IAPP-EY Annual Privacy Governance Report 2016

Building a better working world

Introduction

Some privacy professionals were likely beginning to feel like the Boy Who Cried Wolf, or perhaps Cassandra: The General Data Protection Regulation is coming! The General Data Protection Regulation is coming!

Yet, finally, it is here. Or it will be in May of 2018.

Now, with this second annual IAPP-EY Privacy Governance Report, the result of data provided by 600 privacy professionals across the globe, we can see that your efforts have not been in vain. Organizations around the world are getting ready — hiring DPOs, investing in training, and fretting about just how they'll operationalize things like the right to be forgotten and allowing customers to revoke their consent.

As privacy professionals, this is your time. It's no surprise that privacy is now a board-level issue for 73 percent of all organizations. It's in the news, it's being discussed at the highest levels of government, and it's increasingly being seen as a business factor that must be addressed and done well.

It's no wonder that 57 percent of you report a likely increase in budget next year.

Hopefully, this data can help you stretch that budget even further. Or, better yet, help you get a bit more budget dedicated to your team and efforts. Our hope is that it will continue to serve as a benchmarking tool and feedback mechanism for all of you to use as you go about the continuingly difficult work of operationalizing privacy by design, documenting accountability, and, well, just getting people to consider privacy as they go about product development and serving their various constituencies.

J. Trevor Hughes
CIPP, CEO and President, IAPP

Sagi Leizerov
CIPP/US, Executive Director, Privacy Practice, EY

The study was sponsored by EY. All copyrights remain those of the IAPP and the IAPP retained all editorial oversight.

Already we see privacy operations evolving. More of you have vendor management programs and more of you are happy with them. Your reporting structures are getting more diffused throughout your organizations. For the first time, at least half of you say you're consulted throughout ongoing operations and projects within your organizations.

That's progress. No doubt, it will continue.

There is clearly room for improvement. Many of you still report not having nearly enough budget to accomplish the tasks in front of you. Just how to transfer data across borders continues to be an issue that will vex the most advanced privacy operations. Small companies report almost zero insight into the product development stage.

Hopefully, this document is something you can take into high-level meetings to get you those things that will help make your privacy programs successful. Mature programs report more consultation, bigger budgets, an eye toward risk, and a connection to the brand and customers in a way that should get you excited.

That's where you're going. We'll help you get there.

Contents

1 **Executive Summary**

2 Background and Method

3 How the Job of Privacy Is Done

4 Background on Companies and Individuals

5 Privacy Group Characteristics: Structure

6 Privacy Group Characteristics: Responsibilities

7 Privacy Function in the Business Context

8 Internal and External Resources

9 Thoughts About the Profession

10 Cross Border Data Transfer

Executive Summary

For privacy and data protection professionals, 2017 may prove to be a watershed year. The leading change agent is the ramp up in preparations for the European Union's new General Data Protection Regulation, which enters into force in May 2018 to replace the EU Data Protection Directive. A privacy regulation of the GDPR's scope not only resonates globally, with a massive impact on transatlantic commerce, particularly, but also brings with it a compliance lift that challenges even the largest of firms, and can leave small- and medium-sized companies scrambling. Together with the challenges brought by the invalidation of the Safe Harbor framework and entry into force of the new Privacy Shield, all eyes will be on Europe.

In the United States, a landmark privacy overhaul initiated by President Barack Obama calls for appointment of a Senior Agency Official for Privacy (SAOP) at each federal government agency.[1] The package of revisions to the policy that governs federal information resources management (Circular A-130) also requires privacy training across departments and functions, use of privacy impact assessments, application of the Fair Information Practice Principles to personally identifiable information (PII), and SAOP oversight in information technology capital investments and budgets.

Together, the GDPR, Privacy Shield and Circular A-130 elevate the need for and role of privacy professionals as 2016 draws to a close. But that's only the leading edge of the past year's privacy developments. From Turkey to Japan, Peru to Brazil, major privacy legislation has been proposed, ushered through, or come into force. Perhaps no area of global public policy has seen as much activity as privacy and data protection.

Together with the challenges brought by the invalidation of the Safe Harbor framework and entry into force of the new Privacy Shield, all eyes will be on Europe.

In response to this activity, this second annual study of data governance in organizations, surveying modern privacy operations, confirms that privacy tasks and responsibilities are spreading steadily throughout organizational functions and initiatives. This spring, like last year, the IAPP and EY surveyed more than 600 privacy professionals, seeking input about the role and title of the privacy professional within organizations, as well as information about privacy budgets, operations, organizational structure, zones of influence, and priorities.

In addition, the survey asked respondents specifically about their strategy to address cross-border data transfers and the GDPR.

The GDPR imposes new obligations regarding data subject consent and the right to be forgotten, establishes data security standards and EU-wide breach notification rules, and requires many organizations to appoint or hire a data protection officer. The IAPP has estimated that at least 28,000 new DPO positions will be created in the coming years in response to the GDPR.[2] Now we have a document

[1] Managing Federal Information and a Strategic Resources, July 27, 2016, https://www.whitehouse.gov/blog/2016/07/26/managing-federal-information-strategic-resource.

[2] GDPR will require 28,000 DPOS in Europe, study shows, Computer Weekly, 20 April 2016, http://www.computerweekly.com/news/450283253/GDPR-will-require-28000-DPOs-in-Europe-study-shows.

of the intended response: Fifty percent of all companies surveyed reported an intention to invest in privacy training as a direct result of the GDPR, 35 percent are increasing their privacy budget, and 34 percent are increasing staffing.

The GDPR maintains the current Data Protection Directive's strict prohibition on cross-border transfer of personal data without adequate safeguards, although it more explicitly defines how organizations can establish such safeguards. In a jurisdiction — like the U.S. — that is not officially deemed to have "adequate" data protection, organizations importing protected EU data are required to use alternative data transfer mechanisms. These may include standard contractual clauses, binding corporate rules, use of a self-regulatory mechanism such as the Privacy Shield, or a number of explicitly defined derogations such as the data subject's explicit consent or pursuant to a contract with the data subject.

As this report reveals, however, many companies remain wary of Privacy Shield and are still weighing other transfer compliance options. This is especially true of small companies for whom GDPR compliance presents a formidable challenge. While 50 percent of all companies that transferred personal data between the EU and U.S. in the past used Safe Harbor, just 34 percent say they intend to use Privacy Shield in the future. At the same time, more than 80 percent of companies rely on pre-approved standard contractual clauses, which are currently under legal attack in the Court of Justice of the European Union. Although one-third of all respondents use BCRs, moreover, only 8 percent of companies with fewer than 5,000 employees see this costly data transfer mechanism as viable going forward.

This year's survey also shows signs of privacy's maturation not only as a profession but also as an industry. The privacy technology sector — still very young — is beginning to get traction and is showing signs of a promising future. Vendor management is improving, with respondents reporting an 11 percent increase over last year in the thoroughness of their programs and more than two-thirds reporting privacy involvement in vendor selection and contracting.

The political and legal upheaval of 2016 validates privacy professionals' contributions, and creates not only new privacy jobs but also more opportunities for career advancement.

The political and legal upheaval of 2016 validates privacy professionals' contributions, and creates not only new privacy jobs but also more opportunities for career advancement. More than half the organizations surveyed expect privacy budgets to grow, while 72 percent report that privacy is now a board-level concern. More than 50 percent of privacy leaders are within two rungs of the CEO position. For the first time, moreover, 50 percent of respondents report that privacy is involved throughout ongoing company operations and more than two-thirds are now regularly using privacy impact assessments (PIAs). And government survey respondents report a likely 30 percent increase in federal privacy positions in the near future.

It's no wonder, then, that 91 percent of respondents say that privacy "helps open career doors."

Contents

1 Executive Summary

2 **Background and Method**

3 How the Job of Privacy Is Done

4 Background on Companies and Individuals

5 Privacy Group Characteristics: Structure

6 Privacy Group Characteristics: Responsibilities

7 Privacy Function in the Business Context

8 Internal and External Resources

9 Thoughts About the Profession

10 Cross Border Data Transfer

Research Objectives

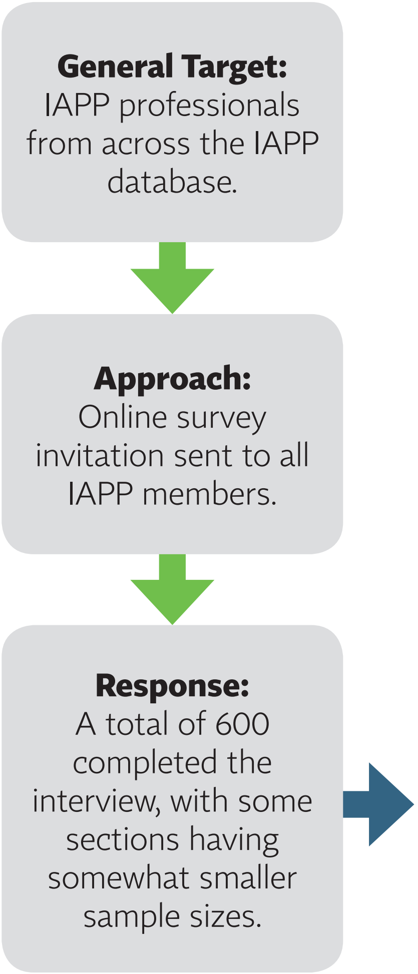
The overarching goals of this research are to provide a profile of how privacy departments and programs are structured within organizations of various sizes and sectors—and to track how those departments evolve over time.

Privacy program detail, including how long the program has been in place, how often it's updated, the different parts of the organization it touches, the number of employees involved in implementing or monitoring the program, etc.

Privacy program spending—current spending, how spending has changed over time, and how spending is expected to change in the future.

Privacy Professional influence, exploring what aspects of the company's business the professional has input into, the nature of that input (recommendations or requirements), and the aspects the professional feels he or she should have input into but doesn't.

Method



General Target: IAPP professionals from across the IAPP database.

Approach: Online survey invitation sent to all IAPP members.

Response: A total of 600 completed the interview, with some sections having somewhat smaller sample sizes.

The survey asked for a variety of detailed information on privacy budgets, employees, salaries, and department structures.

NOTE: The bulk of this report focuses on responses from in-house privacy professionals (from section 5 on).

WEIGHTING: The 2016 results were statistically weighted to match the employee size distribution of firms answering the 2015 survey. This distribution matching allows us to make "apples to apples" comparisons between findings from both years.

Percentages may not add up to 100 percent due to rounding.

Contents

1 Background and Method

2 Executive Summary

3 **How the Job of Privacy Is Done**

4 Background on Companies and Individuals

5 Privacy Group Characteristics: Structure

6 Privacy Group Characteristics: Responsibilities

7 Privacy Function in the Business Context

8 Internal and External Resources

9 Thoughts About the Profession

10 Cross Border Data Transfer

How the Job of Privacy Is Done

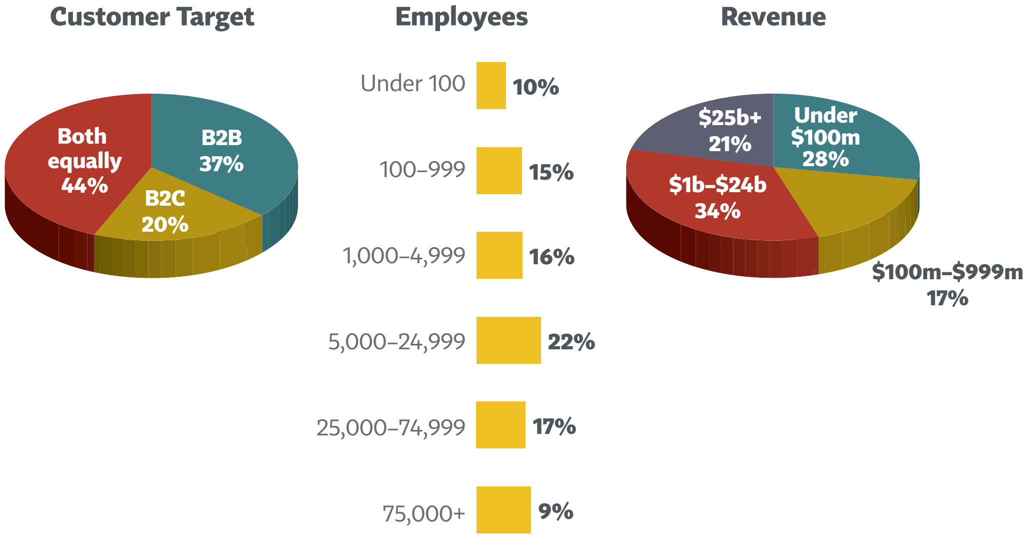
Profile of Survey Respondents

The English-language survey was sent to subscribers of the IAPP's Daily Dashboard, most of whom are IAPP members. A majority of the respondents — 63 percent — work for organizations headquartered in the United States. Around one in five (19 percent) work for EU-headquartered organizations, and just over 10 percent are from Canadian firms.

