ISACA®

OneTrust
PRIVACY, SECURITY & GOVERNANCE

Privacy in Practice 2022

Privacy

CONTENTS

ABSTRACT

Privacy in Practice 2022 reports the results of the ISACA® global *State of Privacy Survey*, conducted in the third quarter of 2021. This report focuses on the composition of privacy teams, the privacy workforce, privacy-related challenges and privacy by design. Some survey findings align with last year's findings, such as technical privacy roles are harder to fill than legal/compliance privacy roles. Other findings provide new insights on the privacy-related challenges that enterprises face and the creative strategies they employ to mitigate those challenges.

Executive Summary

Privacy in Practice 2022 examines enterprise privacy teams, the privacy workforce, privacy-related challenges, privacy by design and the future of privacy, based on results of the ISACA global *State of Privacy Survey*, conducted in the third quarter of 2021. The data that an enterprise collects about its data subjects have the potential to reveal a great amount of personal information. In an age when 2.5 quintillion bytes of data are created daily[1] and digital trust is becoming paramount, enterprises that demonstrate they protect data and preserve user privacy can gain a considerable competitive advantage. This paper reports on the state of enterprise privacy.

Key Findings

The following are key survey findings:

- Technical privacy teams are more understaffed than legal/compliance privacy teams.
- Technical privacy positions take longer to fill than legal/compliance roles.
- The demand for privacy professionals is expected to increase over the next year, with the demand for technical privacy roles increasing more than the demand for legal/compliance roles.
- Technical experience continues to be the biggest skill gap among privacy professionals.
- Most boards of directors adequately prioritize privacy, and most enterprise privacy strategies align with organizational objectives.
- The likelihood of privacy budgets decreasing in the next 12 months is low—many survey respondents believe that their privacy budgets will increase.
- A lack of privacy training is identified as a common privacy failure.
- Enterprises that practice privacy by design are more likely to:
  - Appropriately staff their technical privacy department
  - Have a board of directors that prioritizes enterprise privacy
  - Align their privacy strategy with organizational objectives
  - Be completely confident in the ability of their privacy team to ensure data privacy and achieve compliance with new privacy laws and regulations
  - Use the number of privacy incidents as a metric to assess effectiveness of privacy training
  - Mandate documented privacy policies, procedures and standards

Survey Methodology

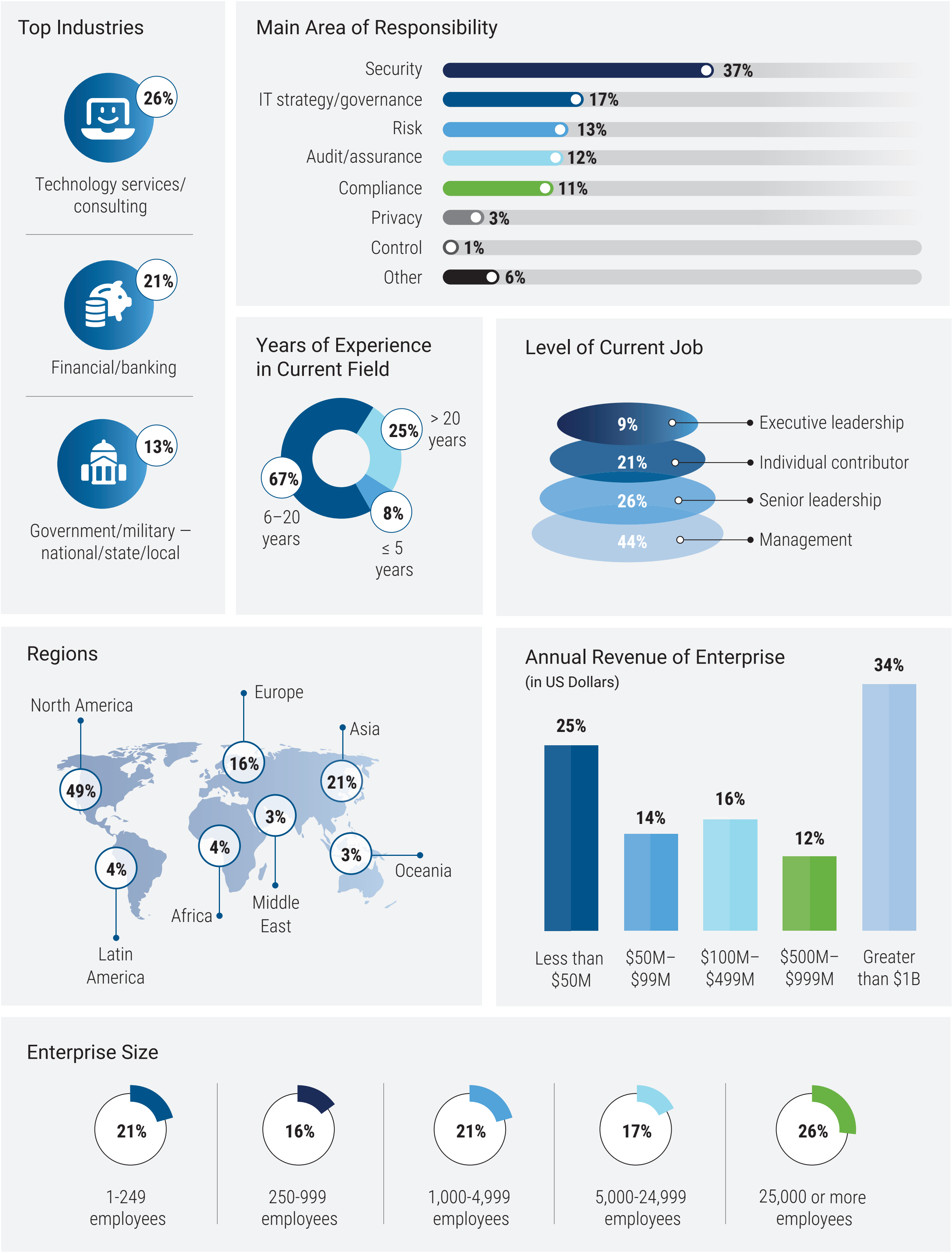
In the third quarter of 2021, ISACA sent survey invitations to approximately 27,000 ISACA constituents globally who hold an ISACA CSX Cybersecurity Practitioner Certification™ (CSX-P™), Certified Information Security Manager® (CISM®) or Certified Data Privacy Solutions Engineer™ (CDPSE™) designation or are applicants for CDPSE. Survey data were collected anonymously via Survey Monkey. A total of 832 respondents completed the survey in its entirety. Thirty-seven percent of respondents indicate that their primary professional area of responsibility is security, followed by 17 percent whose primary responsibility is IT strategy/governance. Seventy-one percent of respondents hold the CISM certification, 44 percent hold the Certified Information Systems Auditor® (CISA®) certification and 42 percent hold the CDPSE certification.

Figure 1 shows additional survey-respondent demographics.[2]

[1] Marr, B.; "How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read," *Forbes*, 21 May 2018, www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/?sh=6d28ee8f60ba

[2] Despite fewer respondents this year compared with last year, the demographic profile of this year's respondents is very similar to the demographic profile of last year's respondents. The only noticeable difference is that last year, 37 percent of respondents had five or fewer years of experience, and this year, only eight percent of respondents are in this category.

