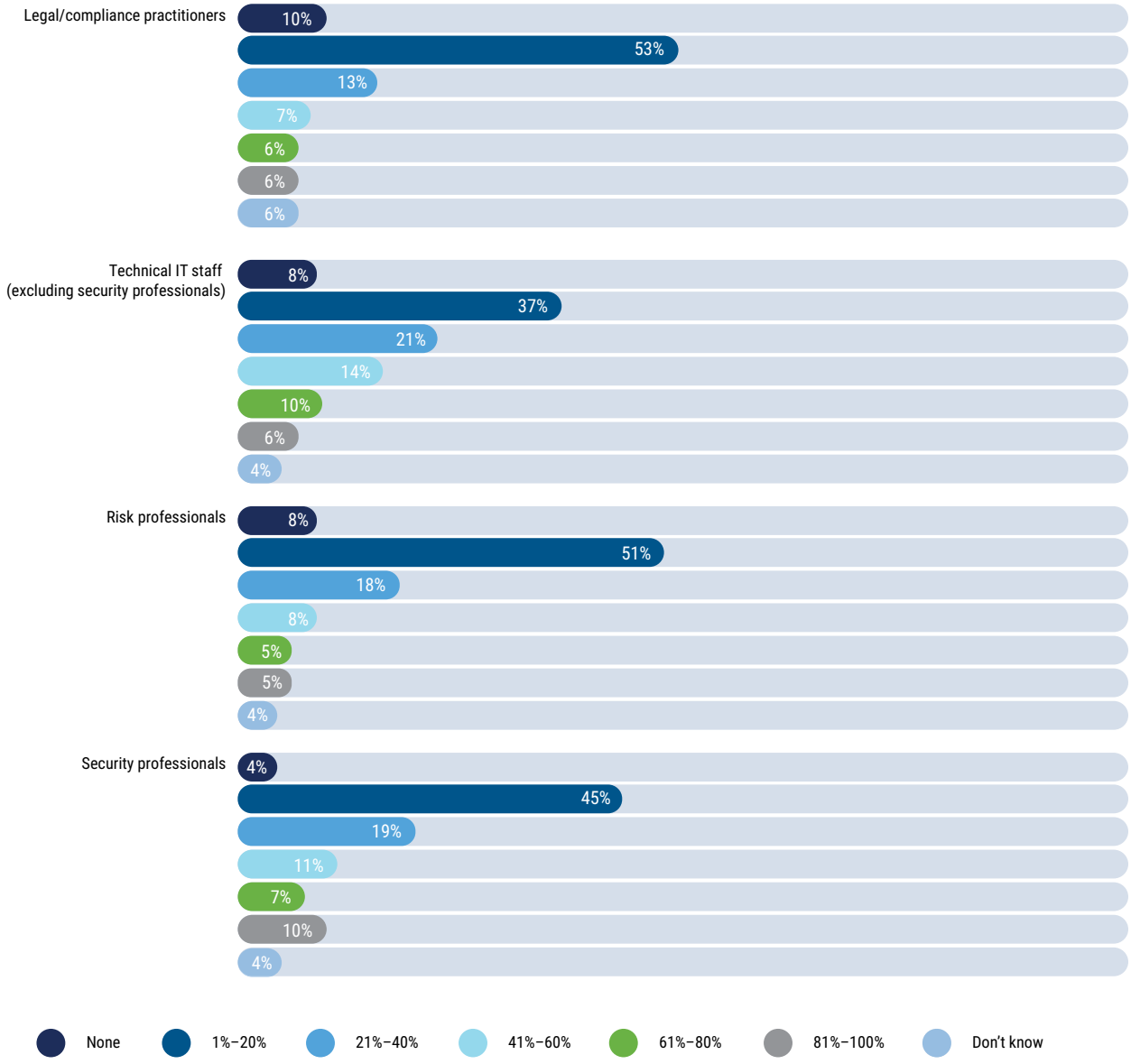
According to the survey findings, the mean number of full-time-equivalent employees who have privacy-related responsibilities within an enterprise is 26, which is slightly higher than last year's average (25).

Privacy staff roles include legal/compliance practitioner, technical IT staff, risk professional or security professional. **Figure 2** shows the percentage of staff in each of these roles.

Privacy practitioners can usually be classified into one of two groups—legal/compliance or technical. Legal/compliance privacy professionals have knowledge of the privacy laws and regulations that apply to an enterprise but may not have extensive technical expertise; technical privacy professionals have the technical expertise to apply controls that help preserve privacy and achieve compliance.

FIGURE 2: Staff Privacy Roles

What percentage of your staff are in the following roles?



Both legal/compliance and technical privacy teams are understaffed, according to the ISACA survey results. Forty-four percent of respondents indicate that legal/compliance privacy teams are somewhat or significantly understaffed, and 53 percent of respondents report that technical privacy teams are somewhat or significantly understaffed. Larger understaffing in technical privacy teams than in legal/compliance teams is consistent with previous years' findings. Although understaffing remains concerning, it has improved from last year (**figure 3**). This may be due to enterprises prioritizing privacy more compared to last year and/or increasing privacy budgets—35 percent of last year's survey respondents reported that their privacy budget would increase in the next 12 months.

Some enterprises are taking steps to address understaffing. Twenty-seven percent of respondents say that their enterprises have open legal/compliance privacy positions, and 34 percent indicate they have open technical privacy roles. Often, filling privacy positions can be time consuming (**figures 4** and **5**).

FIGURE 3: Privacy Understaffing Compared With Last Year

Understaffing of Privacy Roles

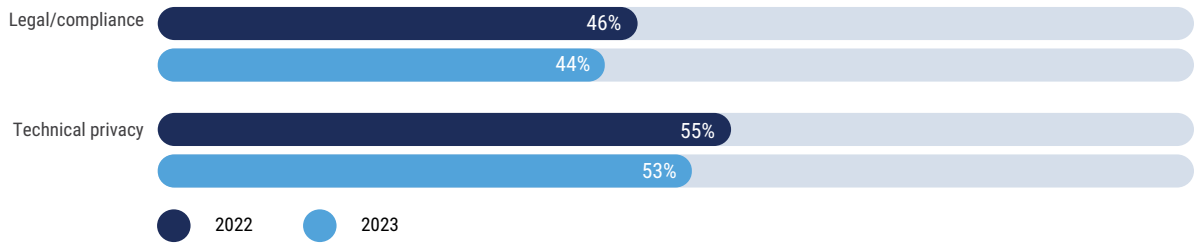


FIGURE 4: Time to Fill Open Legal/Compliance Privacy Positions

On average, how long does it take to fill legal/compliance privacy positions with a qualified candidate?