Fewer respondents work in industries in which privacy is explicitly regulated in the United States such as health care, pharmaceuticals, financial services and insurance (32 percent) than in what are typically considered unregulated industries (52 percent). Looking more closely, 20 percent of the respondents are in financial services, while another 20 percent work for technology or telecommunications firms, and 17 percent are in professional services. Respondents from the health care and pharma sectors make up 12 percent of the survey results, while 11 percent work in the government sector.

In terms of business models, revenues, and employee size, the 2016 survey reflects a balanced representation of the market. Nearly half of respondents (44 percent) work in industries that have a mix of business-to-business (B2B) and business-to-consumer (B2C) models, with the other half weighted toward B2B (37 percent) over B2C (20 percent). Respondent companies are evenly distributed by annual revenues as well; the category with the most responses is firms earning between U.S. $1 billion and $24 billion at 34 percent. Finally, representing company size by number of employees, responses also came from companies across the spectrum — 22 percent of respondents work for organizations employing 5,000-24,999 people, while 36 percent work for larger organizations (over 25,000) and 41 percent work for smaller ones (under 5,000).

Company Profiles



Customer Target

Employees

Revenue

Privacy Throughout the Organization

Privacy professionals regularly benefit when their colleagues throughout the organization — from product development, information security, and IT teams, to the board of directors — have an understanding of and interest in privacy. Now, privacy training and teaching efforts appear to be paying off. As this year's survey reveals, privacy has infiltrated new corners of the organization with more disciplines gaining at least some privacy duties. What is more, privacy is integrated earlier and more consistently than ever before with product development and other company initiatives — respondents report they are 7 percent more likely than in 2015 to be involved throughout an activity and more report "much greater" involvement and influence than last year.

The private sector remains the largest employer by far of privacy professionals, with 69 percent of respondents reporting they work as in-house privacy or IT professionals for private businesses. Only 11 percent work for firms providing external privacy support services, and 10 percent work in-house for the government.

Not surprisingly, most privacy professionals find themselves working closely with or in legal or compliance departments. But increasingly they are also either reporting to or working closely with IT and information security. This may explain why fewer privacy professionals than in prior years report devoting themselves full time to privacy. More people within the organization, who do not necessarily identify as "privacy professionals," are taking on privacy duties as part of their job responsibilities. Indeed, this year saw a meaningful growth in the number of respondents who work in information security, and these professionals are far less likely than other respondents to devote 100 percent of their time to privacy. Privacy responsibilities, in other words, are spreading beyond the privacy team throughout the organization. It follows that privacy knowledge, skills

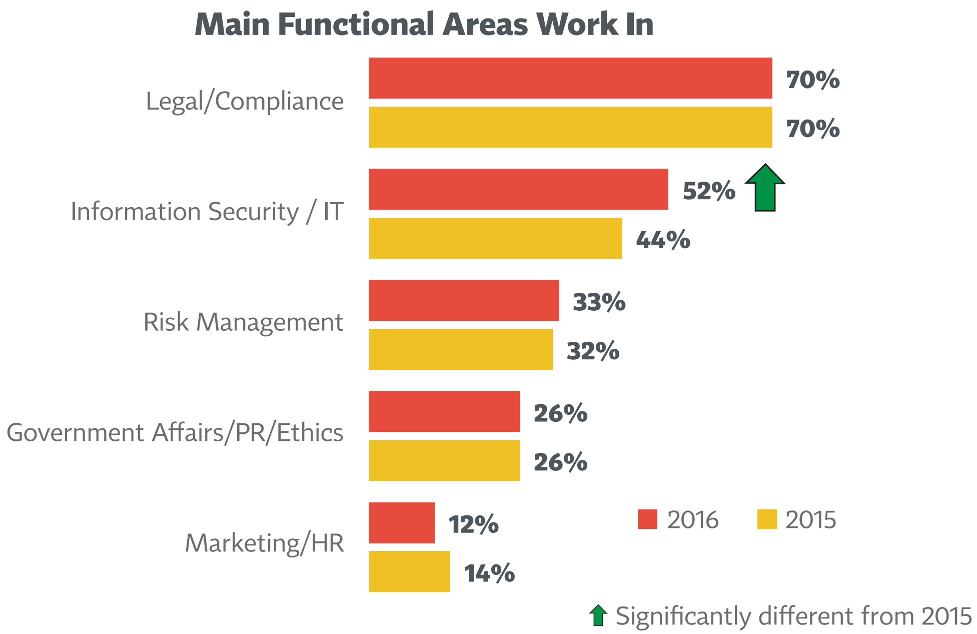
The Rise of the DPO

A key area to watch is the data protection officer (DPO) position, which will become obligatory for many firms under the GDPR. Among survey respondents who believe they fall within the GDPR's scope, 35 percent report their companies will be appointing a DPO and 16 percent plan to appoint multiple DPOs.

While the Regulation has yet to be applied and fully interpreted, it seems the DPO role will differ in meaningful ways from the more strategic role played by the modern Chief Privacy Officer. Under Article 39 of the GDPR, DPOs and CPOs share some common functions, such as advising employers on compliance with the GDPR and other data protection laws, monitoring compliance, training staff, conducting internal audits, and advising on PIAs.

But DPOs by law also will serve as internal regulators and be responsive directly to data subjects. The GDPR requires DPOs to work and cooperate with the relevant supervisory authority, and be available for inquiries from data subjects "relating to data protection practices, withdrawal of consent, the right to be forgotten, and related rights." These functions could be construed as ombudsman-style roles, and the job description envisioned in the GDPR could potentially place the DPO at odds with the controller or processor, in contrast with the close relationship between CPOs and their employer.

As companies grapple with filling the DPO role internally or externally, it will be interesting to see where the DPO stands on the corporate ladder and in what departments they will sit.

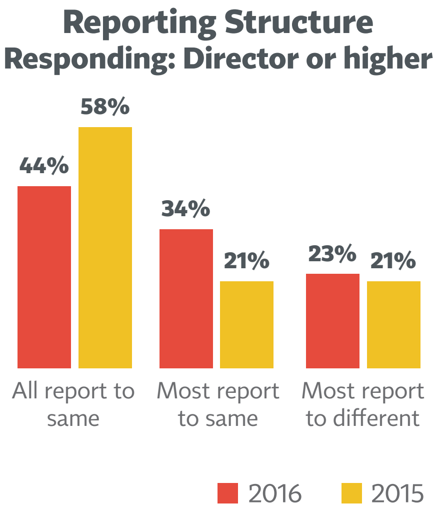


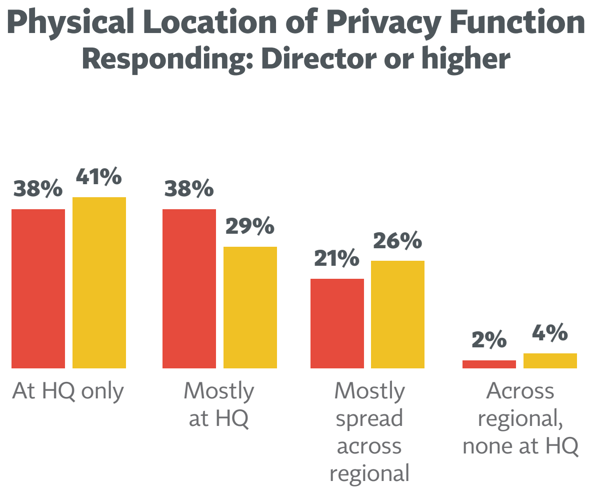
and abilities are being written into the job descriptions of a host of job titles, including IT, information security, human resources, and the like.

Privacy's spread throughout the organization certainly plays out in the government sector, where privacy responsibilities are being doled out to a variety of positions within government agencies, resulting in a preponderance of respondents with a title below manager (40 percent). The tech industry, where some of the largest privacy teams exist, is also more likely than others to assign privacy responsibilities to employees with titles lower than manager (32 percent). In regulated industries like finance, however, privacy professionals hold some of the highest positions in the firm with 30 percent serving in the C-suite.

What credentials do privacy pros hold? According to the survey, and unsurprisingly, among the credentials held by privacy professionals, IAPP's certifications dominate, with 39 percent of overall respondents holding the CIPP/US credential, and 16 percent earning the CIPM. The next most common credential was the CIPP/E designation, held by 15 percent of respondents overall.

Another interesting trend is the growing role of the privacy professional in "corporate ethics" departments. Although data ethics do not have the dominance of legal/compliance roles across all market segments and throughout a privacy program's lifecycle, corporate ethics seems to be a growing vocation for privacy professionals. Twenty-nine percent of respondents in privacy programs at the "mature" stage of their development report involvement in corporate ethics roles, while just 15 percent of early-stage programs engage with corporate ethics.





Today’s Typical Privacy Professional:

- Holds at least one IAPP certification (54 percent hold the CIPP designation).
- Works in-house and in the private sector (61 percent).
- Holds a title of at least director (46 percent).
- Works in the legal or compliance department (70 percent), but may also work with information security or IT (52 percent).
- Has responsibilities beyond privacy (70 percent).

The U.S. Privacy Professional:

- Holds an IAPP certification (more than 70 percent).
- Is more likely to reach the C-suite (19 percent) than counterparts in the EU (10 percent) or Canada (14 percent).

The EU Privacy Professional:

- Is the most likely to focus exclusively on privacy.

Aiming for the C-Suite? Your Chances Are Greatest if Your Employer:

- Is in finance (30 percent).
- Has fewer than 5,000 employees (20 percent).
- Has a mature privacy program (41 percent).

Privacy Teams and Budgets

A note about the survey methodology: We asked respondents to identify their title within the organization. Respondents who did not self-identify as director-level or higher (which we define as between "manager" and VP) were not presented with the question sets relating to budgets and staffing. This was based on the assumption that privacy professionals in senior management positions have more accurate data about budgets and staffing than those in junior roles. The narrowing of budgets and staffing questions to only a subset of respondents produced more consistent and reliable data, but also created sample-size issues. In particular, the sample of responses from EU-based firms was smaller than is acceptable for breaking out by region. This reflects the IAPP's still-maturing membership base in the EU, as well as the EU's still-maturing privacy industry, itself.

There is no such thing as a "typical" privacy team. Privacy programs are scalable, with large companies reporting numerous employees having full-time or part-time privacy duties, while smaller organizations employ just a few. Because the average age of a privacy program is just over six years, it is not surprising that headcount for privacy teams — and even privacy roles outside the core teams — is still in the single digits for many organizations.

Eliminating the very few outliers reporting 1,000 or more employees with privacy responsibilities, the mean number of employees on a privacy team is six full-time and four part-time staff. Regulated industries have slightly larger privacy groups on average than unregulated ones, and large companies skew the averages much higher with robust privacy teams. The most telling indicator of privacy team size is an organization's annual revenue — the two directly correlate. Companies with more than $25 billion in revenue protect it with an average of 15 full-time privacy staff while those under $100 million generally have just one full-time pro.

Employees Dedicated to Privacy

	Mean	Median
Full time privacy, in privacy program	6	3
Part time privacy, in privacy program	4	1
Full time privacy, in other units	4	0
Part time privacy, in other units	17	3

But due to a strong and growing penetration of privacy knowledge and skills outside of the core team, the role of part-time privacy professionals cannot be ignored. On average, respondents reported 17 professionals outside the privacy unit dedicating themselves at least partly to privacy. This means that employees who fill primarily human resources or IT functions, for example, are also becoming responsible for privacy at least part-time. Also noticeable is the role many professionals are playing on privacy working groups. Nearly half of survey respondents report

Mean Privacy Employee Size

BY COMPANY REVENUE

	Under $100 million	$100–$999 million	$1–$24 billion	$25 billion or more
Full time privacy, in privacy program	1	6	5	15
Part time privacy, in privacy program	3	4	2	8
Full time privacy, in other units	1	4	3	13
Part time privacy, in other units	4	6	13	59

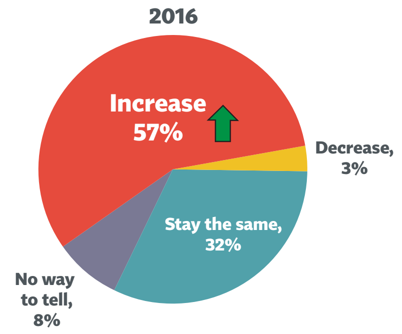
Expected Employee Change in Coming Year
Responding: Director or Higher

	% Saying Increase	% Saying Decrease	% Saying Stay the Same	Net % Change
Full time privacy, in privacy program	37%	2%	61%	+11%
Part time privacy, in privacy program	25%	1%	75%	+7%
Full time privacy, in other units	24%	0%	76%	+8%
Part time privacy, in other units	39%	2%	60%	+11%

having a privacy working group, membership of which is highly diverse. The role of IT professionals on such groups grew 9 percent over the last year while human resources professionals are 12 percent more likely than in 2015 to be part of a privacy working group.