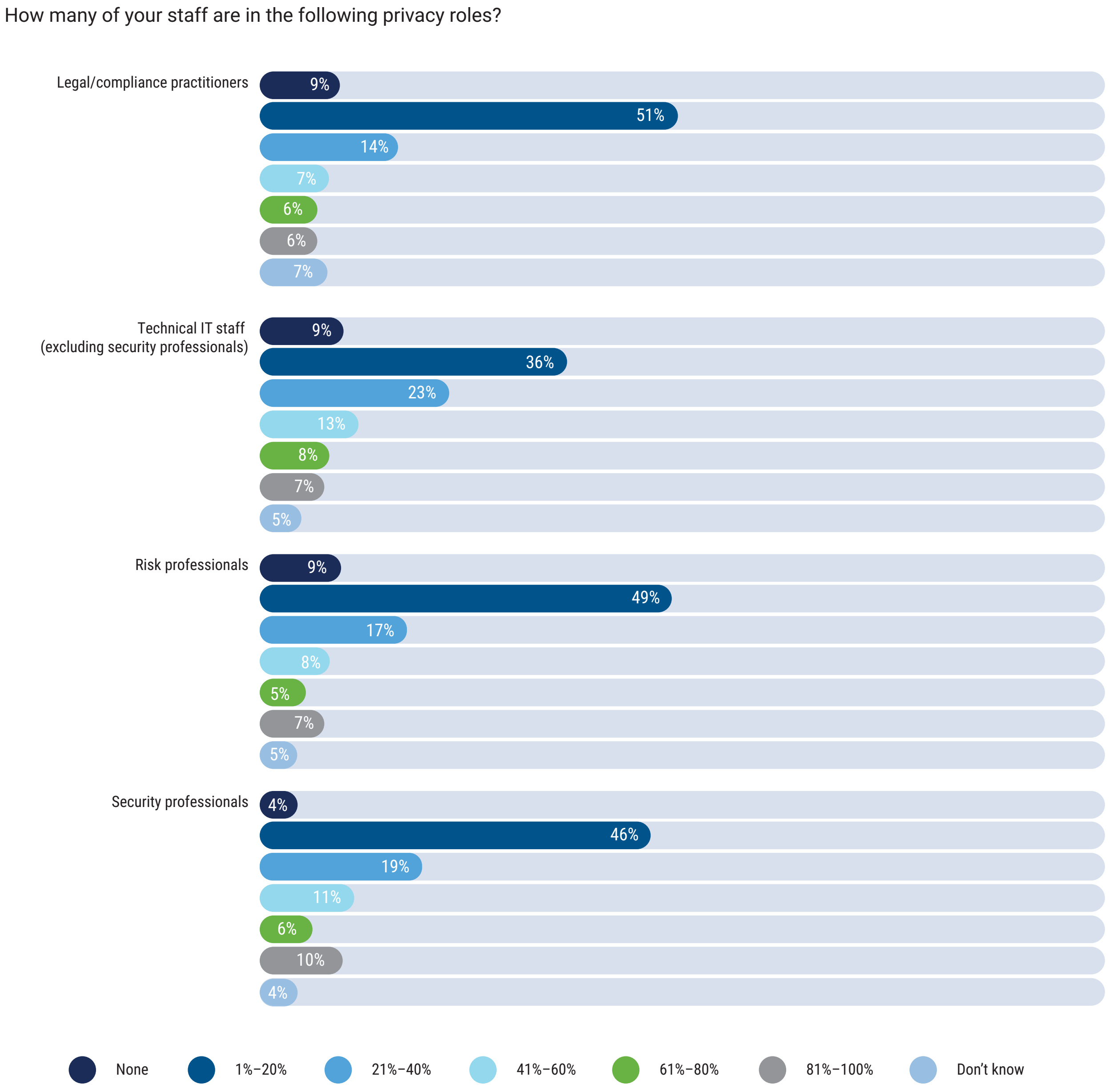
FIGURE 1: Respondent Demographics



Privacy Team Composition

Although the structure and composition of privacy teams vary based on enterprise size, industry, budget, etc., the survey found some privacy team trends across enterprises. The average number of full-time-equivalent individuals who work on privacy within enterprises is 25, and the median privacy staff size is nine. The median staff size this year is higher than last year, which was seven, indicating that enterprises understand the importance of privacy and having adequately staffed privacy teams. Privacy professionals have different roles—legal/compliance, technical IT, risk and security. **Figure 2** shows what percentage of staff are in these roles.

FIGURE 2: Staff Privacy Roles



Privacy professionals are often classified into one of two groups: legal/compliance—those who have a knowledge of the laws and regulations with which an enterprise must comply—and technical—people with an expertise in the technology that can achieve privacy objectives. ISACA survey results reveal that both legal/compliance and technical privacy teams are understaffed. Overall, understaffing issues have worsened since last year (**figure 3**). The following factors may be influencing this trend:

- The COVID-19 pandemic and the move to remote work made privacy a higher priority for enterprises.
- Given the overall lack of privacy professionals holistically and the competition for talent, privacy professionals have more job opportunities and enterprises cannot backfill positions easily upon attrition of privacy talent.

Enterprises are trying to hire talent to address this staffing issue. Twenty-five percent of respondents indicate that their enterprise has open privacy legal/compliance roles, and 31 percent say they have open technical privacy roles. Given that understaffing percentages are higher than open position percentages at enterprises, it may take a long time to remedy the lack of sufficient privacy staff.

When hiring new privacy staff, managers often look at candidate certifications to validate their expertise. The most common certification held by privacy officials or privacy office staff is CISM (52 percent). Other certifications include CISA (45 percent), Certified Information Systems Security Professional (CISSP) (36 percent) and CDPSE (36 percent).

Regardless of the exact composition and skills of a privacy team, for a privacy program to function optimally, privacy team members must interact with other departments:

- Seventy-seven percent of survey respondents report that their privacy teams always or frequently interact with information security teams.
- Sixty-six percent of respondents report that their privacy teams always or frequently interact with legal and compliance.
- Sixty-one percent of respondents report that their privacy teams always or frequently interact with risk management.

When hiring new privacy staff, managers often look at candidate certifications to validate their expertise. The most common certification held by privacy officials or privacy office staff is CISM.

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

Technical privacy teams should meet with legal/compliance professionals regularly to better understand legal and regulatory requirements and how technical teams can support compliance.

FIGURE 3: Understaffing Trends

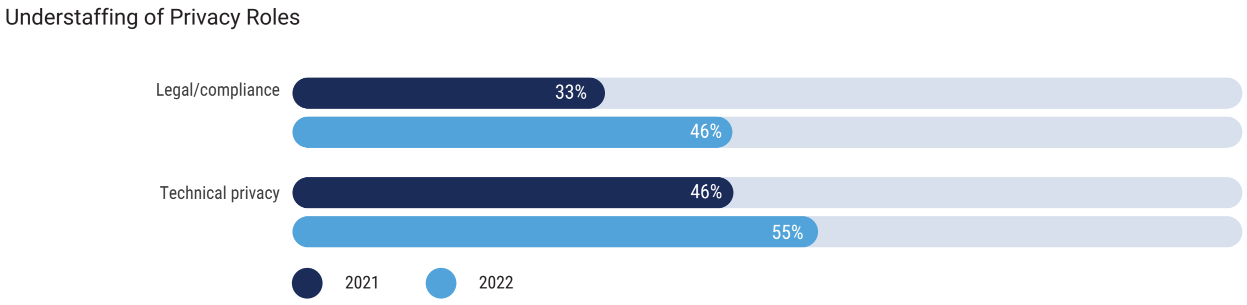


Figure 4 shows how often privacy professionals meet with legal and compliance teams.

Identifying who is accountable for privacy within an enterprise is crucial because it ensures that someone can oversee all privacy activities. In the event of a material privacy breach, that person can guide recovery efforts to ensure they align and are conducted in a way that protects the enterprise.

One-quarter of respondents say the chief information security officer or chief security officer is accountable for privacy. Twenty-one percent of respondents say the chief privacy officer is accountable for privacy, and 14 percent say the chief executive officer is accountable (**figure 5**). Three percent of respondents report that no one is accountable for privacy. This response is concerning because it indicates there may not be oversight of privacy activities. In the event of a privacy breach, recovery efforts would likely be fragmented and there might not be clear direction on how to respond.

FIGURE 4: Frequency of Technical Privacy Teams Meeting Legal/Compliance Teams

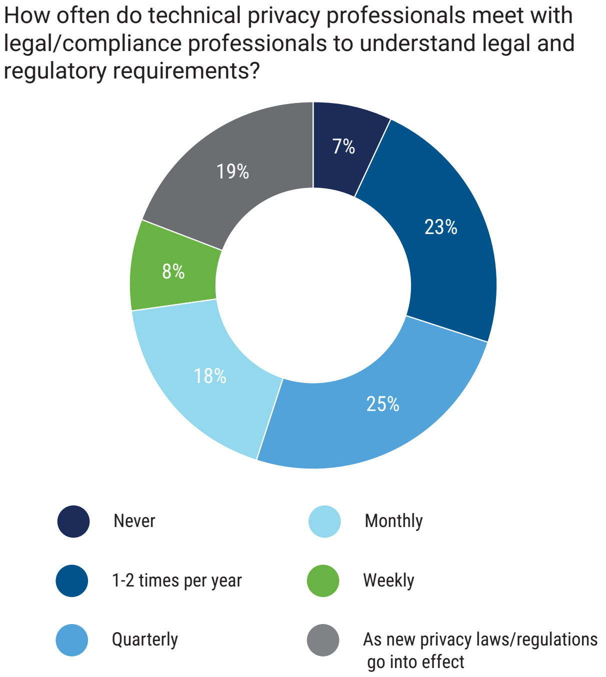
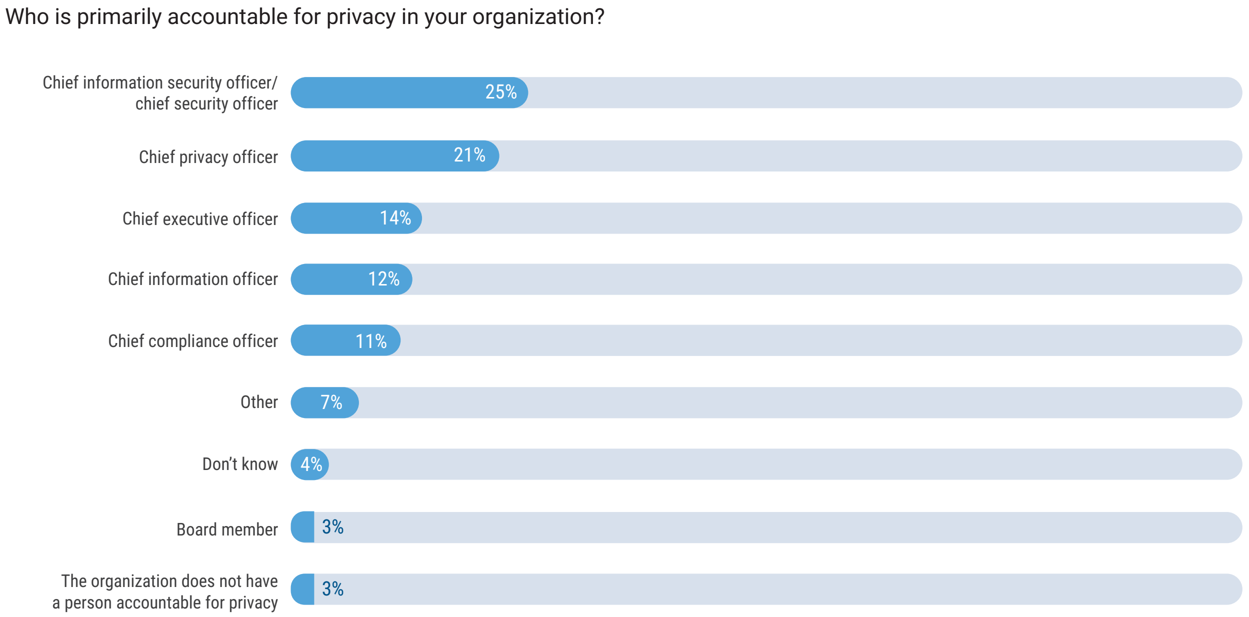

How often do technical privacy professionals meet with legal/compliance professionals to understand legal and regulatory requirements?