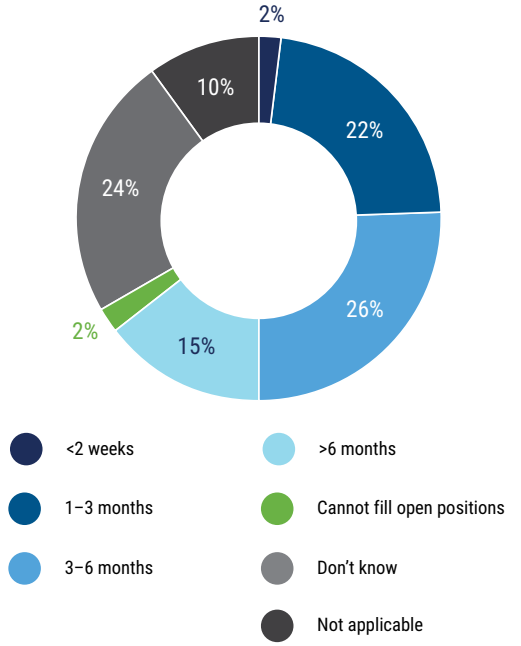
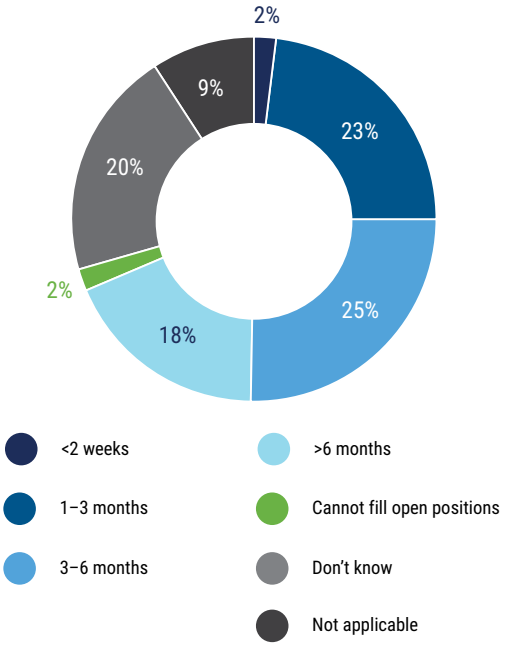


FIGURE 5: Time to Fill Open Technical Privacy Positions

On average, how long does it take to fill technical privacy positions with a qualified candidate?

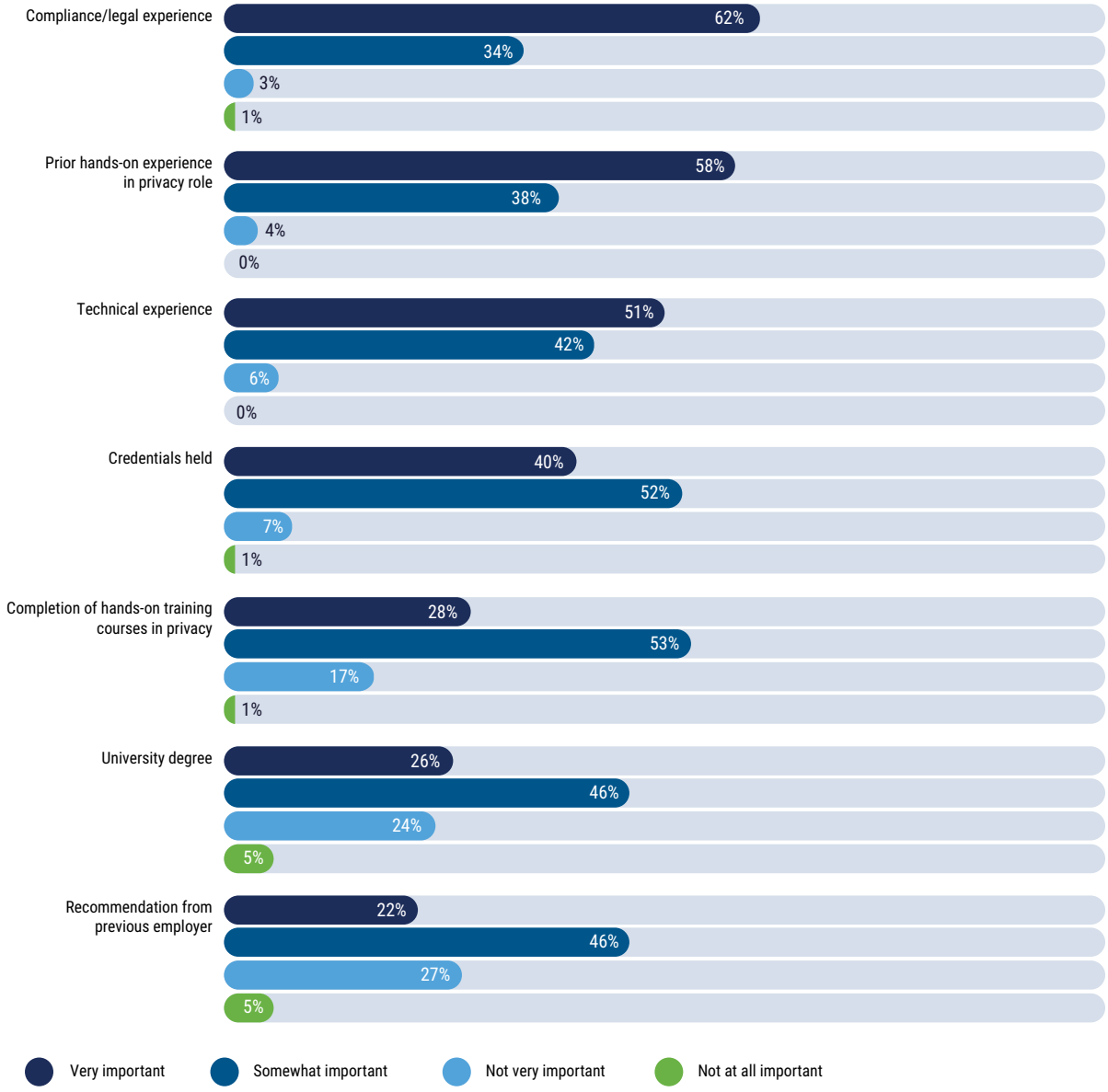


Although some survey respondents report that the time to fill open privacy positions decreased in the past year, most report that the amount of time to fill roles increased or stayed the same. For legal/compliance roles, 14 percent of respondents say that the time to fill positions somewhat or significantly decreased, 19 percent report that it significantly or somewhat increased and 31 percent say that it stayed the same. Time to fill technical privacy positions is similar, with 16 percent saying that it somewhat or significantly decreased, 23 percent saying that it significantly or somewhat increased and 30 percent indicating it stayed the same.

One challenge to quickly filling roles is a lack of qualified applicants. For approximately one-fifth of respondent enterprises, less than one-quarter of privacy-position applicants were well qualified for the positions to which they applied (for both legal/compliance and technical privacy positions). Experience is the primary factor in determining an applicant's qualifications. **Figure 6** shows the importance of factors that are used to evaluate if a privacy candidate is qualified.

FIGURE 6: Importance of Factors Determining an Applicant's Qualifications

How important are each of the following factors in determining if a privacy candidate is qualified?



According to 76 percent of ISACA survey respondents, expert-level privacy roles are the most difficult level to hire, followed by the practitioner knowledge level (51 percent) and entry-level/foundational knowledge level (12 percent).