Employment trends indicate significant growth over the coming year in two areas — the number of positions for full-time privacy professionals on privacy teams is expected to grow by 37 percent while an additional 39 percent growth is expected for part-time privacy responsibilities in units other than privacy. This is consistent with adjustments companies will need to make to comply with the GDPR, as well as with the growing awareness that privacy issues are important to many different job functions within the organization, including marketing, HR, data security and IT.

Compared to 2015, moreover, respondents are far more bullish on privacy budget increases, with 57 percent expecting budget to grow in the coming year compared to just 34 percent last year. Clearly, the extra money is needed, but there's some question as to whether it will be enough: Sixty-nine percent report that their budget is insufficient, compared



Vendor Management Is Top of Mind

In 2015, telecommunications giant AT&T agreed to settle for $25 million a U.S. Federal Communications Commission investigation into three data breaches caused by its vendors in Mexico, Colombia and the Philippines. This followed the 2013 Target breach, in which hackers stole network credentials from the retailer's HVAC subcontractor and exposed as many as 70 million customers to credit card fraud. After these cases — and many others — came to light, information security professionals could no longer ignore the need for a rigorous process of vendor selection, security monitoring, liability controls, and ongoing audits.

But are privacy professionals being consulted on vendor oversight? The answer that emerges from the survey is a strong "yes."

Regulations like HIPAA (which explicitly defines subcontractors as "business associates"), the GDPR (which imposes liability on controllers for the actions of processors and subprocessors), and Privacy Shield (which requires organizations to tighten controls over data transfers and onward transfers), put vendor management front and center for privacy teams. The U.S. Federal Trade Commission has for over a decade required companies to protect consumers' data through careful selection and oversight of third parties handling data.[1]

In short, it has become an industry best

[1] The IAPP collects and provides access to the FTC's privacy and security enforcement actions, including those involving third-party vendors, in the FTC Casebook, available at https://iapp.org/resources/ftc-casebook/.

continued on xv

to 62 percent last year. Predictably, most of the budget goes to salaries (55 percent); but there's a growing call for more technology and other resources. Further, nearly half (47 percent) of respondents would like more funding for privacy training.

Last year's report left room for ambiguity with respect to whether salaries of privacy professionals should be reported as part of the "privacy budget," even if they appear on another account, such as HR. This year, the question sets were clearer, resulting in a more detailed picture of the average privacy spend. Respondents reported total privacy spending that averages a total of $1.7 million annually. That's divided into salary of the privacy team (35 percent), external spend by the privacy team (27 percent), and the remainder as salary and spend by the rest of the organization (38 percent). To use a thumbnail metric, organizations generally spend annually about $350 per employee on privacy.

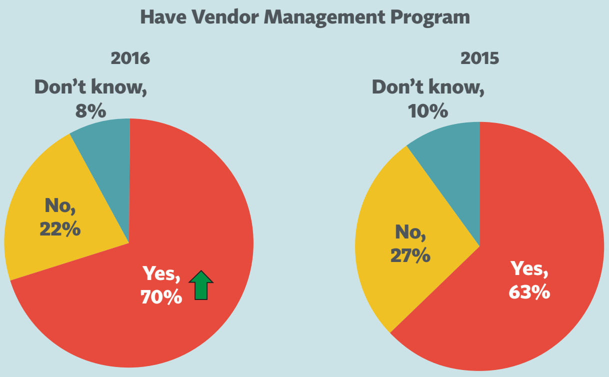
It is not surprising that larger companies tend to have bigger privacy budgets. Larger companies have also invested greater amounts outside the core privacy team, in contrast to smaller companies, which dedicated a greater proportion of their budgets to the privacy team itself. Indeed, the survey shows that a handful of high-revenue firms spent profusely outside the privacy team, pulling the average external spend for companies between 25,000 and 74,999 employees up to more than $6 million. This could be due to a heavy investment in compliance, litigation, settlement or related events. Most organizations devote a bulk of their external budgets to hiring attorneys, but some of these expenses reflect investments in privacy-related technological tools and infrastructure.

As mentioned above, privacy professionals are having success spreading the privacy message and privacy duties more widely throughout the organization. Organizations are

continued from xv

practice to share personal data only with trusted and reliable third parties. Indeed, 70 percent of respondents — up from 63 percent in 2015 — now have a formal vendor management program in place.

The goal is to find and select only those vendors that treat personal data with appropriate privacy and security safeguards. This involves vetting service providers prior to their selection, checking the results of third-party audits, and verifying that vendors have earned certain certifications and credentials. It also involves introducing privacy and security obligations into contracts, requiring that vendors have adequate cyber and other liability insurance, and shifting the risk and costs of a data breach to the vendor when a breach occurs through the vendor's systems and controls.



⬆ Significantly different from 2015

Ongoing monitoring and oversight is also important. Failure to apply continuous oversight will try the patience of regulators like the FTC following a breach.

Establishing a vendor program is the first step, but making it comprehensive and effective is an ongoing battle that privacy professionals are increasingly winning. Although six in 10 report their vendor management programs are only "somewhat" thorough, 31 percent say their programs are "very" thorough — up from just 20 percent in 2015.

continued on xvii

recruiting or training privacy professionals to sit in different teams throughout the firm. This year, only 44 percent say privacy employees all report to the same function compared with 58 percent in the 2015 survey. Some of this growth is in the information security unit, which saw a 6 percent growth in privacy functions compared to last year. This data is directional but worth noting as organizations perceive PII loss as one of the highest cybersecurity risks and look to train the information security team on privacy.[1]

Privacy Leadership

A significant majority of director-level respondents (63 percent) reported leading their privacy teams. Two out of three respondents have "counsel" in their title — more than any other term — with "compliance" running a close second and "chief" winning the bronze.

Privacy and security may still get confused at the layman's level, but on the corporate ladder the roles and responsibilities are becoming more defined. Thirty-two percent of the time, the CPO is an equivalent-level position to the CISO, with 14 percent of respondents saying they are actually the same person. Thirty-five percent of respondents report that the CPO is a junior position to the CISO, while in 12 percent of the cases the CPO is on a higher rung.

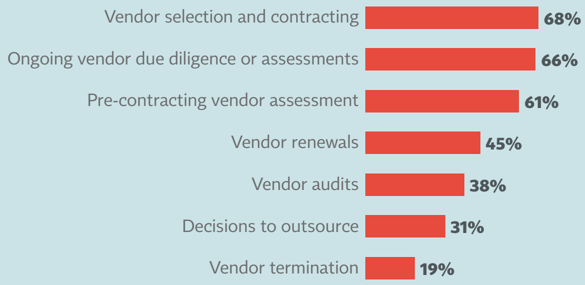
If a company has a Chief Privacy Counsel, the CPO often fills that role herself (32 percent), or at least is on the same leadership level with the Chief Privacy Counsel (16 percent of the time). The CPO is just as likely to be senior to the Chief Privacy Counsel (11 percent), moreover, as he or she is to serve in a junior role (10 percent).

[1] How IT and InfoSec Value Privacy, https://iapp.org/resources/article/how-it-and-infosec-value-privacy/ .

continued from xvi

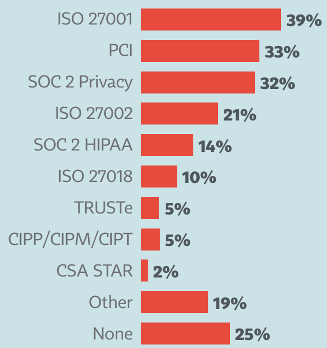
Privacy professionals are involved in vendor management functions from the start — 61 percent say they are consulted at the pre-contracting vendor assessment phase, and 68 percent assist with vendor selection and contracting. Even after a deal is done, the privacy team is consulted 66 percent of the time on ongoing due diligence and continuous assessments.

Privacy Involvement in Vendor Management



One area for improvement is the vendor contract renewal stage — fewer than half of respondents (45 percent) weigh in on vendor renewal decisions, and one in three privacy professionals simply does not know if vendors handling PII have self-renewing contracts.

Required from Vendors



The biggest concern is still data security. The top two audit or credentialing standards required of vendors are ISO 27001 (39 percent) and PCI (33 percent), while ISO 27002 is requested by one of five respondents. The SOC 2 privacy credential is expected 32 percent of the time. But one out of four privacy professionals eschews credentialing altogether, presumably preferring to verify for themselves that vendors are treating their organization's personal data with care.

Privacy leads are more often than not just one or two rungs removed on the corporate ladder from the CEO, although there is room for advancement, with 46 percent reporting they are three or more rungs away from the top. The privacy lead most commonly reports to the General Counsel (29 percent) followed by the Chief Information Officer (23 percent). Still, about one out of six privacy pros reports directly to the CEO.

The privacy lead works exclusively on privacy only about one-third of the time (36 percent) and the average number of years organizations have had a privacy leader is now 6.5, showing once again that the profession is still young and growing.

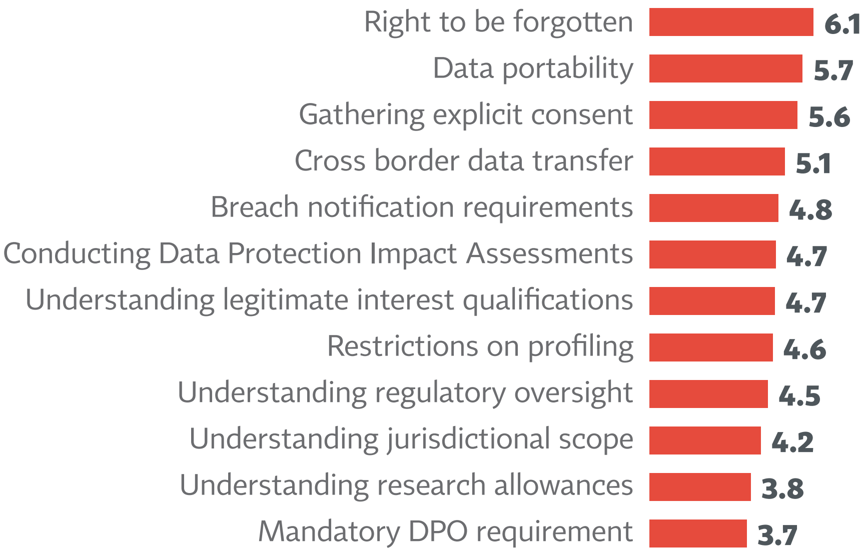
Privacy's Near Future

The GDPR is clearly fueling privacy budget and staff increases — 80 percent of companies who engage in cross-border data transfer say they are subject to the GDPR, and the majority of the rest are not quite sure. The GDPR applies to the transfer of EU data subjects' personal data to controllers or processors outside the EU, including to the onward transfer of that data, and thus affects many organizations not headquartered in the EU.

The GDPR's most vexing requirement, overall, is the right to be forgotten. To be sure, Google has already grappled very publicly with the right to be forgotten, including in litigation at Europe's highest court; but the survey makes clear that the new right is quickly becoming a formidable challenge to multiple industry sectors, far beyond the realm of online search. According to the survey, financial services and manufacturing firms rank the right to be forgotten first among the GDPR's new compliance obligations, with a 7.5 difficulty on a scale of 10. The second-most difficult GDPR compliance challenge is data portability, also initially perceived to be focused on specific industries or even companies but apparently now impacting much broader swaths of the economy, followed closely by explicit consent. Respondents from the hospitality industry rate "gathering explicit consent" a difficulty of 8.3 out of 10. Organizations with smaller privacy budgets and revenues tend to worry most about understanding the GDPR's regulatory oversight requirements.

EU privacy professionals appear concerned their current efforts will not be enough to comply with the GDPR. In a small sample, EU respondents anticipate 30 percent growth in privacy team employment, and 78 percent growth in budget, while a full 90 percent are concerned their budgets are insufficient for necessary privacy compliance.

GDPR Obligation Difficulty
(Mean Score On 0–10 Scale: 0 = Not At All Difficult; 10 = Extremely Difficult)



The U.S. government is also planning to go on a hiring spree, reporting a similar 30 percent growth in privacy staff, with 75 percent of government respondents expressing concern that their budgets will not stretch far enough. Privacy professionals looking for new jobs might also consider organizations at the early stage of developing privacy teams; they project a 21 percent growth in privacy head count, although they remain uncertain whether resources are adequate, with 89 percent reporting budget deficiencies.

While more than half of all companies plan on budget increases in the coming years, the largest firms are the most likely to spend more on privacy and the least likely to project budget inadequacy. Mature privacy teams, moreover, will experience the largest budget growth, and the fewest new hires, suggesting much of their spending growth in the coming years will be on privacy tools and technologies. This, in turn, may be a good sign for the budding industry of privacy tech.

Privacy Motivations

Predictably — and consistent with last year — survey respondents report that their organizations value privacy mostly for regulatory compliance purposes as well as to avoid the risk of data breach. Indeed, respondent organizations are nearly evenly split between compliance and risk-based approaches. Very large corporations are an exception, leaning strongly to the "compliance" direction. Enhancing brand and public trust is a close third-place finisher behind compliance and risk bases for privacy programs.