FIGURE 5: Privacy Accountability


Who is primarily accountable for privacy in your organization?

The Privacy Workforce

Many enterprises have understaffed privacy teams. Similar to last year, legal/compliance privacy teams (see **figure 6**) are less understaffed than technical privacy teams (see **figure 7**). Despite 46 percent of respondents indicating legal/compliance staffing shortages and 55 percent of respondents indicating technical privacy staffing shortages, only 25 percent of respondents report that their enterprises have open legal and compliance roles, and only 31 percent have open technical privacy positions (**figure 8**).

FIGURE 6: Legal/Compliance Privacy Team Staffing

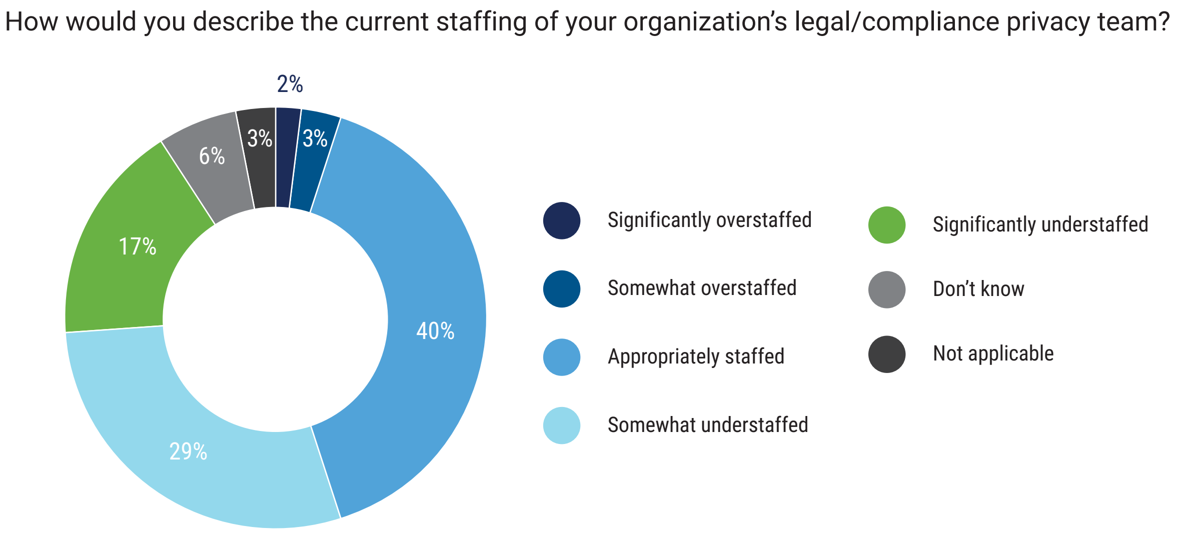


FIGURE 7: Technical Privacy Team Staffing

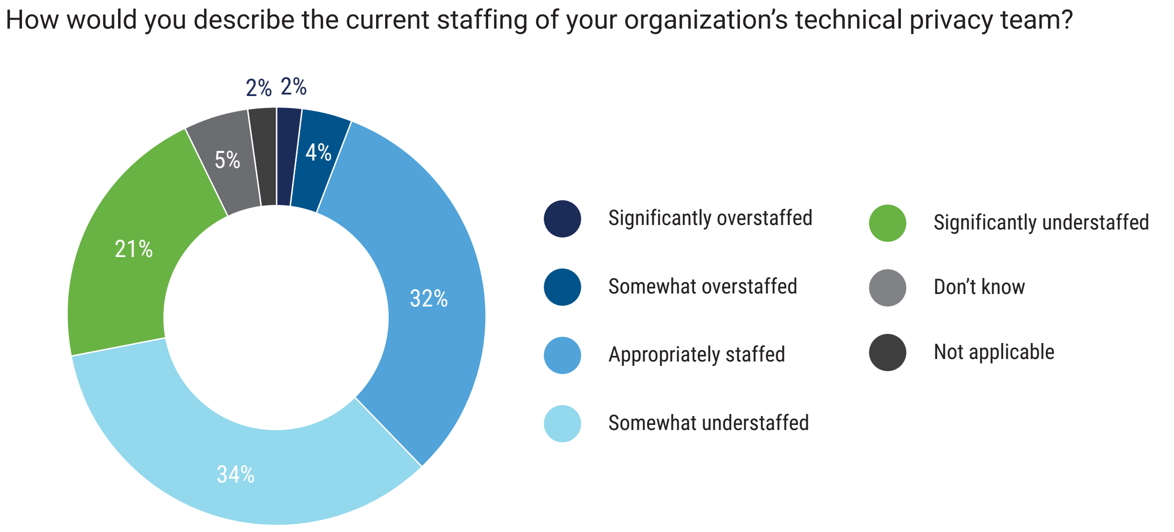
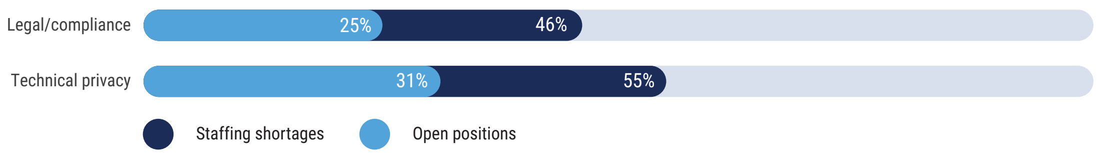


FIGURE 8: Disparity Between Staffing Shortages and Open Positions



> “The role of privacy professionals is evolving, broadening from a sole focus on compliance to encompassing building trust as a competitive advantage—helping to make companies stand out based on the values they hold and the commitments they fulfill. It’s important that we continue to monitor the changes in resources, board-level sponsorship and the positive trajectory of privacy at large. The transparency and accountability that privacy professionals help their organizations demonstrate have never been more important, as more consumers, employees and investors dictate the success of organizations that they do, or don’t, trust.”
>
> **ALEX BERMUDEZ**, FIP, CIPP/E, CIPM | DIRECTOR, ONETRUST

The finding that there are fewer open roles than identified staffing shortages indicates that understaffing issues are not likely to resolve soon. Senior management support for privacy does not always ensure funding for additional staff to meet privacy needs. Even if enterprises have posted open privacy positions, it may take a while before staffing shortages are remedied. Two percent of respondents say they are unable to fill legal/compliance roles and technical privacy roles. **Figures 9** and **10** show how long it takes to fill privacy positions. Legal/compliance and technical privacy positions take roughly the same amount of time to fill positions.

FIGURE 9: Time to Fill Legal and Compliance Privacy Roles

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

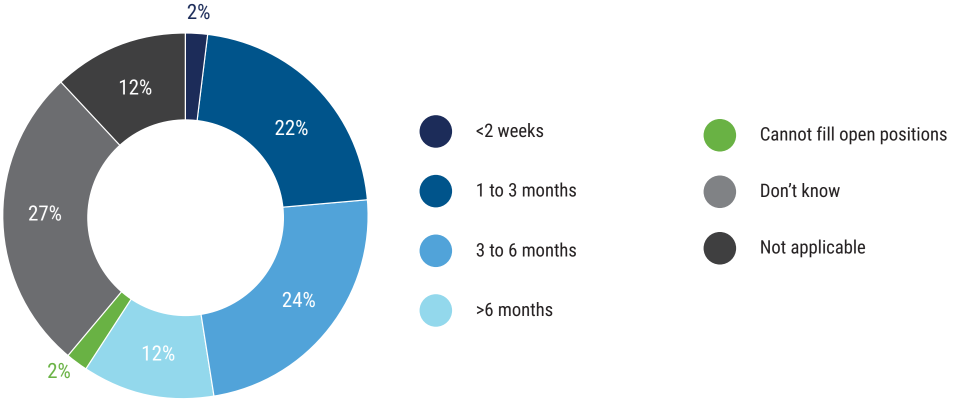
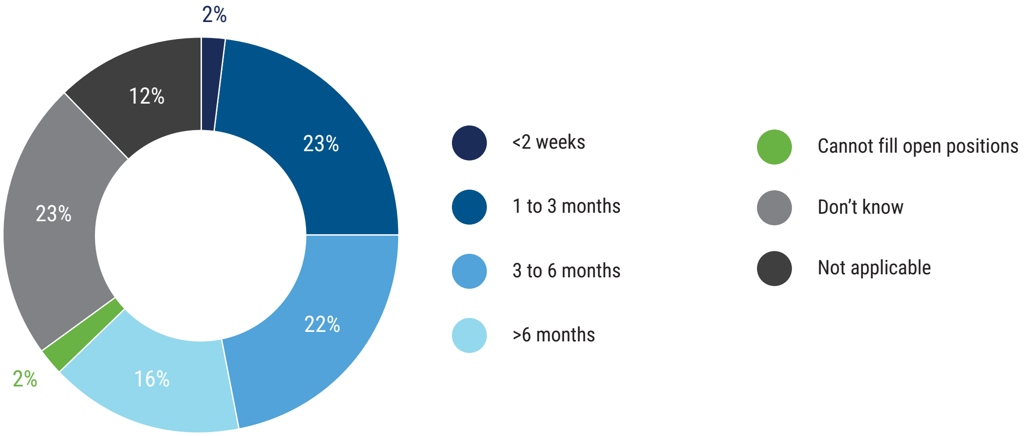


FIGURE 10: Time to Fill Technical Privacy Roles

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

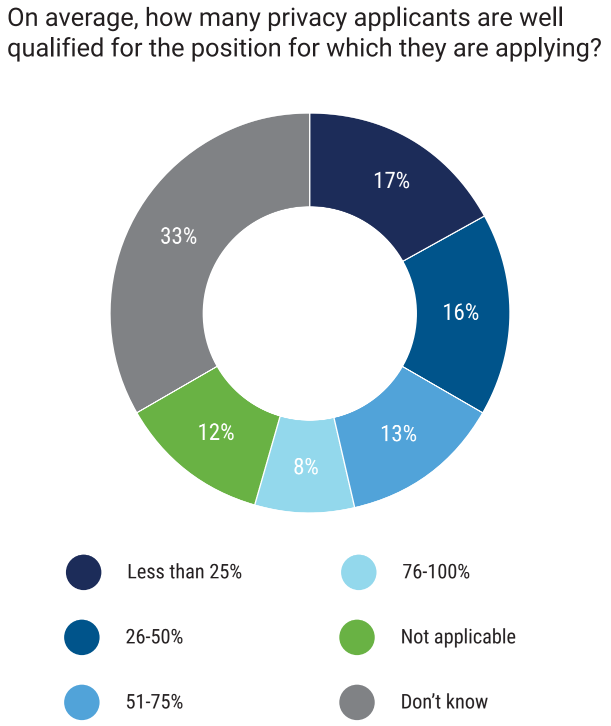


One reason the time to fill positions is so long may be the lack of qualified applicants. Only eight percent of respondents say that more than 75 percent of applicants (for both legal/compliance privacy roles and technical privacy roles) are qualified for the position they seek. **Figures 11** and **12** show the qualification of applicants for privacy positions.