Skill Gaps

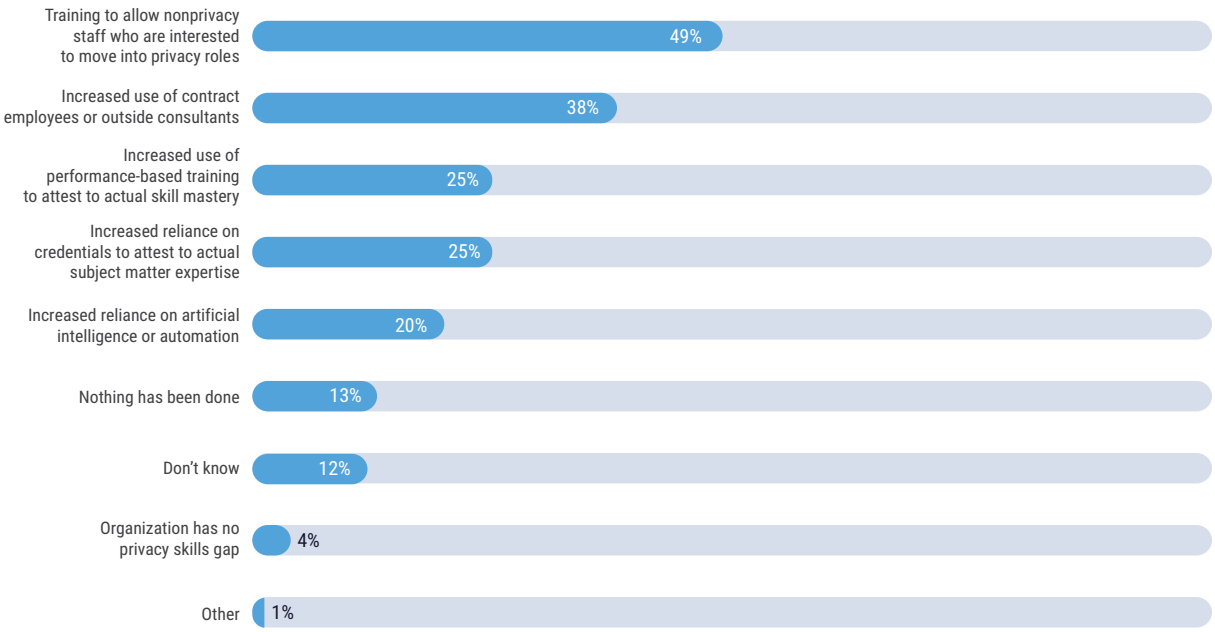
Survey respondents identify a lack of experience with different types of technologies and/or applications as the biggest skill gap in current privacy professionals (indicated by 63 percent of respondents); this aligns with the finding that experience is the most important factor when evaluating privacy-position candidates (**figure 6**). Fifty-four percent of respondents report that experience with frameworks and/or controls is a large skill gap. The next most-commonly identified skill gap is understanding the laws and regulations to which an enterprise is subject (46 percent), followed closely by a lack of technical expertise (45 percent). Other skill gaps include:

- Business insight (39 percent)
- IT operations knowledge and skills (38 percent)
- Soft skills, such as communication, flexibility and leadership (34 percent)
- Networking and/or other infrastructure knowledge and skills (33 percent)
- Business ethics (18 percent)

Enterprises are working to reduce these skill gaps. **Figure 7** shows the solutions that enterprises are applying.

FIGURE 7: Methods of Addressing the Privacy Skills Gap

Which, if any, of the following has your organization undertaken to help decrease this privacy skills gap? Select all that apply.



A challenge to quickly filling privacy roles is a lack of qualified applicants. Experience is the primary factor in determining an applicant's qualifications.

Privacy Budgets

In addition to privacy skill deficiencies, insufficient budgets contribute to the staffing challenges that privacy teams face. Forty-two percent of ISACA survey respondents report that their enterprise privacy budget is somewhat or significantly underfunded, 36 percent say it is appropriately funded, seven percent say it is significantly or somewhat overfunded and 14 percent do not know. This is a slight improvement from last year, when 45 percent of respondents felt their privacy budget was underfunded, and a larger improvement from 2021, when 49 percent of survey respondents believed their privacy budget was underfunded.

Those respondents who feel that their privacy budget is appropriately funded increased from 33 percent last year to 36 percent this year. These improvements may indicate that enterprises are beginning to recognize the importance of privacy and are taking steps to improve funding. Although the percentage of respondents that believe that their enterprise privacy budget will significantly or somewhat increase in the next 12 months decreased slightly to 34 percent—from 35 percent last year—that decrease may be due to the increased percentage of respondents who believe that their privacy budget is appropriately funded and therefore may not see a need to increase funding.

Forty-two percent of respondents report that their enterprise privacy budget is somewhat or significantly underfunded.

Twelve percent of respondents believe that their privacy budget will somewhat or significantly decrease in the next 12 months—an increase from eight percent last year—so some enterprises will likely need to scale back and make do with the limited resources they have.

Privacy Program Trends

Depending on an enterprise's structure and the skills and competencies of executives, the role accountable for enterprise privacy varies. **Figure 8** shows the role primarily accountable for privacy in survey-respondent enterprises. Twenty-one percent of respondents say the chief privacy officer is accountable for privacy. Sixteen percent of respondents say the chief information officer is accountable for privacy, and 14 percent say the executive-level security officer— e.g., chief information security officer (CISO) or chief security officer (CSO)—is accountable.

Ensuring the appropriate person is accountable for privacy is essential because this individual can help guide efforts in the event of a breach and advocate for the privacy team, including advocating for funding and other resources. This accountability also improves the alignment of privacy with other organizational objectives.

Thirty-nine percent of respondents say that a lack of executive or business support is an obstacle to forming a privacy program, and 38 percent of respondents say that a lack of visibility and influence in the organization is an obstacle—these challenges can be mitigated by having a strong C-level privacy advocate. **Figure 9** shows additional challenges enterprises face when forming a privacy program.

FIGURE 8: Accountability for Privacy

Who is primarily accountable for privacy in your organization?