The value of brand and trust grows as privacy programs mature, however, once the higher-priority compliance and risk functions are securely established. Among programs ranking themselves as "mature" — on average 10.2 years old — 76 percent listed "enhancing brand and trust" as a

Wariness and Uncertainty Swirl Around Transatlantic Data Flows

Recent studies estimate that transatlantic data flows are associated with roughly $250 billion worth of U.S.-EU trade — a quarter of the annual trade in goods and service between the regions.[1] Survey respondents — half of whom are involved in cross-border data transfers — raised significant concerns about the future of these data flows given the complexity, difficulty and expense of complying with EU data protection laws.

With Safe Harbor invalidated, many companies fell back on standard contractual clauses as a legal mechanism to authorize data transfers from the EU to the U.S. In fact, more than 80 percent of companies surveyed rely on standard contractual clauses to comply with EU data protection laws, including 89 percent of all EU companies transferring data to the U.S. But Max Schrems' challenge is not over yet, with the Court of Justice of the European Union currently pondering whether to invalidate standard contractual clauses as a legal data transfer mechanism.

A ruling of invalidation would radically upend the marketplace.

What is more, the EU-U.S. Privacy Shield Framework, recently put forward to replace the former Safe Harbor Framework, continues to be viewed with skepticism. Although 50 percent of all companies that transferred personal data between the EU and U.S. say they used Safe Harbor, just 34 percent say they intend to use Privacy Shield in the future. This may in part be

continued on xx

[1] Joshua Meltzer, The Importance of the Internet and Transatlantic Data Flows for U.S. and EU Trade and Investment, The Brookings Institute Global Development & Policy Working Paper 79 (October 2014), available at https://www.brookings.edu/wp-content/uploads/2016/06/internet-transatlantic-data-flows-version-2.pdf.

privacy priority, while 71 percent valued "meeting consumer expectations" as well. Younger (two-year-old) privacy programs focused far more heavily on compliance versus brand.

What They Do

So, what do privacy professionals do as part of their daily job routine? Of course, they safeguard data — primarily customer and employee private information, although six in 10 are also required to look after service provider information, and other confidential business information. This is done through drafting policies and providing documentation, as well as implementing programs and training. Privacy professionals also do a lot of writing, teaching and communicating within and outside of their organizations.

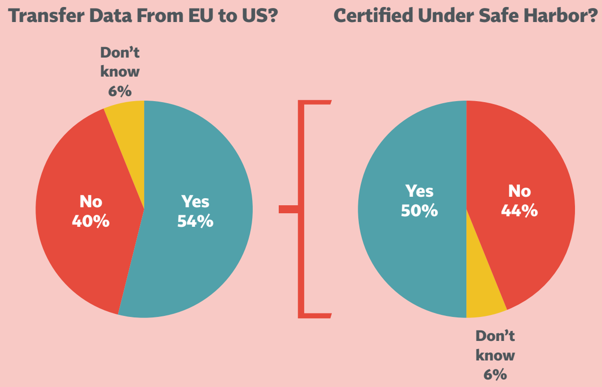
In particular, privacy professionals: work on privacy policies, procedures and governance structures; provide privacy-related awareness and training throughout the organization; respond to privacy and security incidents; manage privacy communications; design and implement privacy controls; manage privacy issues arising with new and existing products; conduct privacy-related employee monitoring and investigations; help with privacy staff development; and participate in privacy-related data committees.

Privacy impact assessments are also among top-tier data protection duties, and growing in their usage — 67 percent report using them this year compared to 59 percent in 2016.

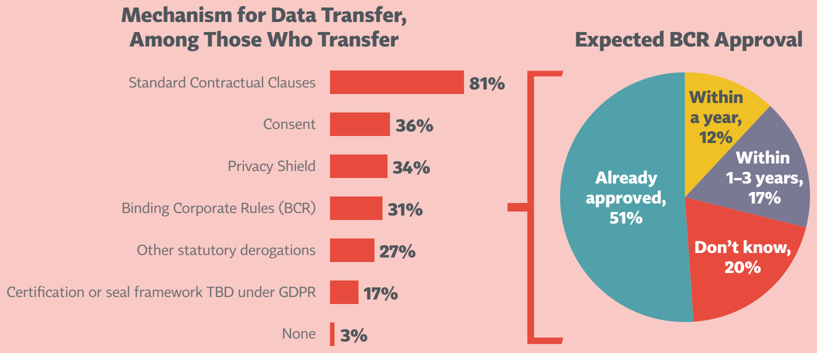
Tasks performed less frequently but still quite often, include: working on privacy by design and vendor management projects; handling privacy audits; managing proper cross-border data transfers; and preparing for the GDPR. Slightly

continued from xix

explained by the fact that the survey was fielded concurrently with the finalization of the Privacy Shield. A decade ago, Safe Harbor as well took several years to gather steam.



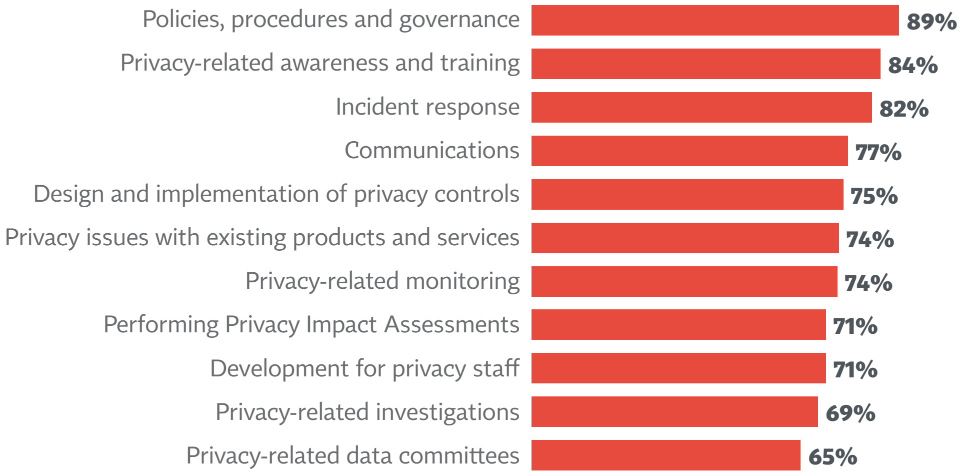
Dialing in deeper, looking at only U.S.-based companies regulated by the Federal Trade Commission, and thus authorized to use Safe Harbor and Privacy Shield, 73 percent used Safe Harbor in the past, but only 42 percent intend to use Privacy Shield in the future. One explanation could be that companies are hesitant to invest in implementing a framework that remains susceptible to legal challenge in European courts. Of all non-government respondents in the survey, 31 percent of EU companies, and 36 percent of U.S. companies said they are eyeing Privacy Shield for the future.



An alternative to standard contractual clauses and Privacy Shield self-certification

continued on xxi

Top Privacy Team Responsibilities
Responding: Director or higher



fewer than half the time privacy professionals interface with privacy-related legal counsel and conduct data inventory and mapping.

Because privacy issues arise with multiple everyday activities within an organization, as well as with new products and services, the survey inquired as to what point privacy teams get involved in organizational initiatives. Compared to last year, respondents report greater involvement in initiatives from the outset (36 percent in 2016 compared to 31 percent in 2015) as well as throughout a project's development (50 percent, up from 43 percent in 2015). New projects are much more likely to involve privacy professionals at the development stage than at any other time — 65 percent of new initiatives involve privacy at the development stage, up from 59 percent last year. More than half of respondents also report that privacy is integrated at least some, if not a great deal, into their organization's planning and development, a directional increase over last year as well.

continued from xx

is the use of binding corporate rules, which companies can get certified by data protection authorities for use in transferring data. Unfortunately, these only seem to be an option for large firms. Just 8 percent of companies with fewer than 5,000 employees see BCRs as a viable solution going forward, versus 53 percent of companies with more than 75,000 employees.

Indeed, some smaller firms seem to be depending on a bit of finger crossing. Even though the EU's General Data Protection Regulation has strict rules about when consent, the fulfillment of a contract, and other derogations can be used to transfer data to the U.S., 36 percent of small firms still intend to rely on these derogations for transfer, anyway, versus just 19 percent of firms with more than 75,000 employees. Put differently, small- and medium-sized enterprises are unable to afford BCRs, may face the invalidation of the less expensive solution of standard contractual clauses, and remain uncertain about using Privacy Shield. This puts considerable pressure on explicit consent, legitimate purpose, and other key derogations in the GDPR.

In contrast to a full 41 percent of companies overseen by the FTC in the United States that report an intention to use consent as a basis for transfer going forward, only 16 percent of their counterparts in the EU do the same. On the one hand, given that three of the four top issues of concern for those complying with the GDPR relate to data transfer, data portability, and data subject consent, the road ahead looks challenging. On the other hand, there will be no shortage of work for privacy pros.

Overall, when asked to compare their integration and influence to a few years ago, respondents say privacy is much more likely to be integrated with, and have a significant influence on, initiative planning and implementation. Among mature privacy programs, as many as 76 percent of respondents report privacy involvement at the development stage, and more than half report involvement throughout the lifecycle of an ongoing initiative.

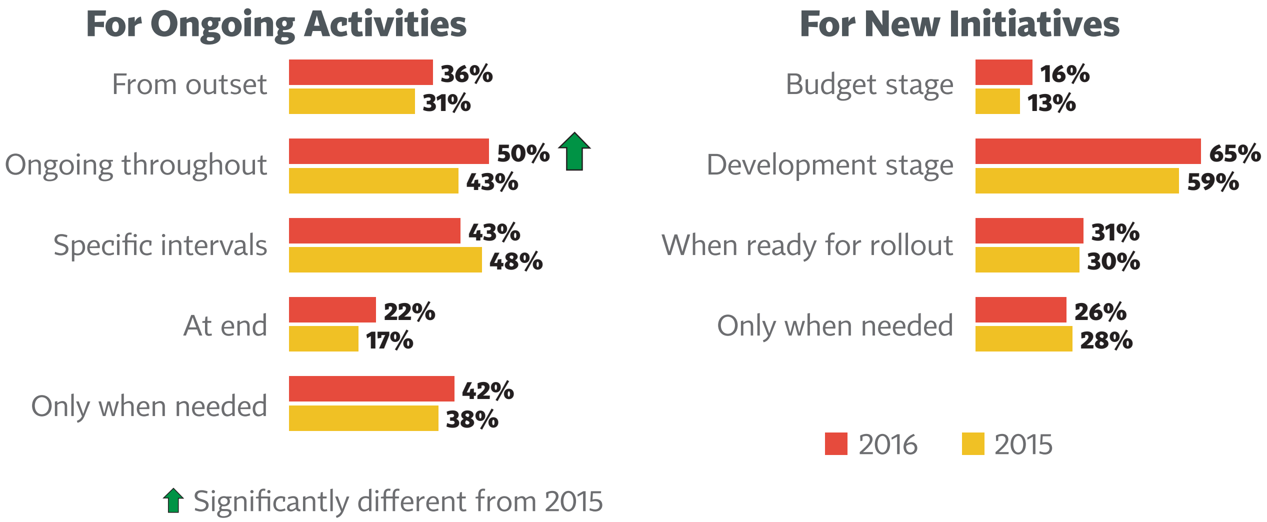
Early-stage privacy programs show different results, however. Only 15 percent report involvement from the outset in ongoing initiatives, and for project planning and implementation only 9 percent feel they had a strong influence. No one in an early-stage program — 0 percent — reported strong integration.

Still, young privacy programs are more likely than not to be involved at the development stage of new initiatives. And U.S. respondents may have more robust “privacy by design” programs than their EU counterparts, as they are 13 percent more likely to get involved with projects from the outset.

Privacy is not only influencing organizations from the bottom up, including those in the trenches building new products and programs, but also from the top down, as it becomes a board-level issue. More than 70 percent of respondents report that privacy issues are brought to the board of directors at least on an ad hoc basis, if not routinely. Organizations with very large privacy budgets are even more likely to earn their board’s attention. Nearly as often as the General Counsel it is the CPO who does the reporting to the board. Because privacy is often seen as a component of data breach risk, of course, it is not surprising that privacy matters are often reported to the board of directors along with data breach concerns.

Nearly one in three, however, says the board addresses privacy issues independent of security.

Privacy Involvement in Initiatives



Tools of the Trade

Privacy attorneys dominate the list of frequently used external services, followed by participation in trade associations, with privacy consultants coming in a distant third, nearly tied with privacy technology solutions.