One reason the time to fill positions is so long may be the lack of qualified applicants.

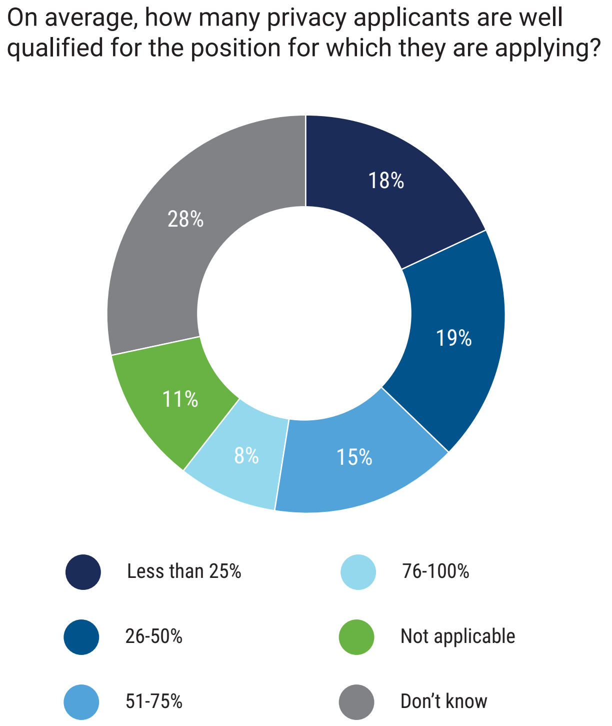
The time to fill privacy roles over the last year largely remains the same relative to a year ago. Thirty-one percent of respondents indicate that the time to fill open legal/compliance privacy positions has stayed the same, while 29 percent indicate that the time to fill technical privacy positions has stayed the same. Sixteen percent of respondents say that the time to fill open legal/compliance privacy positions in the last year either somewhat or significantly increased. Nineteen percent of respondents say that the time to fill technical privacy roles increased somewhat or significantly in the last year.

FIGURE 11: Qualification of Legal/Compliance Privacy Applicants



Hiring managers value experience the most when determining an applicant's abilities to do a job. Sixty-two percent of respondents indicate that compliance/legal experience is very important in determining if an applicant is qualified, 56 percent say that prior hands-on experience in a privacy role is very important and 48 percent say that technical experience is very important. Although knowledge of privacy is an important factor in determining an applicant's qualifications, that knowledge does not necessarily need to be in the form of a university degree. For example, 29 percent of survey respondents indicate that a university degree is not an important factor when evaluating a candidate.

FIGURE 12: Qualification of Technical Privacy Applicants



Experience is an important factor in hiring decisions, but it is also one of the biggest skill gaps. Sixty-four percent of respondents report that experience with different technologies and/or applications is one of the biggest skill gaps. Fifty percent of respondents report that understanding the laws and regulations to which an enterprise is subject is a skill gap, and 50 percent say that experience with frameworks and/or controls is a skills gap. The next most-commonly identified skill gap is a lack of technical expertise (46 percent). Other skill gaps include:

- Business insight (40 percent)
- IT operations knowledge and skills (35 percent)
- Networking and/or other infrastructure knowledge and skills (35 percent)
- Soft skills (31 percent)

Hiring people with the right experience for all privacy roles is difficult, but hiring experts is the most challenging. Seventy-eight percent of respondents indicate that it is most difficult to hire experts, 47 percent say it is most difficult to hire practitioners and 10 percent say that it is most difficult to hire foundation-level knowledge professionals.

The demand for privacy professionals is expected to increase (see **figures 13** and **14**), which poses a significant challenge for privacy teams that are already understaffed and indicates that staffing shortages will continue for a while. For teams that are already overwhelmed, it appears relief will not be arriving any time soon.

Hiring people with the right experience for all privacy roles is difficult, but hiring experts is the most challenging.

To combat these hiring challenges and anticipate the demand for more privacy professionals, enterprises are taking action to address the privacy skills gap. One of the most common methods to address the skills gap is to train interested non-privacy staff so that they can move into privacy roles (48 percent). Enterprises are also relying more on contract employees or outside consultants (36 percent).

FIGURE 13: Forecasting the Demand for Legal/Compliance Privacy Roles

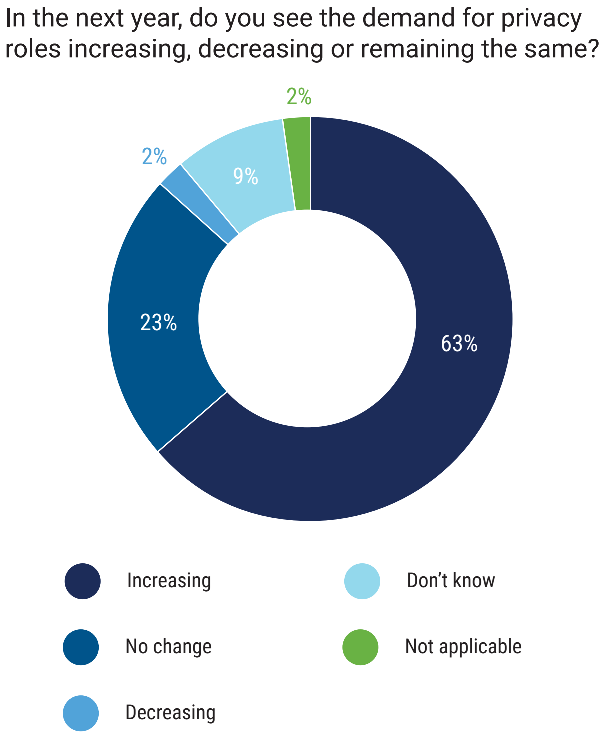
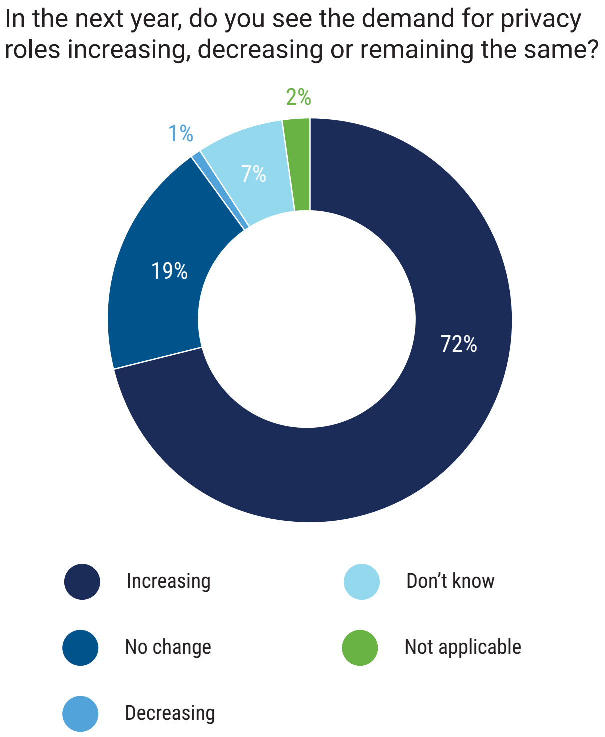


FIGURE 14: Forecasting the Demand for Technical Privacy Roles



Privacy Program Management

To ensure that a privacy program is meeting its goals and functioning as intended, enterprises need to evaluate and monitor it. **Figure 15** shows the methods that respondent enterprises use to evaluate the effectiveness of their privacy program. These findings are consistent with last year's results.

One of the biggest challenges in forming a privacy program is a lack of competent resources (41 percent). This response is not surprising considering the understaffing and skills shortages that survey respondents identify. Last year, the biggest obstacle was a lack of clarity on the mandate, roles and responsibilities (45 percent), compared to 40 percent this year. Other obstacles that survey respondents report this year include:

- Lack of executive or business support (39 percent)
- Lack of visibility and influence within the organization (38 percent)
- Complex international legal and regulatory landscape (35 percent)
- Management of risk associated with new technologies (33 percent)
- Lack of a privacy strategy and implementation road map (30 percent)

Some enterprises find it difficult to identify and understand privacy obligations. Twenty-three percent of respondents say it is difficult or very difficult for their enterprises to identify/understand privacy obligations, which helps to explain why a lack of clarity is the second-biggest obstacle to forming a privacy program. An established and organizationally agreed-on scope is essential to understanding a privacy team's mandate, roles and responsibilities. **Figure 16** shows the top 10 identified areas or controls that fall within the scope of respondents' privacy teams.