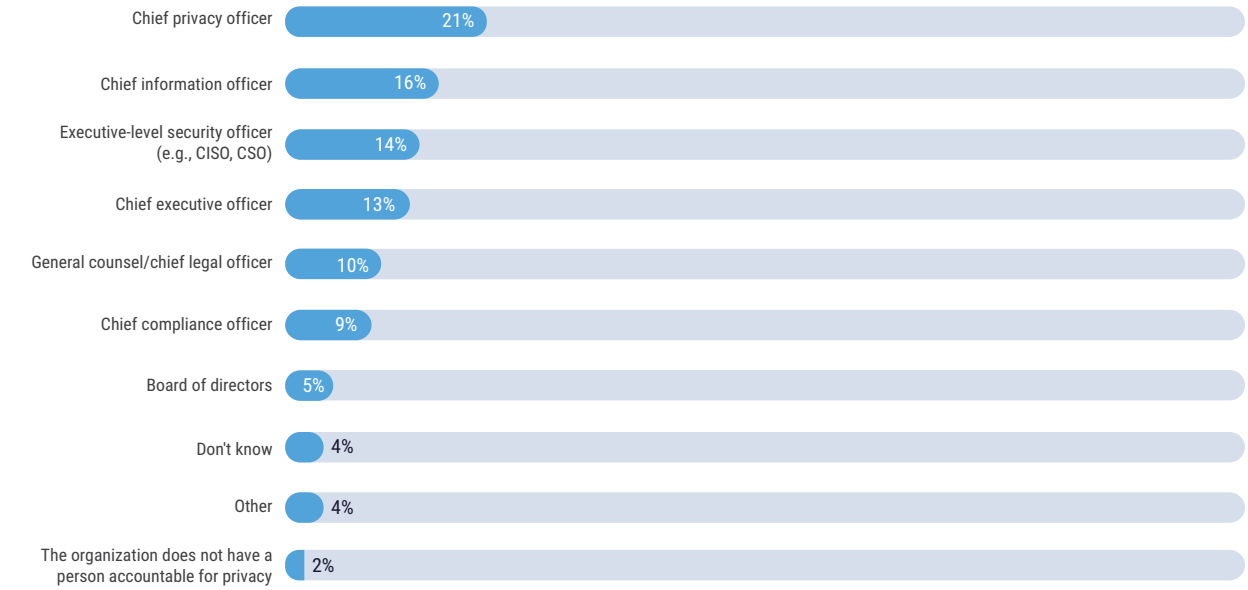
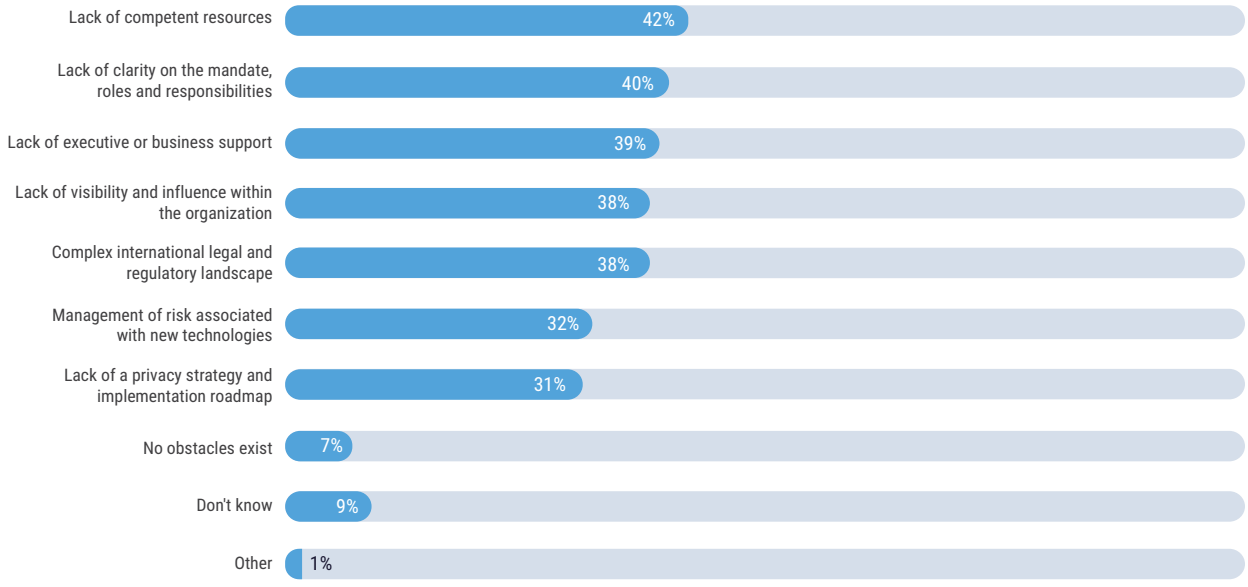


FIGURE 9: Obstacles to Forming a Privacy Program

Which, if any, of the following are obstacles faced by an organization in its ability to form a privacy program? Select all that apply.



Privacy Team Interaction With Other Areas

Given the challenges of understanding the legal and regulatory landscape of privacy, it is imperative that technical privacy professionals work closely with legal/compliance privacy professionals. These teams should meet regularly to understand their legal and regulatory obligations and ensure that technical controls are in place to achieve compliance. **Figure 10** shows how frequently technical privacy professionals meet with legal/compliance privacy professionals in survey-respondent enterprises.

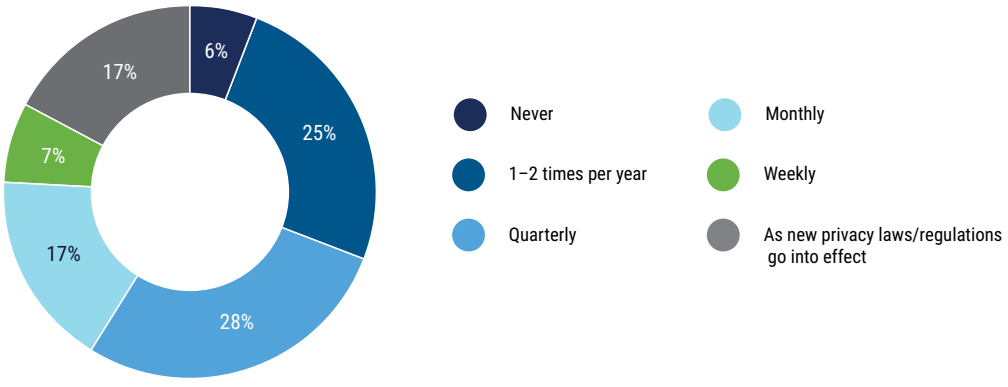
Twenty-eight percent of respondents say that their technical privacy professionals and legal/compliance privacy professionals meet quarterly, 25 percent say that these professionals meet once or twice a year and 17 percent report that they meet monthly. Another 17 percent of respondents report that their technical and legal/compliance privacy professionals meet when new privacy laws and regulations go into effect.

It is concerning that nearly one-third of respondents meet less than quarterly. The regulatory landscape is rapidly changing, and the evolution of business operations may necessitate more frequent meetings between technical and legal/compliance privacy professionals. Equally concerning is that nearly one-fifth of respondents only meet when new privacy laws and regulations go into effect; privacy efforts may be reactionary and delayed if meetings are prompted only when the compliance landscape changes.

Privacy teams must work cross-functionally to ensure privacy considerations exist throughout the enterprise. Survey respondents report that their privacy teams continually interact with information security (32 percent of respondents), legal and compliance (29 percent of respondents) and risk management (22 percent of respondents).

Privacy teams also interact regularly with IT operations and development, procurement, internal audit, human resources, sales/marketing/customer relations, finance, product/business development and public and media relations.

FIGURE 10: Frequency of Meetings Between Technical and Legal/Compliance Privacy Professionals
How often do technical privacy professionals meet with legal/compliance professionals to understand legal and regulatory requirements?



Boards of Directors' Privacy Involvement

A board of directors' approach to privacy can greatly impact the day-to-day operations of a privacy team. Most survey respondents believe that their board of directors adequately prioritizes privacy. Fifty-five percent of respondents believe that their board adequately prioritizes privacy, 22 percent do not believe that their board prioritizes privacy and 20 percent do not know. (Three percent responded that it is not applicable.) The seemingly large percentage of respondents who do not know if their board prioritizes privacy may be due to a lack of communication from the board. This result may also signal a disconnect between a board's expression of support for privacy and its lack of actions that show that support.