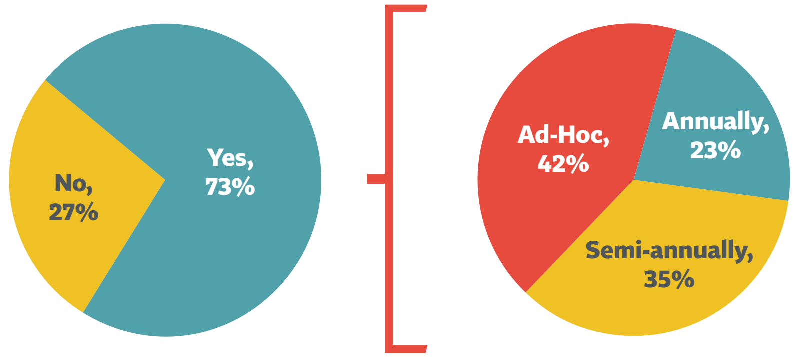
The privacy tech industry, while still nascent, is clearly growing and gaining ground in the competitive battle for external privacy spend.

Some catch-up might be in order first, however, as only 35 percent of privacy professionals report using “governance, risk management, and compliance” (GRC) tools (down from 42 percent last year), and 30 percent simply do not know if their companies use GRC tools or not. If a respondent does use a GRC tool, it is more likely the RSA Archer product than any other currently on the market, and 67 percent plan to expand their use of GRC products next year.

Vendors are facing growing scrutiny from privacy professionals — 70 percent of respondents report having a vendor management program in 2016, up from 63 percent last year. Those vendors looking to invest in the privacy and security standards that privacy teams most commonly seek should consider ISO 27001 (preferred by 39 percent of survey respondents); PCI (33 percent); and SOC 2 Privacy (32 percent). Other preferred credentials include ISO 27002 (21 percent); SOC 2 HIPAA (14 percent) and ISO 27018 (10 percent).

Privacy Matters Reported to Board?
Responding: Director or higher

How Often?
Base: Matters Reported to Board



Conclusion

Regulatory upheaval in Europe and robust privacy initiatives in the U.S. government signal significant growth in privacy hiring and new career advancement opportunities for privacy professionals. The 2016 Privacy Governance Report reveals that IAPP members are bullish about privacy staffing and budgets for the coming year. It also shows that organizations are finding privacy to be a crucial knowledge and skill set for many employees throughout the enterprise, as privacy tasks and responsibilities are spreading beyond the core privacy team.

The GDPR is a high priority for many privacy leaders, in Europe and the U.S., a number of whom are still searching for the best solutions to manage cross-border data transfers in light of the legal challenges in Europe by Max Schrems and others.

The next year or two will see the rise of the DPO, perhaps a greater management role for privacy leaders, and a growing appreciation of data ethics in information-rich organizations. The need for cross-organizational privacy training and awareness has never been greater, as employees from the ground level to the board room are coming to appreciate privacy’s importance. This creates opportunities for privacy leaders to establish large privacy teams and to further integrate privacy into their organization’s planning, new products and services, and strategic vision.

iapp

EY

Building a better
working world

Contents

1 Executive Summary

2 Background and Method

3 How the Job of Privacy Is Done

4 **Background on Companies and Individuals**

5 Privacy Group Characteristics: Structure

6 Privacy Group Characteristics: Responsibilities

7 Privacy Function in the Business Context

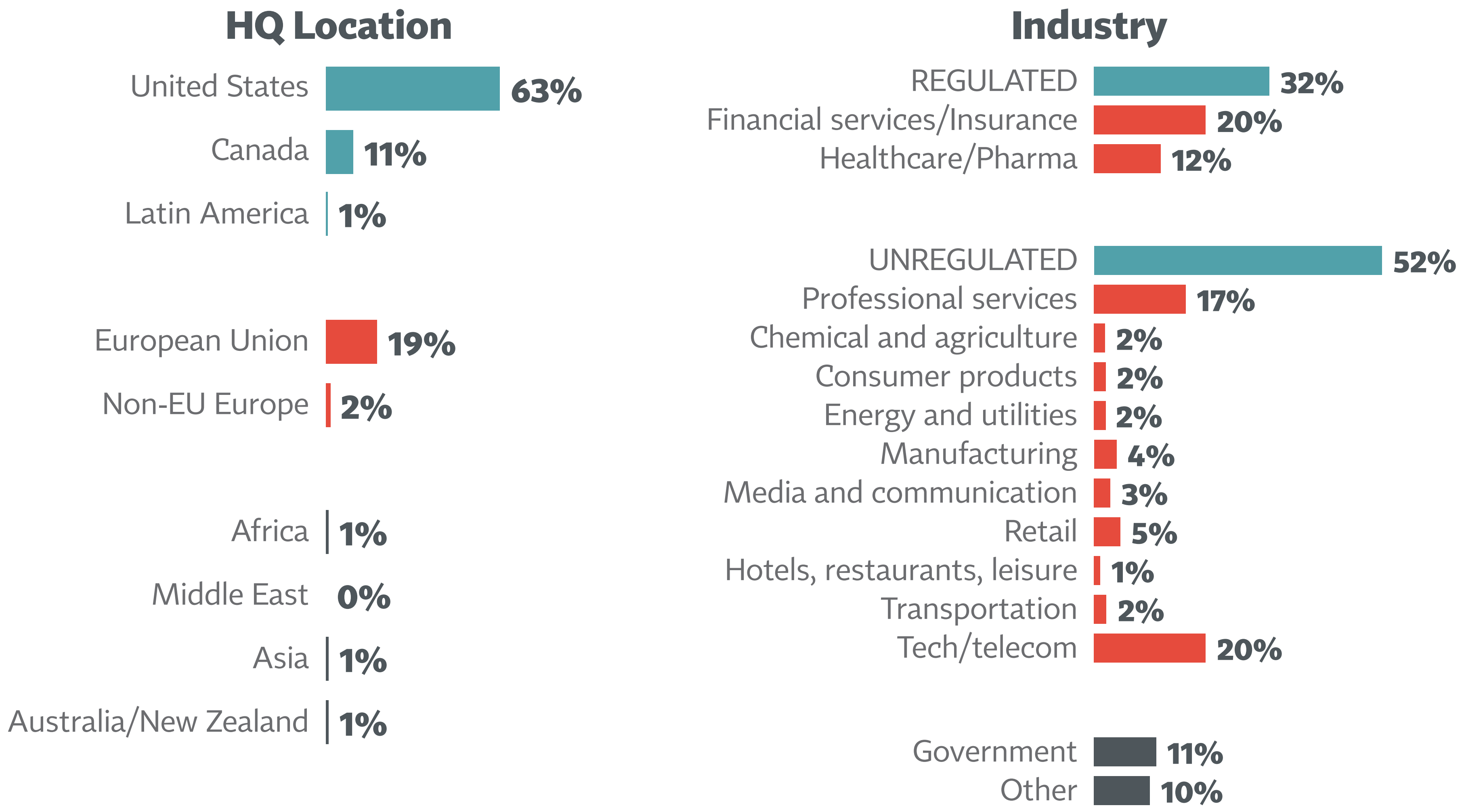
8 Internal and External Resources

9 Thoughts About the Profession

10 Cross Border Data Transfer

The lion's share of study participants are headquartered in the US and are in 'unregulated' industries

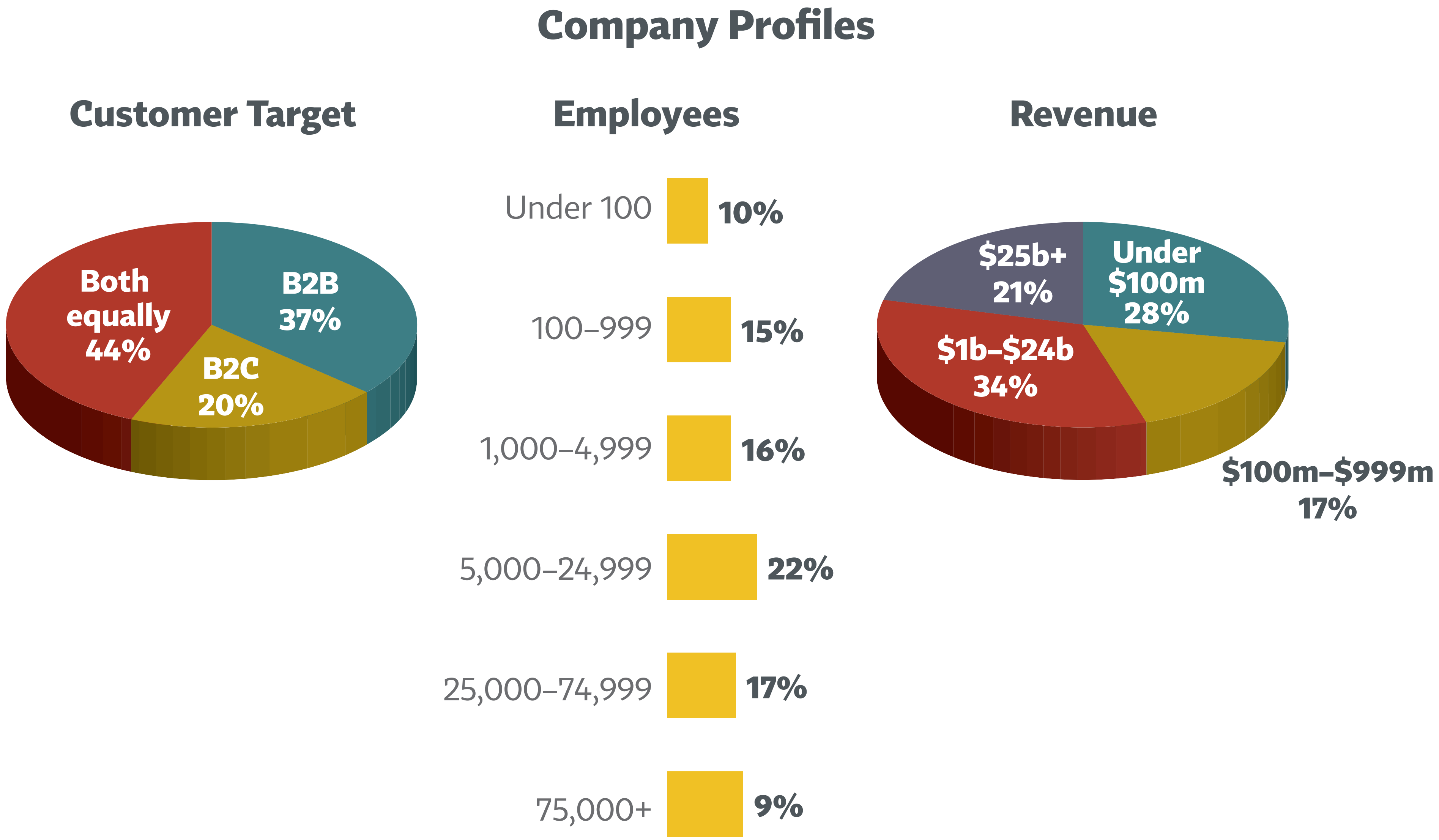
Company Profiles


HQ Location

Industry

A6. What is the primary location of your company's headquarters?
A1. Which sector listed below best describes how your company would be classified?