FIGURE 15: Monitoring the Effectiveness of Privacy Programs

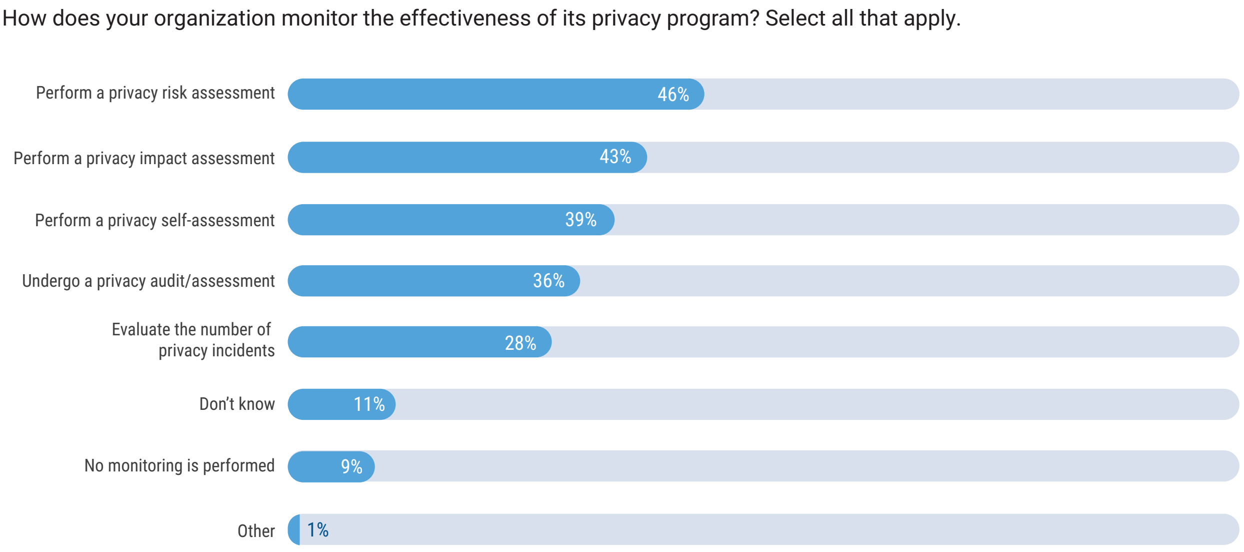
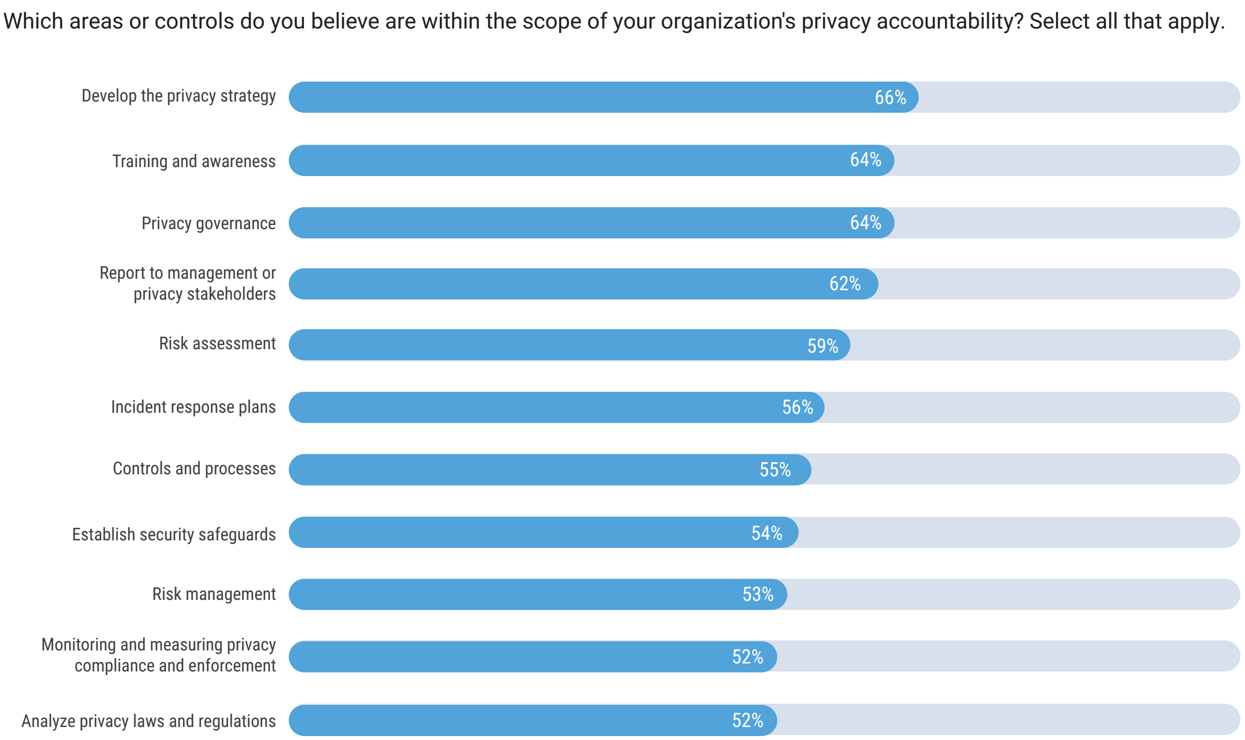


FIGURE 16: Areas or Controls Within the Scope of the Privacy Team



Privacy Prioritization

For privacy to be prioritized adequately, it needs to be top-of-mind for boards of directors. The majority of survey respondents (53 percent) feel that their board of directors adequately prioritizes privacy. Twenty-four percent of respondents do not feel that their board adequately prioritizes privacy, and 19 percent do not know.[3]

Boards may have a few ways of thinking about privacy programs. One approach to privacy is a compliance-driven approach, i.e., the purpose of a privacy program is to support compliance with applicable laws and regulations. Another approach is to think of privacy programs as serving an ethical function, i.e., the need to protect privacy is important to the enterprise mission, regardless of laws and regulations. Another approach combines the compliance-driven approach with the ethical approach by considering regulatory requirements along with the enterprise mission of protecting privacy. Fifty-one percent of respondents indicate their board of directors views privacy programs with this combination approach; 36 percent of respondents indicate that their board views privacy programs as compliance driven, and 13 percent say that their board views privacy programs from an ethical approach.

Board and executive support are crucial to achieving alignment with other organizational objectives. Without this alignment, it may be difficult to gain buy-in for privacy-related efforts. Overall, the survey findings indicate that most privacy strategies are in alignment with organizational objectives. Seventy-one percent of respondents say their privacy strategy aligns with organizational objectives.

Privacy Frameworks

Most enterprises (84 percent of respondents) use a framework or law/regulation to manage privacy. A framework or law/regulation can help ensure compliance and can provide a holistic strategy and approach to privacy. The top 10 frameworks/regulations used to manage privacy are shown in **figure 17**.

The enterprise location can affect which privacy framework or regulation is used to manage privacy. Eighty percent of respondents in Europe use the General Data Protection Regulation (GDPR) to manage privacy, and 63 percent of respondents in the United States use the National Institute of Standards and Technology (NIST) Privacy Framework.

Regardless of whether a framework or regulation is used to manage privacy or which framework/regulation is selected, enterprises should document privacy policies, procedures and standards. Seventy percent (slightly up from 68 percent last year) of respondents report that addressing privacy with documented policies, procedures and standards is mandatory; 24 percent say that it is recommended; and six percent do not know.

The regulatory landscape is constantly changing, which can make it challenging to achieve and maintain compliance. Forty-one percent of respondents are very confident or completely confident in the ability of their privacy team to ensure data privacy and achieve compliance with new privacy laws and regulations. Forty percent of respondents are somewhat confident, eight percent are not so confident and three percent are not at all confident.

Given the privacy harm that can affect data subjects and the substantial penalties that enterprises may face, many enterprises choose to apply privacy controls that exceed legal requirements, e.g., encryption and data loss prevention. **Figure 18** shows additional privacy controls that enterprises use, beyond those that are legally required. This year's responses closely mirror the responses from last year.