Boards may view privacy from a few different perspectives. **Figure 11** shows how boards of directors may view privacy programs.

There are many concerns associated with having a purely compliance-driven privacy approach. The global privacy landscape is evolving rapidly. Organizations whose primary focus is achieving compliance may find themselves struggling to catch up. A purely compliance-driven view of a privacy program may signal that privacy initiatives are reactive rather than proactive—privacy teams may always feel a step behind compliance and unable to work best to protect data subjects' privacy.

Monitoring Privacy Programs

It is crucial that enterprises monitor their privacy programs. Regular monitoring helps enterprises identify and evaluate what they are doing well and areas for improvement. As enterprises increase privacy-program monitoring, they can see how their privacy programs evolve. **Figure 12** shows the common ways of monitoring the effectiveness of privacy programs.

> A board of directors' approach to privacy can greatly impact the day-to-day operations of a privacy team.

Thirty percent of respondent enterprises evaluate the number of privacy incidents as a metric to indicate the effectiveness of their privacy programs. This metric should be combined with another monitoring mechanism; an organization that looks solely at the number of privacy incidents will not know about its privacy program weaknesses until an incident happens, at which point the reputational damage and loss of trust may be irreversible. Significant fines can also result from privacy incidents, so it is best to use forward-looking metrics to evaluate the effectiveness of a privacy program to avoid these high penalties.

FIGURE 11: How Boards of Directors View Privacy Programs

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

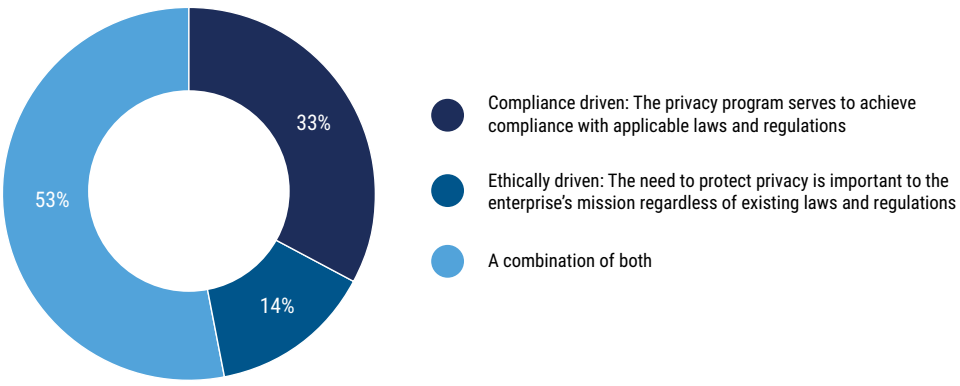
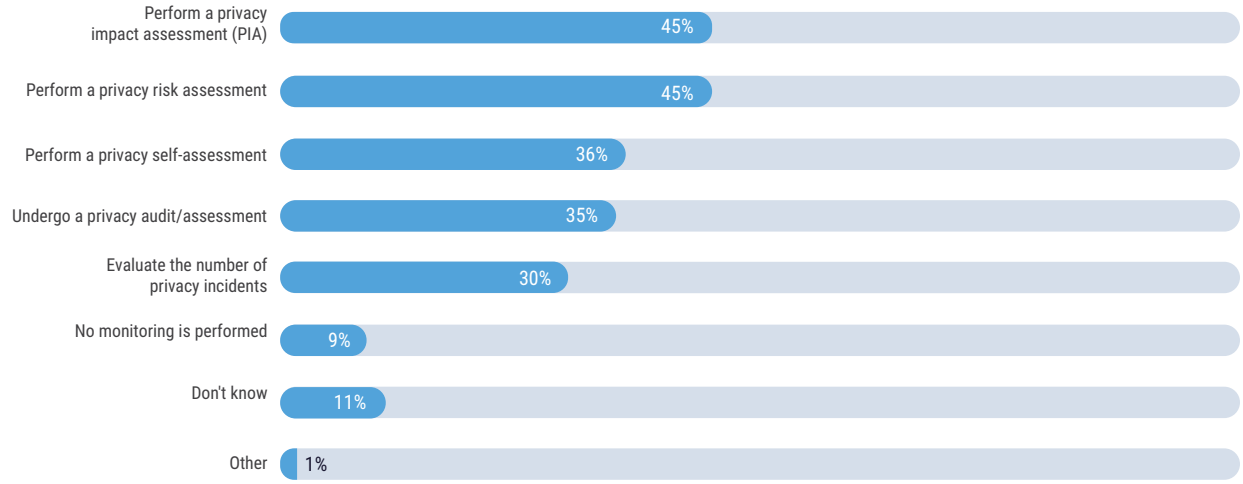


FIGURE 12: How Enterprises Monitor Privacy-Program Effectiveness

How does your organization monitor the effectiveness of its privacy program? Select all that apply.



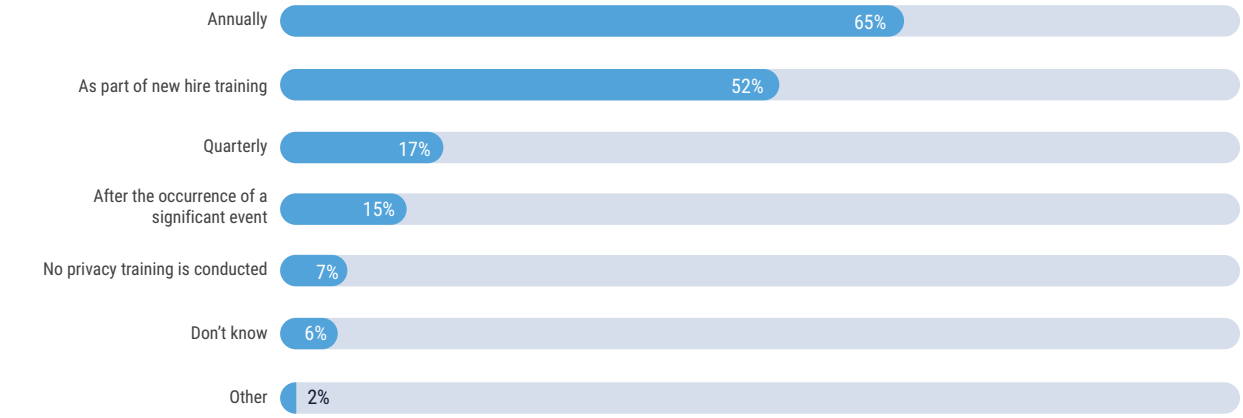
Privacy Awareness Training

Privacy teams may be small and understaffed, but everyone in an enterprise plays a role in preserving privacy, which is why privacy awareness training is so crucial. Eighty-five percent of respondent enterprises provide privacy training for employees. **Figure 13** shows the frequency with which privacy awareness training is provided.

Privacy awareness training should be provided with some regularity, and—because of the rapidly changing privacy regulatory landscape and technology—training should be reviewed and revised periodically. Fifty-nine percent of respondents say that their enterprise reviews and revises privacy awareness training annually, 24 percent review

FIGURE 13: Frequency of Privacy Awareness Training

When does your organization provide privacy training? Select all that apply.



and revise training as new laws and regulations go into effect, nine percent review it every two-to-five years and four percent do not revise their privacy training.