We interviewed a mix of companies by target, employee size, and revenue


Company Profiles

Customer Target

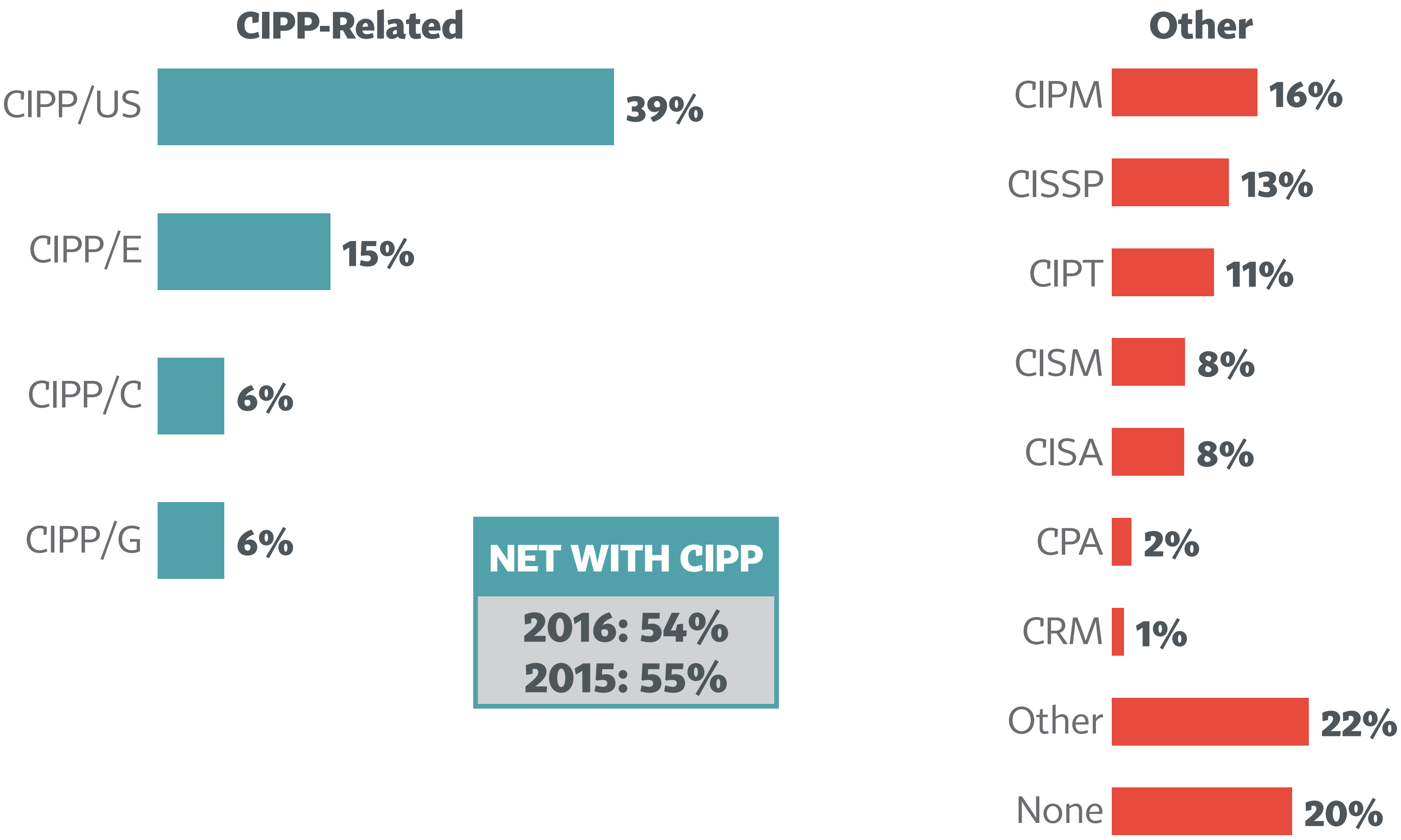
Employees

Revenue

A1a. Does your company primarily serve:
A3. What is the total number of employees in your company (full-time and part-time)?
A2. Please tell us (as accurately as you can) your company’s annual revenue.

A majority of participants have a CIPP certification, statistically the same as in 2015

Credentials Held by Privacy Professionals



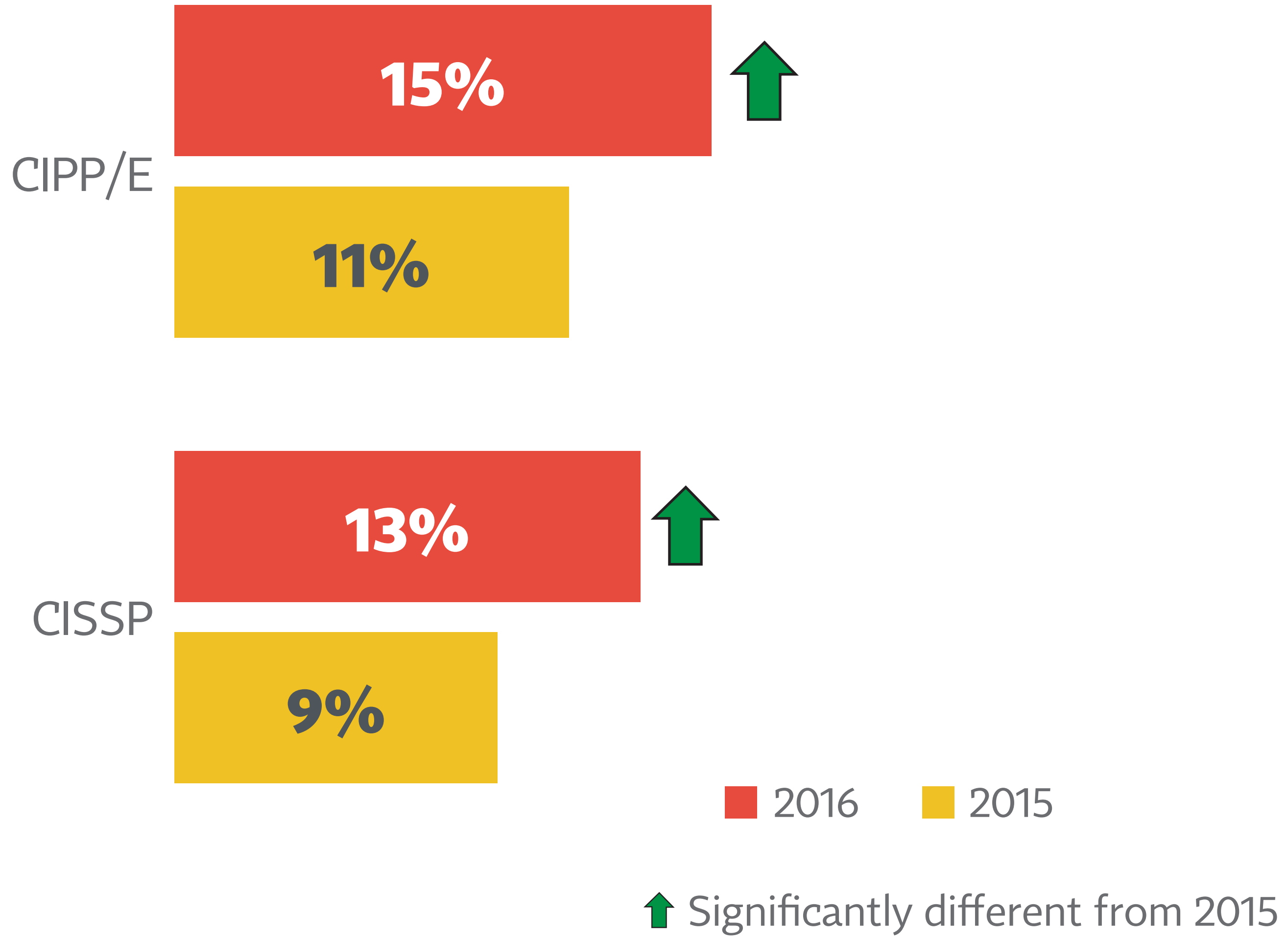
Most common mentions in "other" category: CAP, CGEIT, CHIM, CRISC, HIPAAP, ISEB, PCI

I1: Which certifications do you hold?

Note that the percentage of members with CISSP and CIPP/E has grown significantly since 2015

- Both are up 4 points over the past year

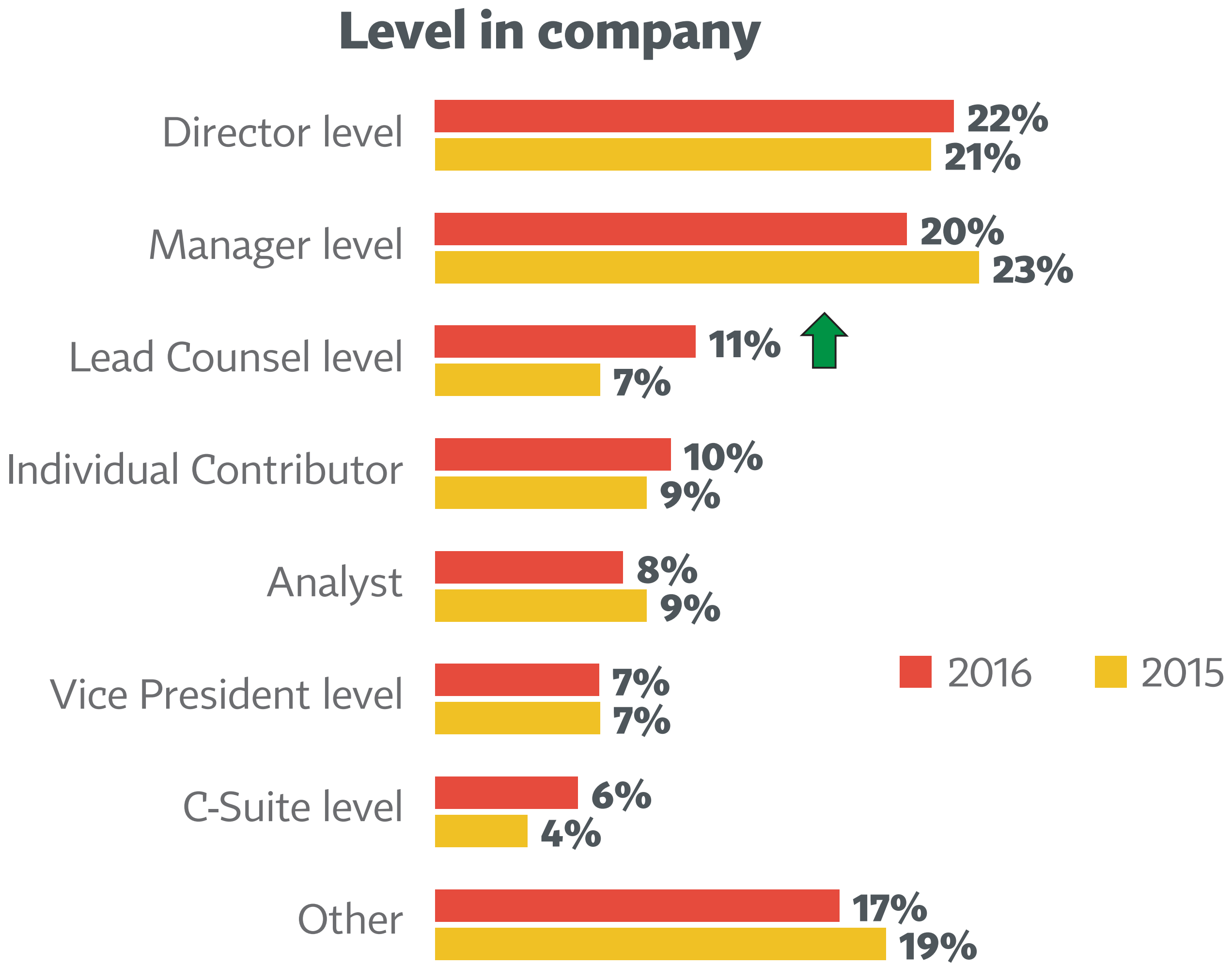
Credentials and Degrees Held by Privacy Professionals



C1: Which certifications do you hold?

As in 2015, privacy professionals are most likely to be directors or managers

- However, this year's wave sees a statistically significant increase in the proportion at the Lead Counsel level, to 11%



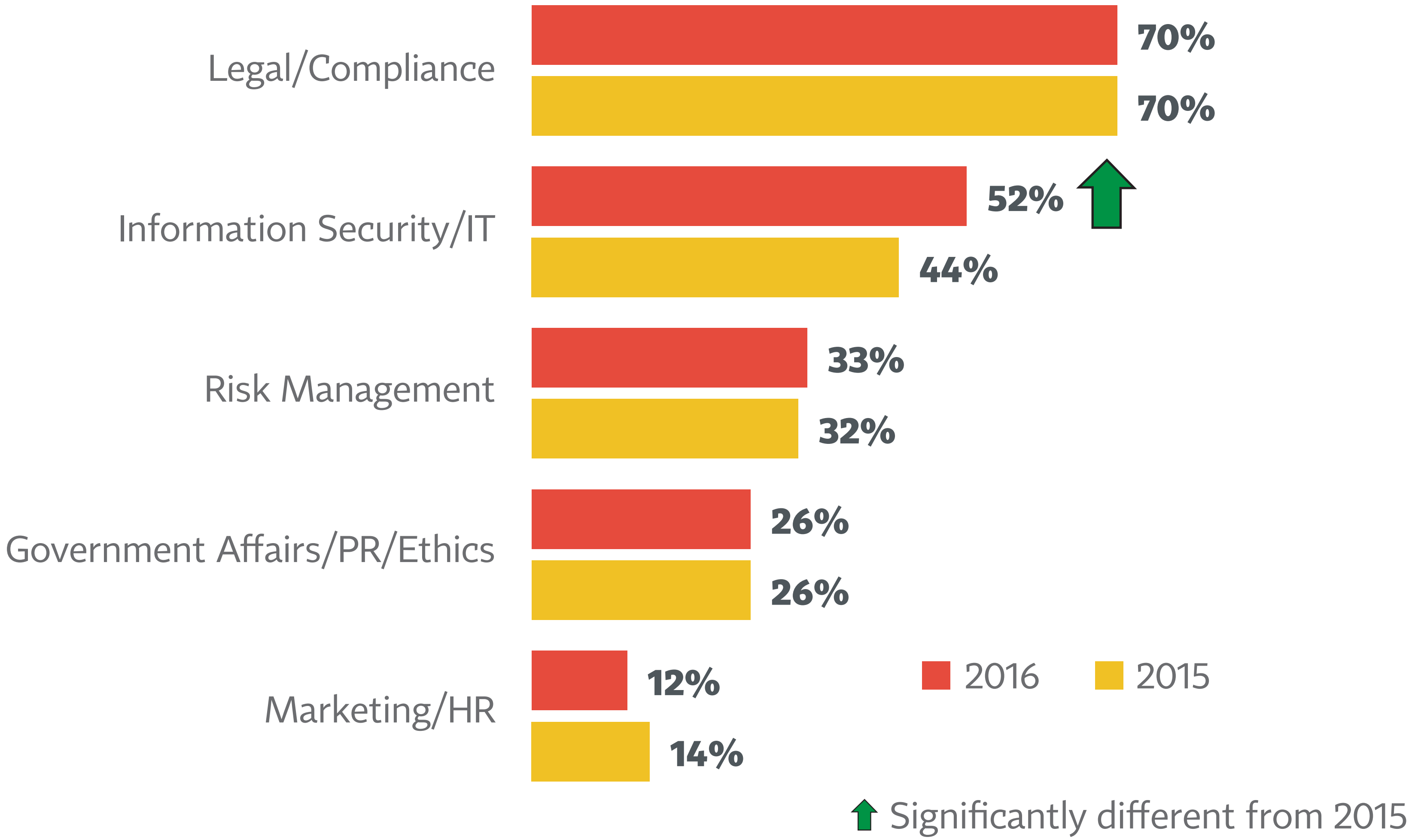
⬆ Significantly different from 2015

C1: Which of the following levels best describes your position in your company?