FIGURE 17: Frameworks/Regulations Used to Manage Privacy

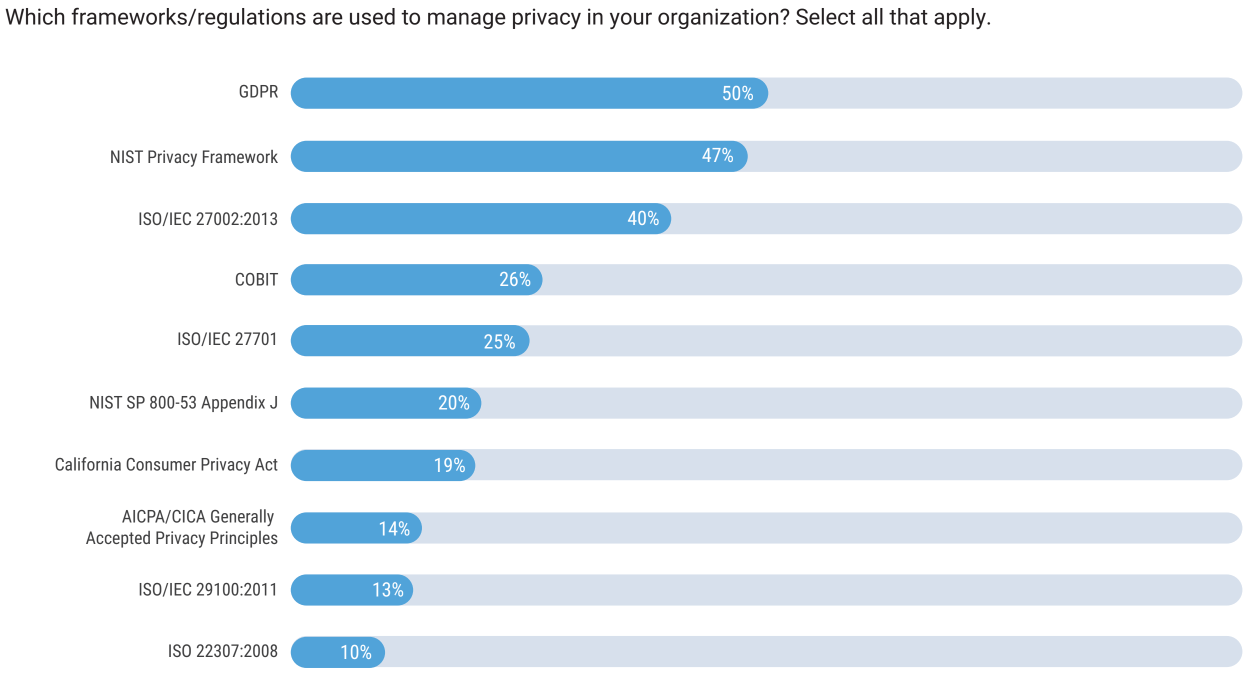
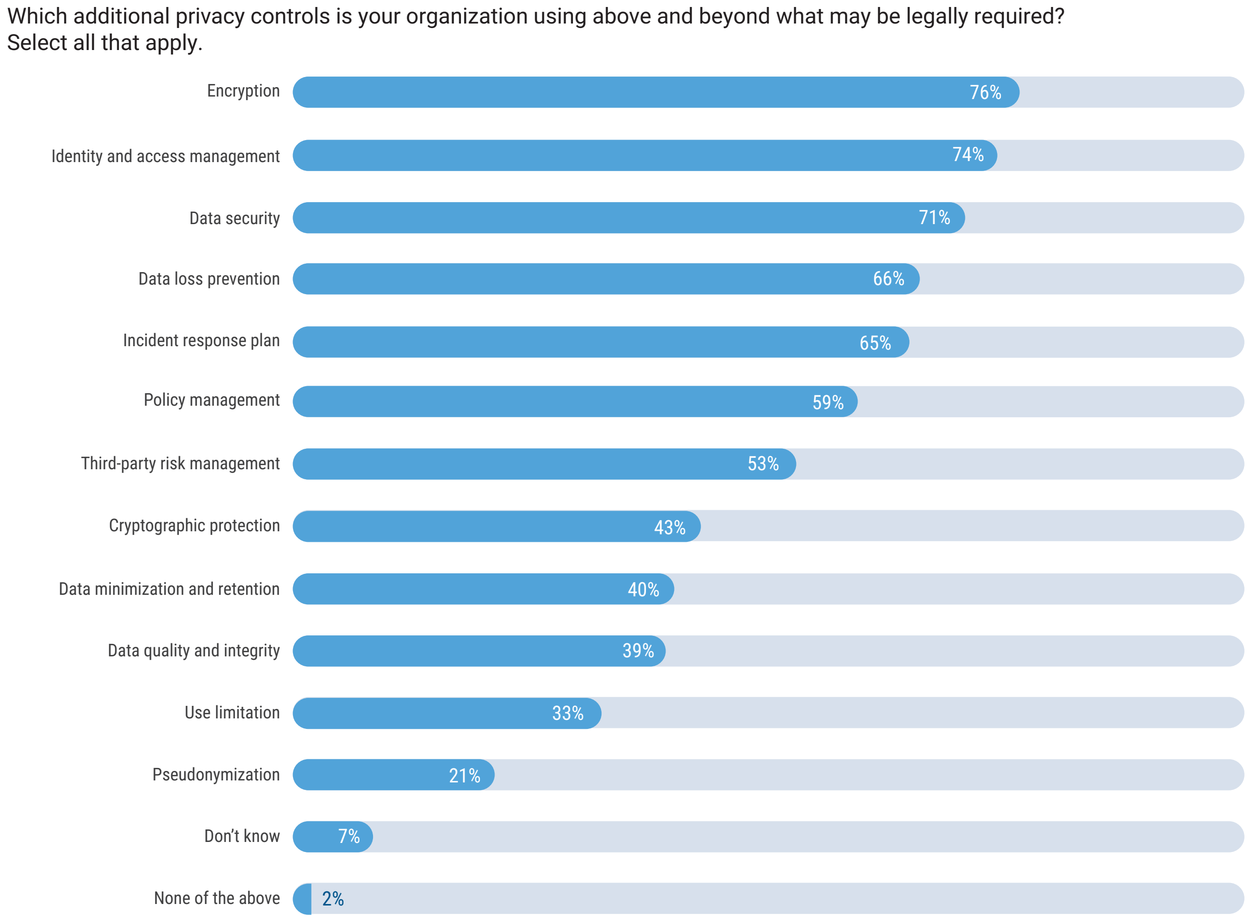


FIGURE 18: Additional Privacy Controls Used Beyond Legal Requirements

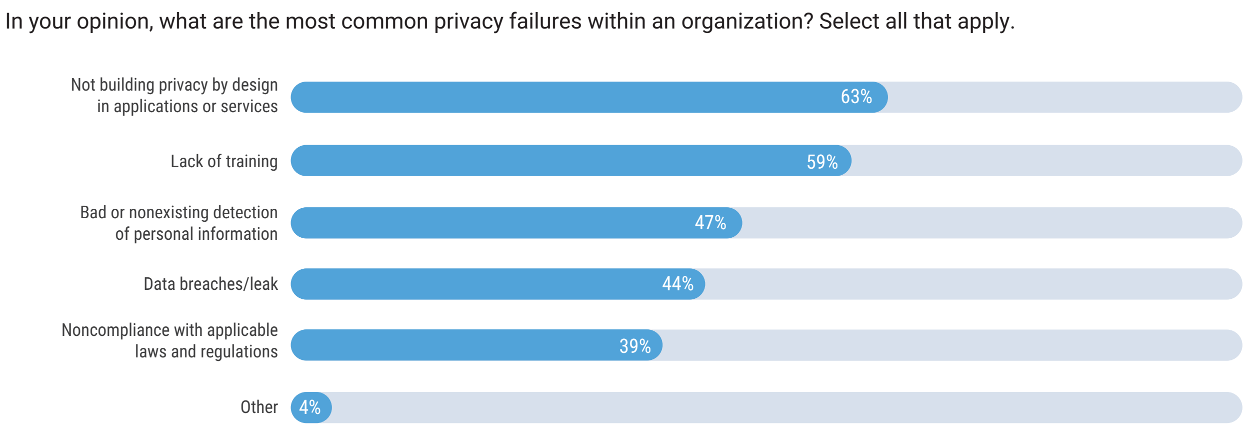


Privacy Program Challenges

Even well-managed privacy programs can experience some failures. The most common failure survey respondents identify is not practicing privacy by design, which entails considering privacy throughout the development process and using privacy as the default setting in applications and services. **Figure 19** shows other common privacy failures.

Many privacy programs are also struggling with insufficient funding. Forty-five percent of survey respondents feel that their enterprise privacy budget is underfunded. Although this response may seem high, it is a decrease from last year (49 percent of survey respondents), which may indicate that enterprises are beginning to recognize the importance of privacy and are taking steps to improve its funding. Thirty-three percent of respondents feel their budget is appropriately funded, and seven percent feel it is overfunded.

FIGURE 19: Common Privacy Failures

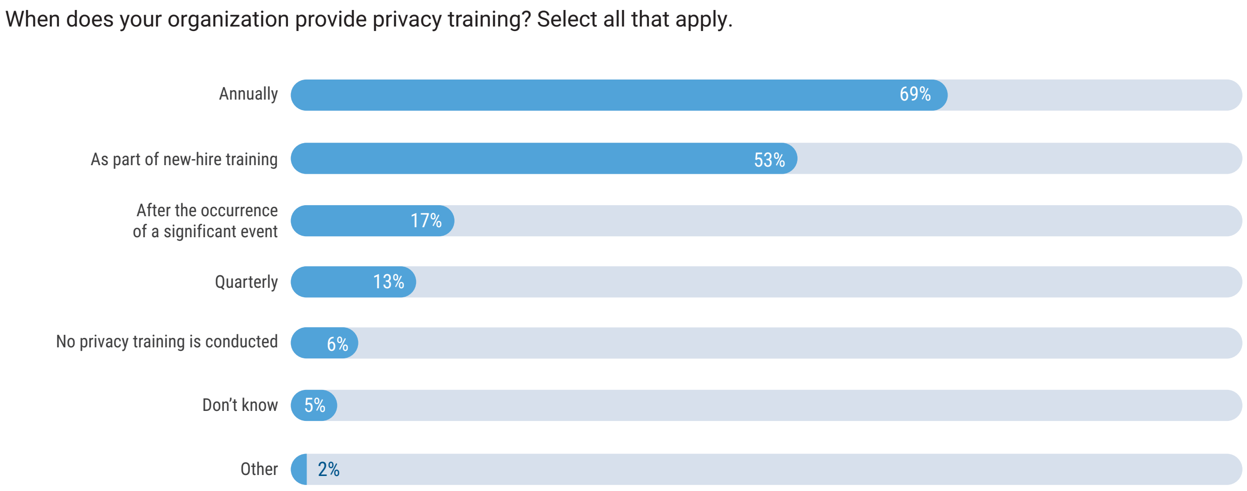


Privacy Training

Given that survey respondents identify a lack of training or poor training as a significant privacy failure, it makes sense that 87 percent of survey respondents report that their enterprise provides privacy awareness training. Ten percent of respondent enterprises do not offer privacy awareness training. **Figure 20** shows how often privacy awareness training is provided.