To evaluate if employees are benefitting from privacy awareness training, enterprises should monitor their training programs. **Figure 14** shows the metrics that respondent enterprises use to evaluate privacy training program effectiveness.

Relying solely on the number of privacy incidents and/or the number of privacy complaints received from customers is problematic because it is reactive; enterprises will not know training is ineffective until a privacy incident occurs or a privacy complaint is received. Although tracking the number of people who complete privacy training may be valuable, it does not reveal the efficacy of the privacy training; it treats training as a check-the-box exercise without evaluating if employees are learning anything from it.

Pre- and post-training assessments are a stronger metric, as they demonstrate if staff have learned from the training programs. If there is no difference or a minimal difference between pre- and post-training assessments, that may be an indicator that the privacy awareness training needs to be revised.

Most respondents believe that privacy training programs benefit their enterprise. Twenty-six percent of respondents say that privacy training and awareness programs have a strong positive impact, and 47 percent say they have some positive impact.

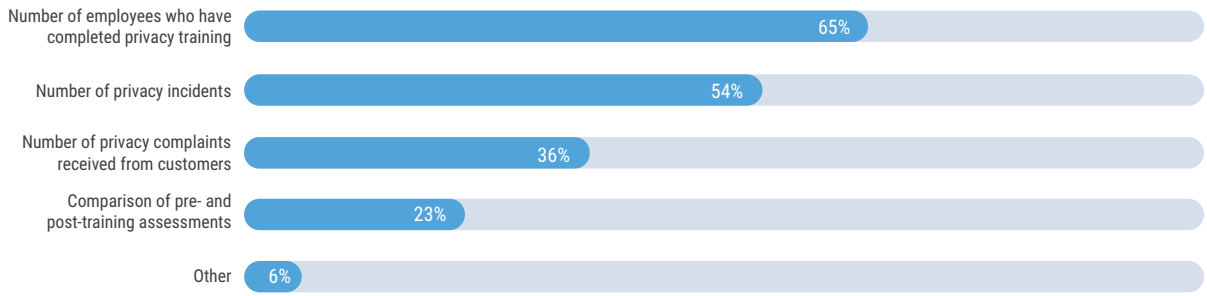
> It is impossible to have privacy without security, but security does not necessarily guarantee privacy.

In 57 percent of respondent enterprises, privacy awareness training is separate from security awareness training, while 31 percent of respondent enterprises do not separate privacy awareness training from security awareness training.

Although privacy and security training can be combined in a way that teaches both topics, a concern is that privacy-specific topics are not covered thoroughly in combined training. It is impossible to have privacy without security, but security does not necessarily guarantee privacy.

FIGURE 14: Metrics to Evaluate Privacy Awareness Training Effectiveness

What metrics does your organization track to evaluate the privacy training program's effectiveness? Select all that apply.



Privacy Frameworks, Laws and Regulations

Eighty-two percent of respondents use a framework or law/regulation to manage privacy in their enterprises. For 73 percent of respondents, it is mandatory to address privacy with documented privacy policies, standards and procedures. The top-three frameworks and regulations most commonly used to manage privacy are:

- General Data Protection Regulation (GDPR): 50 percent
- US National Institute of Standards and Technology (NIST) Privacy Framework: 46 percent
- ISO/IEC 27002:2013 Information technology—Security techniques—Code of practice for information security controls: 36 percent

Unsurprisingly, regional variations exist for the frameworks and regulations used to manage privacy. Seventy-nine percent of European respondents use GDPR. It may be surprising that only 79 percent of respondents in Europe use GDPR, but this may be partially attributable to Brexit. Sixty-one percent of respondents in the United States use the NIST Privacy Framework.

Given the myriad privacy laws and regulations in effect, some enterprises struggle to identify and understand their privacy obligations. Twenty-three percent of ISACA survey respondents say that it is difficult or very difficult to identify and understand their privacy obligations. This finding emphasizes how important it is for technical privacy professionals to meet with legal/compliance privacy professionals on a regular basis, as many technical privacy experts do not have the legal background to understand the specific provisions of laws and regulations.

> Almost a quarter of the survey respondents find it difficult or very difficult to identify and understand their privacy obligations.

A previous section in this report revealed that privacy budgets appear to be more adequately funded this year than last year, and understaffing seems to be improving. Part of the reason for this may be that enterprises felt the strain on their privacy teams and increased privacy budgets and staff sizes accordingly. This strain may be caused partially by an increase in data-subject requests. Thirty-four percent of respondents say that the number of data-subject requests has somewhat or significantly increased.

Privacy Breaches and Failures

Protecting data and achieving compliance with privacy laws and regulations can be challenging, but 45 percent of respondents are completely or very confident in their privacy team's ability to ensure data privacy and achieve compliance with new privacy laws and regulations. Some of this confidence may come from an understanding of common privacy failures. **Figure 15** shows these privacy failures.

Only 11 percent of respondents report that their enterprise experienced a material privacy breach in the past 12 months, which is slightly higher than last year (10 percent). Sixty-four percent of respondents report that their enterprise did not have a privacy breach, 17 percent do not know and nine percent preferred not to answer. Although the percentage of respondents who do not know may seem high, it is possible that they know a security incident occurred but are unsure if personal information was compromised. Dwell time (the time between a breach and when an enterprise discovers the breach) may have also influenced why so many respondents do not know if a privacy breach occurred. **Figure 16** shows the number of enterprises experiencing more or fewer breaches than last year.

FIGURE 15: Most Common Privacy Failures

In your opinion, which of the following are the most common privacy failures in an organization? Select all that apply.