We saw in 2015 that professionals work across a range of functional areas, and that's still the case

- Legal/compliance is the most commonly mentioned area, although there's also been an increase in those who say they're involved in IT

Main Functional Areas Work In

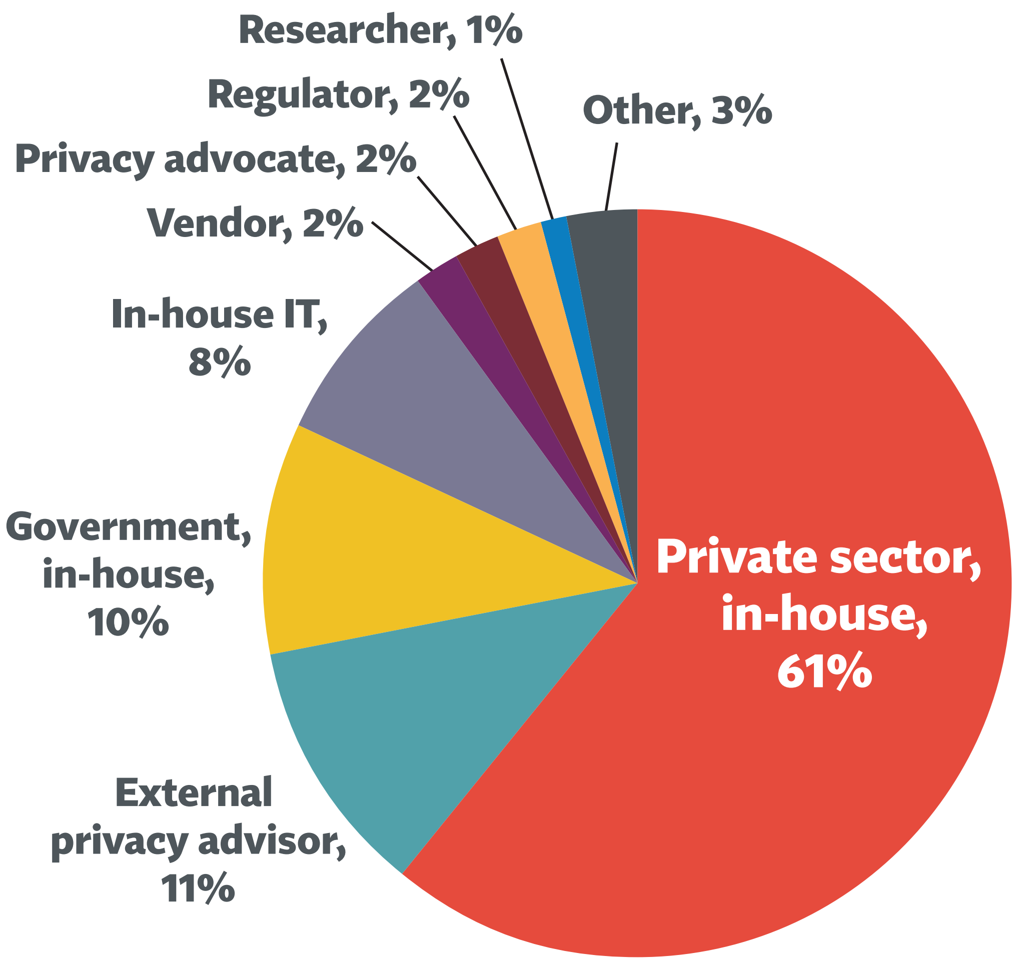


C3: Which of the following functions best describe the areas you regularly work in at your company?

Nearly 8 in 10 privacy professionals work in an in-house capacity, identical to 2015

- And the vast majority of those in-house professionals work in the private sector

Privacy Roles



C4: Next, which of the following best describes the sector of your current position?

US professionals are the most likely to be CIPx certified; they're also more likely than average to be C-level

KEY SEGMENT DIFFERENCES

- On the flip side, those working in government or in tech firms are more likely to have titles lower than manager

Background Characteristics:
Segments with Higher Than Average Results

BY GEOGRAPHY

	US	EU
CIPx certification	71% ▨	43%
C-Suite title	19% ▨	10%
Manager	16%	22%
Work w/ Gov't affairs	9%	4%
Work w/ Records mgmt	15%	13%

BY INDUSTRY

	Gov't	Finance	Health	Tech
C-Suite title	5%	30% ▨	14%	13%
Below Manager	40% ▨	18%	12%	32% ▨
Work w/ Records mgmt	40% ▨	16%	17%	12%
Work w/ Regulatory Compliance	37%	66% ▨	53%	51%

▨ Significantly different than overall mean

Those in large firms are the most likely to be CIPx certified, but also more likely to have lower ranking titles

KEY SEGMENT DIFFERENCES

- As we saw last year, professionals in mature privacy programs are especially likely to have certification and higher-ranking positions

Background Characteristics:
Segments with Higher Than Average Results

BY EMPLOYEE SIZE

	<5K	5–24.9K	25–74.9K	75K+
CIPx certification	51%	66%	68%	▨ 70%
C-Suite, EVP, SVP, VP	▨ 20%	16%	16%	10%
Director	18%	▨ 29%	23%	20%
Below Manager	20%	20%	25%	▨ 35%
Work w/ IT	24%	28%	▨ 39%	32%

BY PRIVACY LIFESTAGE

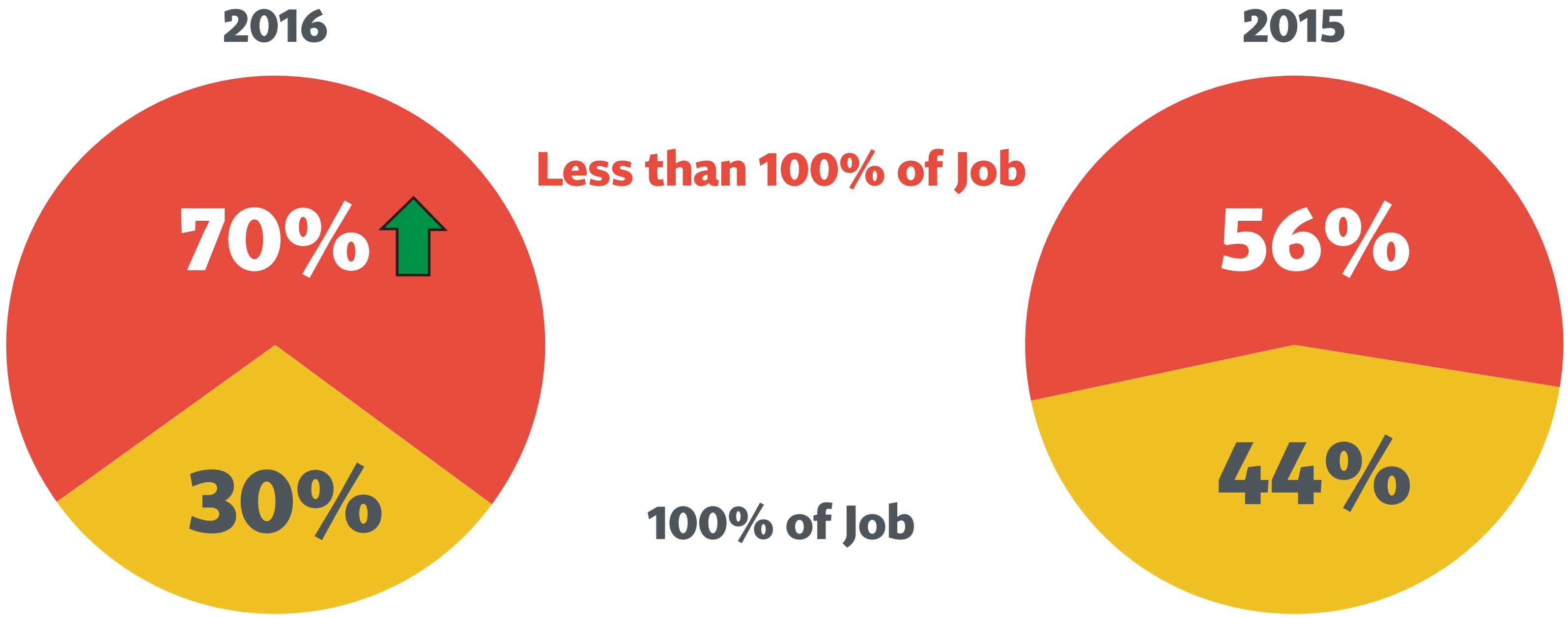
	Early	Middle	Mature
CIPx certification	65%	72%	▨ 78%
Work w/ Corporate Ethics	15%	▨ 28%	▨ 29%
Work w/ Info Security	▨ 67%	44%	38%
Work w/ Regulatory Compliance	40%	▨ 65%	58%
Work w/ Legal Compliance	64%	▨ 82%	77%
Work w/ Marketing/HR	11%	▨ 21%	13%

▨ Significantly different than overall mean

Looking at in-house professionals, we see a drop since 2015 in those saying privacy makes up 100% of their job

- Just 30% say they're dedicated full-time to privacy, vs. 44% a year ago

Privacy Responsibility as % of Job



PRIVACY AS % OF JOB (MEAN)
2016: 64%

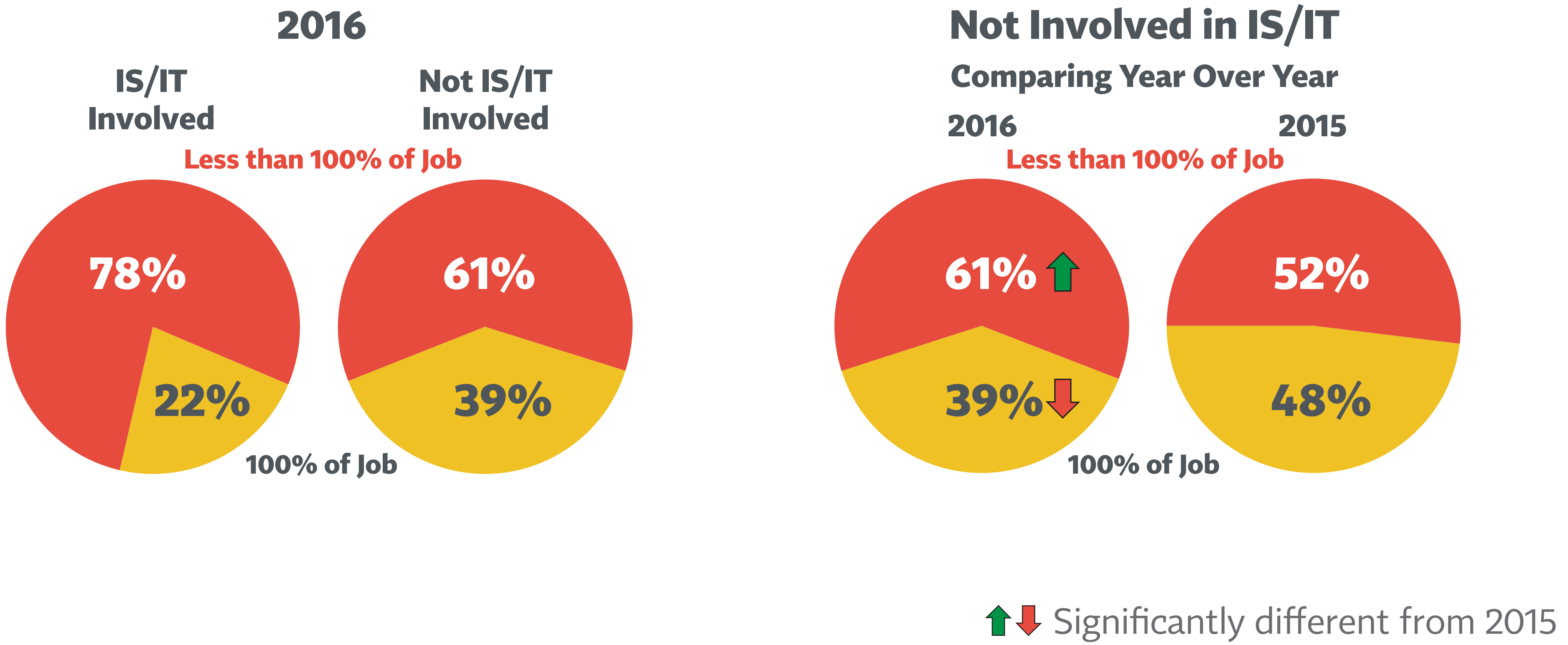
⬆ Significantly different from 2015

Note: Different question structure
2016: D1: About what percentage of your work at your company is made up of privacy responsibilities?
2015: D1: Would you say that privacy responsibilities make up 100 percent of your work at your company or less than 100 percent?