Although most enterprises provide privacy awareness training, 33 percent of respondent enterprises do not provide a privacy awareness training that is separate from security awareness training. Although privacy and security are related, a training that treats them the same may not give employees the information they need to best protect privacy. The survey results show that 59 percent of respondents indicate that privacy awareness training is conducted separately from security training, perhaps indicating that some enterprises understand this distinction.

FIGURE 20: Frequency of Privacy Awareness Training



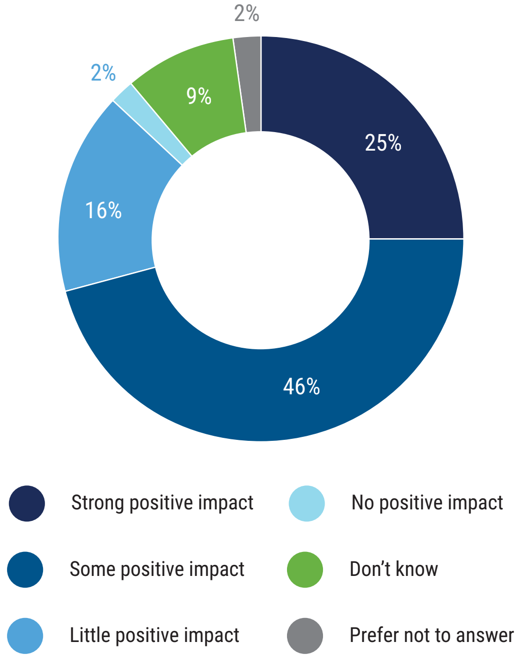
Many enterprises view privacy awareness training as a check-the-box exercise, exemplified by the fact that nearly 70 percent of survey respondents say that they evaluate the success of the privacy training program by looking at the number of employees who complete the training rather than measuring the efficacy of the training. Metrics to evaluate the effectiveness of privacy training programs include:

- Number of employees who have completed privacy training—69 percent
- Number of privacy incidents—55 percent
- Number of privacy complaints received from customers—34 percent

Regardless of which metrics an enterprise uses to evaluate the success of a privacy awareness program, most survey respondents believe that privacy training has a positive impact. **Figure 21** shows the perceived impact of privacy awareness programs on overall employee privacy awareness.

FIGURE 21: Impact of Privacy Training and Awareness Programs

What impact, if any, do you feel that privacy training and awareness programs had on overall employee privacy awareness in your organization?



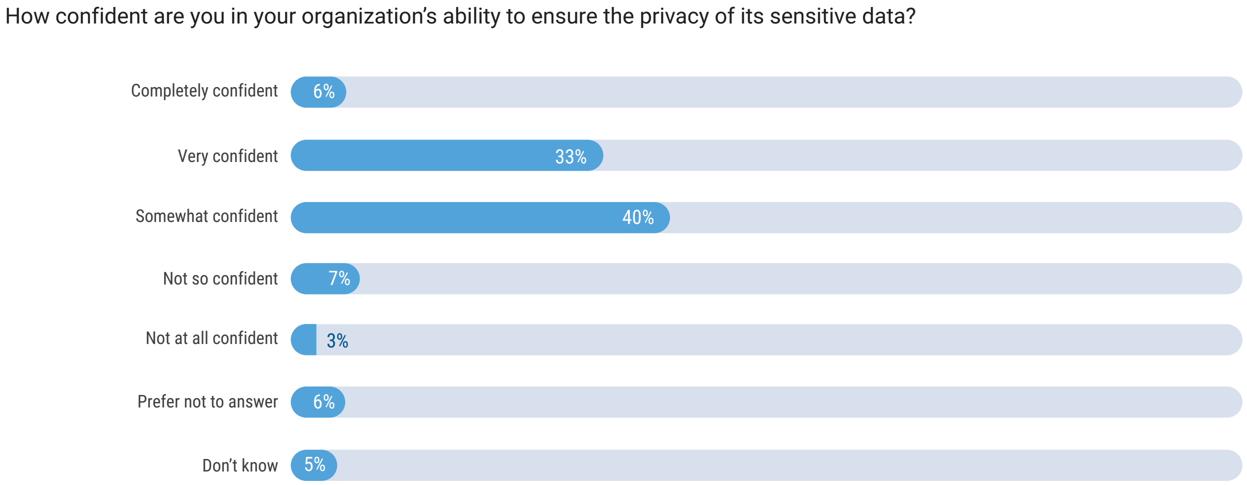
Privacy Breaches

Only 10 percent of survey respondents' enterprises experienced a material privacy breach in the last 12 months. This number is consistent with the prior-year survey findings (10 percent of survey respondents). Sixty-one percent of survey respondents report that their enterprise did not experience a material privacy breach, 19 percent do not know and 10 percent of respondents prefer not to answer.

Although the percentage of respondents who have experienced a material privacy breach remains the same as last year, only 21 percent of respondents report that their enterprise is experiencing the same number of breaches as compared to a year ago. Five percent of respondent enterprises are experiencing more breaches compared to a year ago, 14 percent of respondent enterprises are experiencing fewer breaches and 34 percent of respondents do not know. (Twenty-six percent prefer not to answer this question.)

Many enterprises feel confident about their ability to protect the privacy of sensitive data (**figure 22**).

FIGURE 22: Confidence in Ensuring the Privacy of Sensitive Data

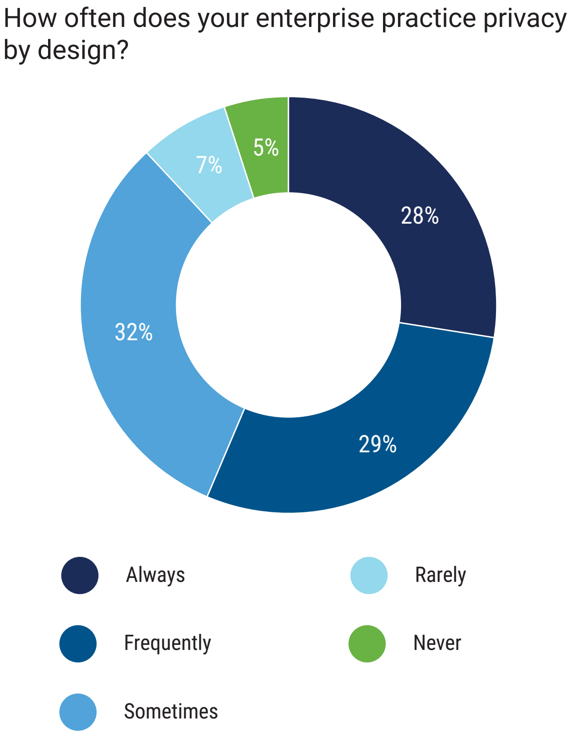


Privacy by Design

Forty-seven percent of respondents indicate that their enterprise practices privacy by design when building new applications and services, which is surprising, considering that 63 percent of respondents say that not practicing privacy by design is a common privacy failure. A reason for this discrepancy may be staffing shortages or a lack of sufficient resources to always practice privacy by design. Thirty-two percent of survey respondents say that their enterprise sometimes practices privacy by design, and seven percent say that their enterprise does not practice privacy by design. **Figure 23** shows the frequency with which privacy by design is practiced.

Enterprises that always practice privacy by design appear to have more resources, which may enable them to always practice privacy by design. Enterprises that always use privacy by design have more employees in privacy roles, with a median staff size of 12, compared to 9 for total respondents. Survey respondents from enterprises that always practice privacy by design are also more likely to say that their technical privacy department is appropriately staffed (41 percent compared to 32 percent of total respondents). Those always practicing privacy by design are more likely to feel their privacy budget is appropriately funded (47 percent vs. 33 percent total), but this is an 8 percentage-point drop from last year.

FIGURE 23: How Often Enterprises Practice Privacy by Design



In addition, 74 percent of respondents from enterprises that always practice privacy by design believe that their board of directors adequately prioritizes privacy, compared to just 53 percent of total respondents. Respondents from enterprises that always practice privacy by design are much less likely to view privacy programs as purely compliance driven (24 percent compared to 36 percent total) and are more likely to view privacy programs as a combination of ethical and compliance approaches (60 percent compared to 51 percent total). Privacy strategy is much more likely to align with organizational objectives among enterprises that always practice privacy by design (91 percent vs. 71 percent total).

Respondents from enterprises that always practice privacy by design are much less likely to view privacy programs as purely compliance driven.

Enterprises that always use privacy by design are nearly three times more likely to be completely confident in their enterprise privacy team's ability to ensure data privacy and achieve compliance with new privacy laws and regulations (26 percent vs. 9 percent total). Enterprises that always practice privacy by design are more likely to use a framework to manage privacy (90 percent vs. 84 percent total).

Enterprises that always use privacy by design are nearly three times more likely to be completely confident in their enterprise privacy team's ability to ensure data privacy and achieve compliance with new privacy laws and regulations.

Training also looks different in enterprises that always practice privacy by design. They are more likely to separate privacy training from security training (67 percent vs. 59 percent total). They are also more likely to look at the number of privacy incidents as a metric to evaluate the effectiveness of privacy training (66 percent vs. 55 percent total).

Enterprises that incorporate privacy by design are perceived to be more adequately staffed, to have privacy practices that are more rigorous, to offer better privacy training that is more likely to be distinct from security training, and to have boards that prioritize privacy. The support and resources may explain why these enterprises are able to always practice privacy by design; their boards may encourage always using privacy by design.

The Future of Privacy

Overall, enterprises understand that privacy needs to remain a priority, evidenced by the finding that privacy budgets are not expected to decrease. Only eight percent of respondents believe that their privacy budget will somewhat or significantly decrease in the next 12 months. Thirty-five percent of survey respondents believe their privacy budget will significantly or somewhat increase. Twenty-seven percent believe that the budget will stay the same. Yet, there is some uncertainty about the future of privacy budgets—29 percent of respondents say that they do not know what will happen to their privacy budgets.