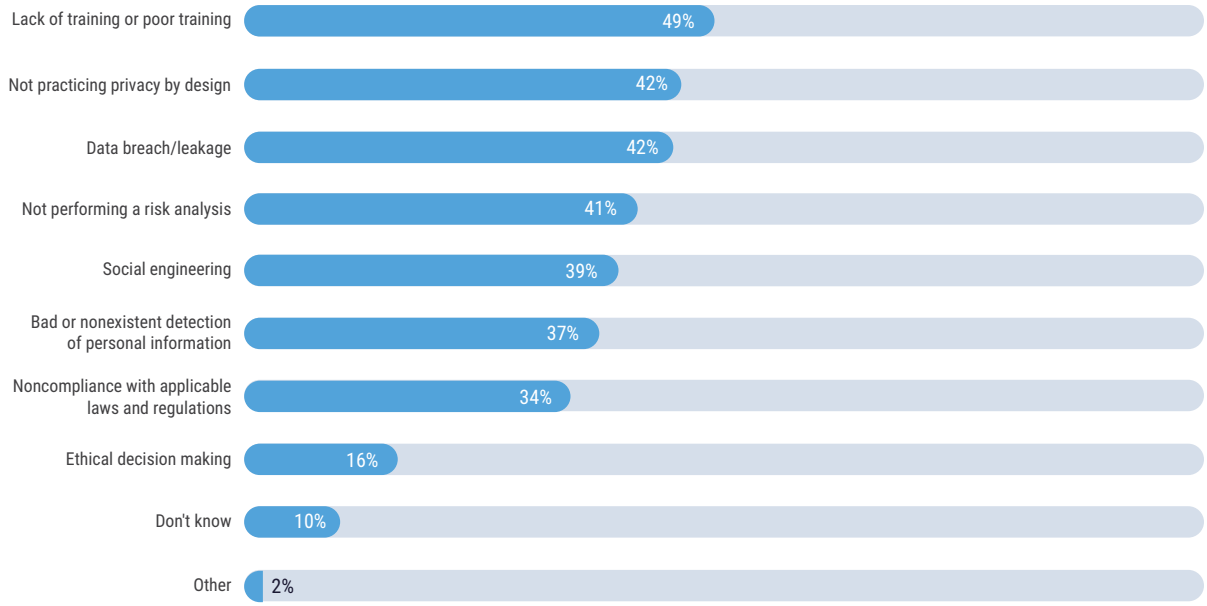
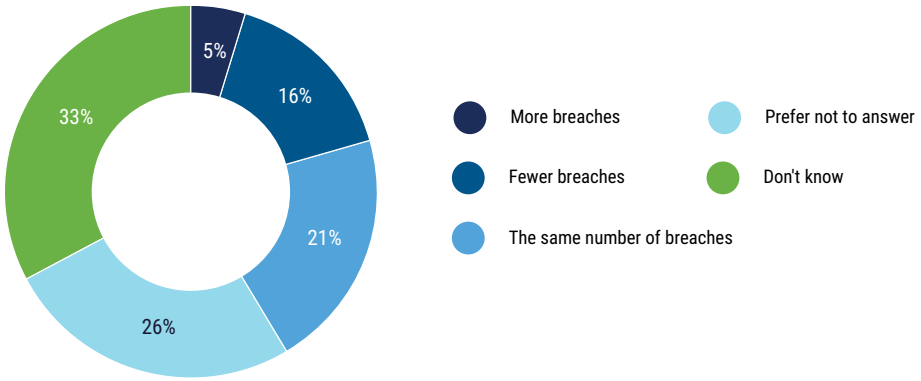


FIGURE 16: Material Privacy Breaches Compared to Last Year

Is your organization experiencing an increase or decrease in material privacy breaches as compared to a year ago?



Privacy by Design

Privacy by design is a systems engineering method that "mandates that any system, process or infrastructure that uses personal data consider privacy throughout its development life cycle and identify possible risk to the rights and freedoms of the data subjects and minimize them before they can cause actual damage."[1] **Figure 17** shows how often respondent enterprises practice privacy by design. Thirty percent of respondents indicate that their enterprises always practice privacy by design, and 30 percent of respondents say that their enterprises frequently practice privacy by design.

Some interesting trends emerge when comparing the enterprises that always practice privacy by design to the total number of respondent enterprises. Those that always practice privacy by design:

- Are more likely to separate privacy training from security training (65 percent vs. 57 percent total)
- Have survey respondents who are one-and-a-half times more likely to be completely or somewhat confident in their organization's ability to ensure the privacy of its sensitive data (65 percent vs. 40 percent total)
- Are more likely to rely on artificial intelligence (AI) or automation (25 percent vs. 20 percent total)

Given that not practicing privacy by design is viewed as a common privacy failure (**figure 15**), it is surprising that more enterprises do not always practice it. The reason may be that enterprises that always practice privacy by design are more likely to have resources that enable them to do so (**figure 18**). The median privacy staff size among enterprises that always practice privacy

FIGURE 17: Frequency of Practicing Privacy by Design
How often does your enterprise practice privacy by design?

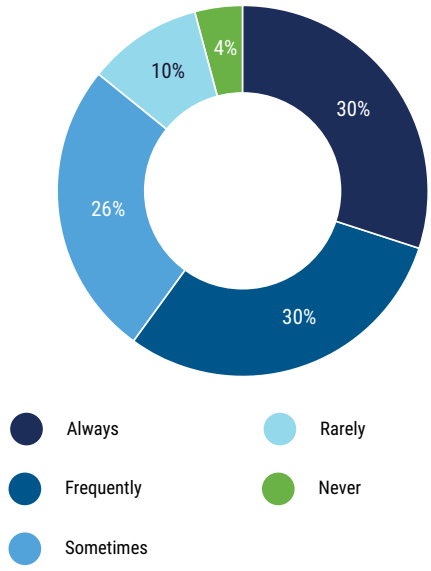
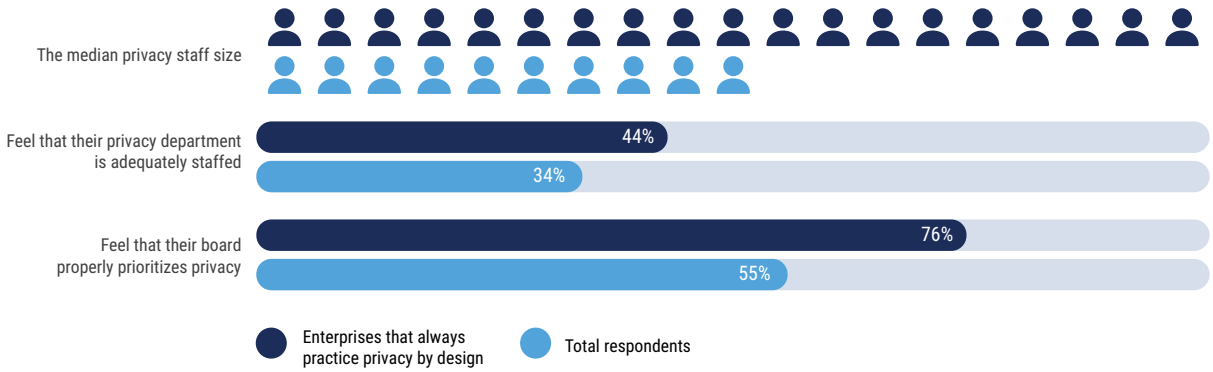


FIGURE 18: Trends in Enterprises That Always Use Privacy by Design



1 ISACA, "Eight Strategies to Help Organizations Implement Privacy by Design and Default," 21 October 2021, https://www.isaca.org/why-isaca/about-us/newsroom/press-releases/2021/eight-strategies-to-help-organizations-implement-privacy-by-design-and-default

by design is almost twice as large—19 compared to 10 for total respondents. Forty-four percent of respondent enterprises that always practice privacy by design feel that their privacy department is adequately staffed, compared to 34 percent of total respondents. It also appears that the boards of directors of enterprises that always practice privacy by design better prioritize privacy; 76 percent of these enterprises feel that their board properly prioritizes privacy, compared to just 55 percent of total respondents.

Respondents from enterprises that always practice privacy by design are significantly more likely to be completely or somewhat confident in their team's ability to ensure data privacy and achieve compliance with new privacy laws and regulations. Seventy-six percent of these respondents feel completely or somewhat confident in this ability, compared to 35 percent of total respondents.

Those who always practice privacy by design are less likely to have boards that view privacy programs as purely compliance driven (24 percent vs. 33 percent). Given that a key tenet of privacy by design is that privacy should be proactive and not reactive, and purely compliance-driven programs are often reactive, it makes sense that enterprises that always practice privacy by design do not operate reactively.