Given understaffing challenges and the skills challenges, it is surprising that more enterprises are not leveraging artificial intelligence (AI) to perform privacy-related tasks. (See **figure 24.**) One reason for this hesitation may be that the use of AI may lead to privacy violations.[4]

Among enterprises that always use privacy by design, reliance on AI or automation is higher (26 percent compared to 18 percent total), which may be a result of higher confidence in their ability to ensure privacy.

Privacy breach forecasts over the next year are ambiguous. There is no clear consensus on the likelihood of experiencing a material privacy breach in the next year, which is mostly consistent with prior-year findings (**figure 25**).

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

FIGURE 24: Plans to Use AI for Privacy Tasks

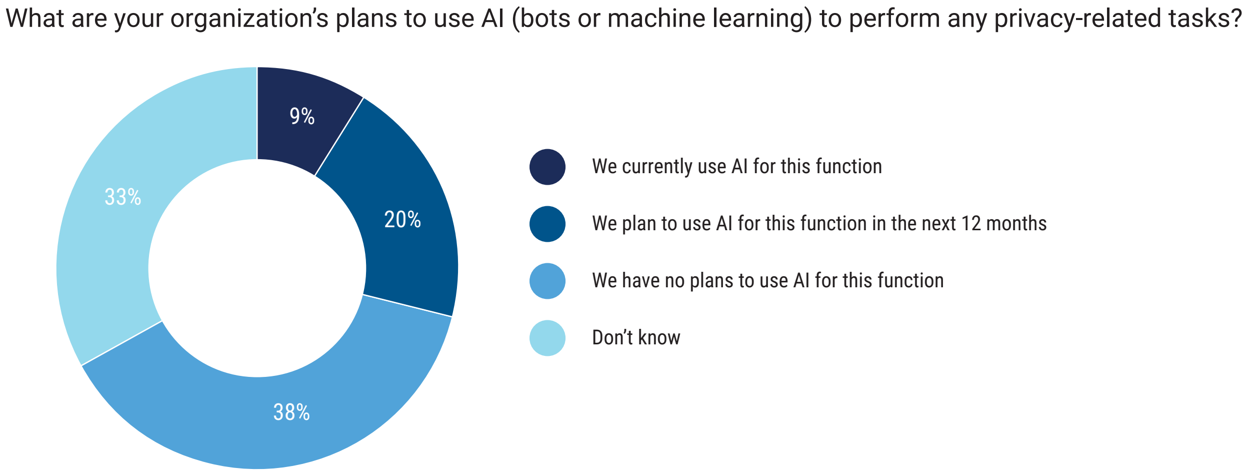
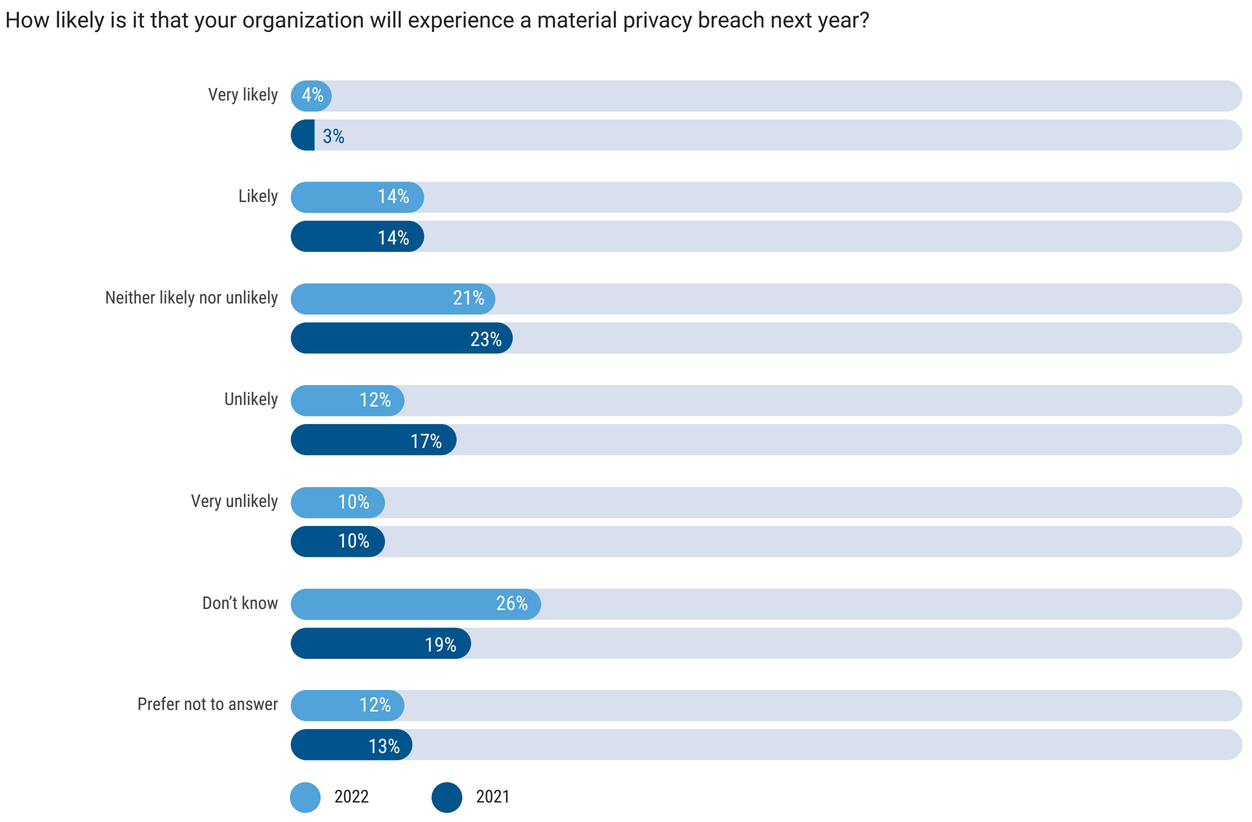


FIGURE 25: Likelihood of Experiencing a Privacy Breach



Conclusion

Trust is becoming a core competency for business.[5]

A privacy violation can irreparably damage trust and hurt data subjects and enterprises alike. Given the reputational and financial harm that comes with a privacy violation, privacy as a technology and compliance discipline is here to stay, and those working in privacy have a challenging task.

The trend toward remote work, which accelerated because of the pandemic, reinforces the importance of privacy. Fortunately, the growing emphasis on privacy by data subjects is mirrored by boards of directors who are largely prioritizing privacy and funding it appropriately.

Privacy will remain on the agendas of boards of directors, but the long time to fill privacy positions, coupled with understaffing, is concerning. With the demand for privacy professionals increasing but the time to fill vacant positions remaining long, enterprises need to take action to retain privacy staff. Enterprises that take steps to prioritize privacy—thus helping to retain employees and creatively fill open positions—can avoid privacy mishaps, retain customer loyalty and gain a competitive advantage.

[5] Taylor, L.; "Alan VanderMolen: Why Trust Must Be a Core Competency," 2 November 2021, www.provokemedia.com/agency-playbook/sponsored/article/alan-vandermolen-why-trust-must-be-a-core-competency

Acknowledgments

Board of Directors

Gregory Touhill, Chair
CISM, CISSP
Director, CERT Division of Carnegie Mellon University's Software Engineering Institute, USA

Pamela Nigro, Vice-Chair
CISA, CGEIT, CRISC, CDPSE, CRMA
Vice President–Information Technology, Security Officer, Home Access Health, USA

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

Niel Harper
CISA, CRISC, CDPSE
Chief Information Security Officer, UNOPS, Denmark

Gabriela Hernandez-Cardoso
Independent Board Member, Mexico

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

Veronica Rose
CISA, CDPSE
Founder, Encrypt Africa, Kenya

David Samuelson
Chief Executive Officer, ISACA, USA

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

Asaf Weisberg
CISA, CISM, CGEIT, CRISC
Chief Executive Officer, introSight Ltd., Israel

Tracey Dedrick
ISACA Board Chair, 2020-2021
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
ISACA Board Chair, 2018-2019
Independent Director, Titus, and Executive Chair, White Cloud Security, USA

About ISACA

For more than 50 years, ISACA® (www.isaca.org) has advanced the best talent, expertise and learning in technology. ISACA equips individuals with knowledge, credentials, education and community to progress their careers and transform their organizations, and enables enterprises to train and build quality teams that effectively drive IT audit, risk management and security priorities forward. ISACA is a global professional association and learning organization that leverages the expertise of more than 150,000 members who work in information security, governance, assurance, risk and privacy to drive innovation through technology. It has a presence in 188 countries, including more than 220 chapters worldwide. In 2020, ISACA launched One In Tech, a philanthropic foundation that supports IT education and career pathways for under-resourced, under-represented populations.

About OneTrust

OneTrust is the category-defining enterprise platform to operationalize trust. More than 10,000 customers, including half of the Fortune Global 500, use OneTrust to make trust a competitive differentiator, implementing central agile workflows across privacy, security, data governance, GRC, third-party risk, ethics and compliance, and ESG programs.

The OneTrust platform is backed by 200 patents and powered by the OneTrust Athena™ AI. Our offerings include OneTrust Privacy, OneTrust DataDiscovery™, OneTrust DataGovernance™, OneTrust Vendorpedia™, OneTrust GRC, OneTrust Ethics, OneTrust PreferenceChoice™, OneTrust ESG and OneTrust DataGuidance™. Learn more: OneTrust.com and LinkedIn.

DISCLAIMER

ISACA has designed and created *Privacy in Practice 2022* (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

Privacy in Practice 2022

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

Provide Feedback:

www.isaca.org/privacy-in-practice-2022

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/