The Future of Privacy

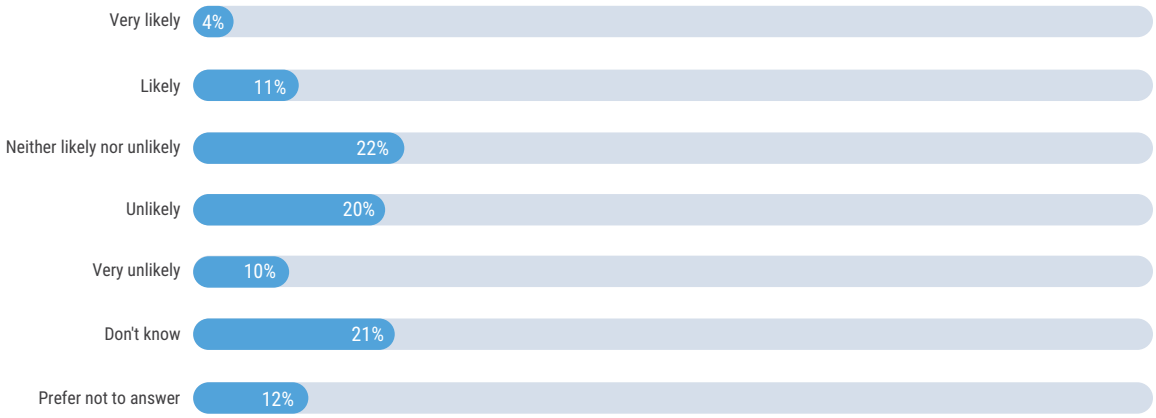
The numerous new privacy laws and regulations—and data subjects' increased attention to privacy—indicate that privacy is important, and the work of privacy professionals is crucial to an enterprise's success.

Given the various requirements privacy teams must meet and the growing number of international privacy laws and regulations, it makes sense that the demand for privacy professionals is expected to grow in the next year. Sixty-two percent of respondents say the demand for legal/compliance roles will increase in the next year, and 69 percent say the demand for technical privacy positions will increase.

A primary responsibility of privacy professionals is to respond to privacy breaches. **Figure 19** shows the likelihood of experiencing a privacy breach in the next year.

FIGURE 19: Likelihood of a Material Privacy Breach in the Next Year

How likely is it that your organization will experience a material privacy breach next year?



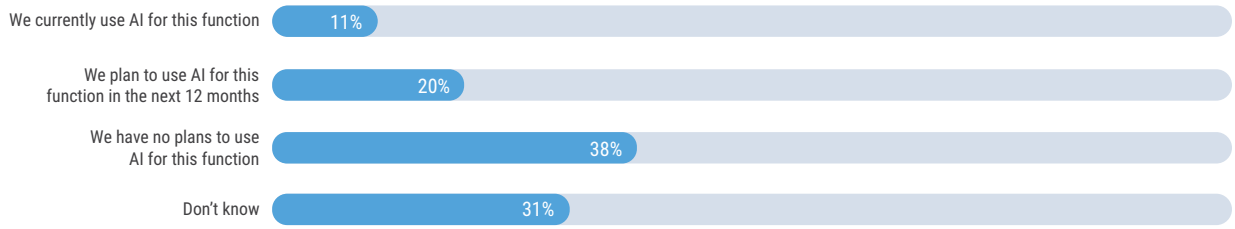
Approximately one-fifth of respondents do not know the likelihood of experiencing a privacy breach in the next year. This may indicate that privacy risk is an area that is not very mature or that enterprises are just not prioritizing it.

The challenges in hiring the right people for privacy positions and the consequences of a material privacy breach are leading some enterprises to start or plan to use AI for privacy. **Figure 20** shows respondent enterprise use of AI for privacy. More respondents use AI this year than last year, but the same number of respondents say they plan to use AI for privacy in the next 12 months.

Given the significant understaffing of privacy teams, it is surprising that nearly 38 percent of respondents do not plan to use AI. This result may be because of the privacy-related concerns associated with AI.[2] The large number of respondents who do not know of plans to use AI for privacy may also be explained by these concerns surfacing when considering AI for privacy-related functions.

FIGURE 20: Plans to Use AI for Privacy-Related Tasks

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



Conclusion

Data can provide information about an individual's health, religion, orientation, political beliefs and more. Protecting data subjects' privacy is critical to building and preserving digital trust, so enterprises must prioritize privacy accordingly. The number of privacy laws and regulations will only increase in the coming years, and making headlines for a privacy violation can damage trust with consumers.

Despite the challenges associated with data privacy, the ISACA survey reveals good news: It appears that enterprise budgets have started adjusting for the growing emphasis on privacy. Privacy teams are larger this year than they were last year. Although there is room for improvement, and many enterprises believe they need more resources, enterprises are moving toward better supporting their privacy teams.

2 Pearce, G.; "Beware the Privacy Violations in Artificial Intelligence Applications," ISACA Now Blog, 28 May 2021, https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2021/beware-the-privacy-violations-in-artificial-intelligence-applications

Acknowledgments

ISACA would like to recognize:

Board of Directors

Pamela Nigro, Chair
CISA, CGEIT, CRISC, CDPSE, CRMA
Vice President, Security, Medecision, USA

John De Santis, Vice-Chair
Former Chairman and Chief Executive Officer, HyTrust, Inc., USA

Niel Harper
CISA, CRISC, CDPSE, CISSP
Chief Information Security Officer, Data Privacy Officer, Doodle GmbH, Germany

Gabriela Hernandez-Cardoso
Independent Board Member, Mexico

Maureen O'Connell
NACD-DC
Board Chair, Acacia Research (NASDAQ), Former Chief Financial Officer and Chief Administration Officer, Scholastic, Inc., USA

Veronica Rose
CISA, CDPSE
Senior Information Systems Auditor–Advisory Consulting, KPMG Uganda, Founder, Encrypt Africa, Kenya

Gerrard Schmid
Former President and Chief Executive Officer, Diebold Nixdorf, USA

Bjorn R. Watne
CISA, CISM, CGEIT, CRISC, CDPSE, CISSP-ISSMP
Senior Vice President and Chief Security Officer, Telenor Group, USA

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

Gregory Touhill
CISM, CISSP
ISACA Board Chair, 2021-2022
Director, CERT Center, Carnegie Mellon University, USA

Tracey Dedrick
ISACA Board Chair (2020-2021) and Interim Chief Executive Officer
Former Chief Risk Officer, Hudson City Bancorp, USA

Brennan P. Baybeck
CISA, CISM, CRISC, CISSP
ISACA Board Chair, 2019-2020
Vice President and Chief Information Security Officer for Customer Services, Oracle Corporation, USA

Rob Clyde
CISM, NACD-DC
ISACA Board Chair, 2018-2019
Independent Director, Titus, Executive Chair, White Cloud Security, Managing Director, Clyde Consulting LLC, 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 more than 165,000 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 its foundation One In Tech, ISACA supports IT education and career pathways for underresourced and underrepresented populations.

DISCLAIMER

ISACA has designed and created *Privacy in Practice 2023* (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

Twitter:
www.twitter.com/ISACANews

LinkedIn:
www.linkedin.com/company/isaca

Facebook:
www.facebook.com/ISACAGlobal

Instagram:
www.instagram.com/isacanews/