More respondents having IS/IT responsibilities may have contributed to this decline

- We saw an eight-point increase in those saying they are involved in Information Security or Information Technology
- And privacy is a smaller proportion of responsibilities for this group

Privacy Responsibility as % of Job

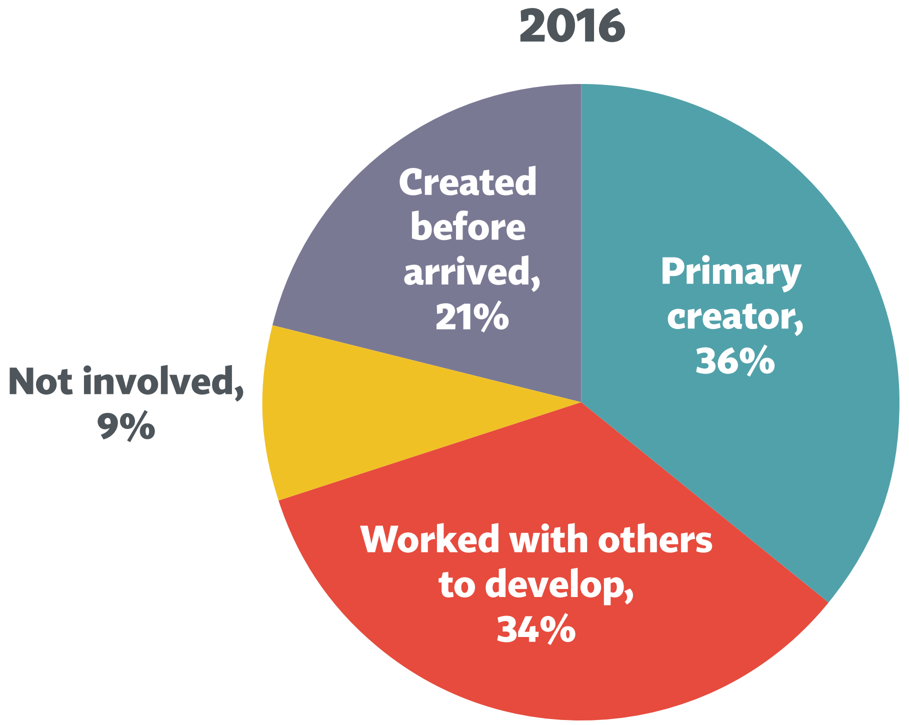


Note: Different question structure
2016: D1: About what percentage of your work at your company is made up of privacy responsibilities?
2015: D1: Would you say that privacy responsibilities make up 100 percent of your work at your company or less than 100 percent?

However, we see almost no change in the % who were the primary creators of their program

- 36% say they themselves took the lead in program creation; another 34% collaborated with others to develop their privacy practice, virtually identical to 2015

Respondent's Role in Developing Program



E3: Which of the following comes closest to describing your role in developing the privacy program of your company?

Government professionals are the most likely to say privacy makes up only part of their job

KEY SEGMENT DIFFERENCES

- Those in health care are at the other end of the spectrum; nearly half say they work in privacy exclusively
- We see no significant differences by regulated vs. unregulated company status; plus, companies that are equally B2B and B2C are directionally more likely to have dedicated privacy pros

In-House Privacy Professionals:
Segments with Higher Than Average Results

BY INDUSTRY/CUSTOMER

	Regulated	Unregulated	Gov't	Finance	Health	Tech	B2B	B2C	Both
Respondent spends full time privacy	34%	30%	17%	28%	46%	31%	24%	29%	34%
Respondent spends less than full time privacy	66%	70%	83%	72%	54%	69%	76%	71%	66%
Worked with others to create	29%	37%	63%	29%	29%	48%	34%	31%	35%

Gov't: Government
Finance: Financial Services and Insurance
Health: Healthcare and Pharmaceutical
Tech: Technology and Telecommunications

▨ Significantly different than overall mean

Dedicated privacy professionals are most likely to be found in larger organizations

KEY SEGMENT DIFFERENCES

- In addition, perhaps not surprisingly, professionals in early-stage privacy programs are the most likely, by far, to say they took the lead in developing the program
- U.S. pros are a bit more likely to spend just part time on privacy, but only directionally

In-House Privacy Professionals:
Segments with Higher Than Average Results

		<5K	5–24.9K	25–74.9K	75K+
BY EMPLOYEE SIZE	Respondent spends full time privacy	16%	34%	42%	39%
	Respondent spends less than full time privacy	84%	66%	58%	61%
	Primary Creator	41%	49%	30%	10%

		Early	Middle	Mature
BY PRIVACY LIFESTAGE	Respondent involved in creating program	86%	67%	65%

		US	EU
BY GEOGRAPHY	Respondent involved in creating program	69%	60%

🟥 Significantly different than overall mean

Contents

1 Executive Summary

2 Background and Method

3 How the Job of Privacy Is Done

4 Background on Companies and Individuals

5 **Privacy Group Characteristics: Structure**

6 Privacy Group Characteristics: Responsibilities

7 Privacy Function in the Business Context

8 Internal and External Resources

9 Thoughts About the Profession

10 Cross Border Data Transfer

Note on budget and team organization questions

"Directors and Higher" refers to respondents who self-identified at a certain level in their organization

A note about the survey methodology: We asked respondents to identify their title within the organization. Respondents who did not self-identify as director-level or higher (which we define as between "manager" and VP) were not presented with the question sets relating to budgets and staffing. This was based on the assumption that privacy professionals in senior management positions have more accurate data about budgets and staffing than those in junior roles. The narrowing of budgets and staffing questions to only a subset of respondents produced more consistent and reliable data, but also created sample-size issues. In particular, the sample of responses from EU-based firms was smaller than is acceptable for breaking out by region. This reflects the IAPP's still-maturing membership base in the EU, as well as the EU's still-maturing privacy industry, itself.

The average privacy team has 10 employees, full-time plus part-time

- An additional 21 employees are involved in privacy, but in other units
- Note that the **mean** results are influenced, mathematically, by those with very large numbers of employees. The **median** results, uninfluenced by large numbers, are somewhat lower

Employees Dedicated to Privacy

	Mean	Median
Full time privacy, in privacy program	6	3
Part time privacy, in privacy program	4	1
Full time privacy, in other units	4	0
Part time privacy, in other units	17	3

Outliers over 999 removed

F1: How many employees are dedicated full-time to your company's privacy program?

Privacy staffs come in many sizes, with large firms often pulling the mean far from the median

KEY SEGMENT DIFFERENCES

Mean Privacy Employee Size

	BY INDUSTRY CATEGORY			BY CUSTOMER TARGET		
	Regulated	Unregulated	Gov't	B2B	B2C	Both
Full time privacy, in privacy program	8	6	3	4	4	8
Part time privacy, in privacy program	5	4	1	4	2	4
Full time privacy, in other units	5	6	1	5	3	5
Part time privacy, in other units	21	23	33	29	8	13

As one would expect, companies with the most employees generally have the largest privacy staffs

Mean Privacy Employee Size

BY EMPLOYEE SIZE

	<5K	5–24.9K	25–74.9K	75K+
Full time privacy, in privacy program	1	3	6	21
Part time privacy, in privacy program	1	1	5	10
Full time privacy, in other units	1	2	6	17
Part time privacy, in other units	3	6	25	56

🟥 Significantly different than overall mean

Privacy staff size is also highly correlated with total company revenue

Mean Privacy Employee Size

BY COMPANY REVENUE

	Under $100 million	$100–$999 million	$1–$24 billion	$25 billion or more
Full time privacy, in privacy program	1	6	5	15
Part time privacy, in privacy program	3	4	2	8
Full time privacy, in other units	1	4	3	13
Part time privacy, in other units	4	6	13	59

🟥 Significantly different than overall mean

Finally, we also see a strong correlation between non-salary privacy budget and privacy staff size

Mean Privacy Employee Size

BY PRIVACY BUDGET
(Excluding Salaries)

	$1–$100K	$101K– $1 million	More than $1 million
Full time privacy, in privacy program	1	5	11
Part time privacy, in privacy program	3	2	4
Full time privacy, in other units	0	5	5
Part time privacy, in other units	4	11	27

🟥 Significantly different than overall mean

Staff increases are expected for all privacy roles, and virtually no one expects staffing cuts

- By how much will staff increase? Respondents expect to add 7%-11% more staff, all told

Expected Employee Change in Coming Year

	% Saying Increase	% Saying Decrease	% Saying Stay the Same	Net % Change
Full time privacy, in privacy program	37%	2%	61%	+11%
Part time privacy, in privacy program	25%	1%	75%	+7%
Full time privacy, in other units	24%	0%	76%	+8%
Part time privacy, in other units	39%	2%	60%	+11%

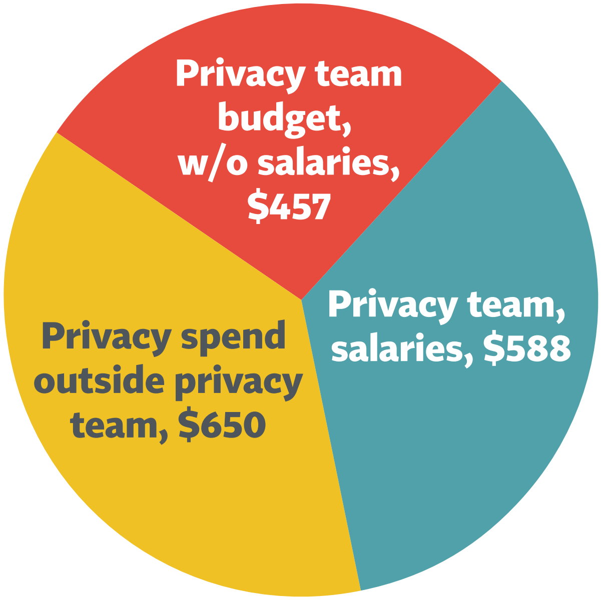
F2: In the coming year, do you expect the number of employees in each of these categories to increase, decrease, or stay the same? If increase or decrease, please enter your estimate of the percentage change you expect.

The average spend on privacy is close to $2 million in these companies…

- The non-salary budget for the privacy practice itself is $457k—the rest is made up of salaries and spending on privacy outside the privacy group.
- Note, again, that the median total spend is much lower than the mean: $450K across all categories

TOTAL PRIVACY SPEND
2016 MEAN: $1.7M 2016 MEDIAN: $415,000
Mean spending per employee: $354

Estimated Privacy Spend (000)



F4: And what is the total privacy spend for your company in each of the following categories?

As one might expect, privacy spend tends to increase with company size…

- Especially for those with 5,000 or more employees

KEY SEGMENT DIFFERENCES

Estimated Privacy Spend (000)

BY EMPLOYEE SIZE

	Under 100	100–999	1–4.9K	5–24.9K	25–74.9K	75K+
Privacy Team Budget, w/o Salaries	$7.6	$82.7	$309.0	$531.3	$447.9	$929.2
Privacy Team Salaries	$24.3	$188.7	$292.4	$866.4	$494.9	$980.5
Spend Outside Privacy Team	$11.5	$38.1	$137.5	$336.7	$755.3	$2,337.8
Total Privacy Spend (Mean)	$43.3	$309.5	$738.9	$1,734.4	$1,698.1	🟥 $4,247.5

🟥 Significantly different than overall mean

Privacy budget generally increases as company revenues increase

KEY SEGMENT DIFFERENCES

Estimated Privacy Spend (000)

BY COMPANY REVENUE

	Under $100 million	$100–$999 million	$1–$24 billion	$25 billion or more
Privacy Team Budget, w/o Salaries	$64.5	$98.5	$742.7	$750.4
Privacy Team Salaries	$205.6	$360.5	$599.7	$1,470.4
Spend Outside Privacy Team	$61.2	$154.6	$716.5	$2,030.2
Total Privacy Spend (Mean)	$331.3	$613.6	$2,058.9	$4,251.0

🟥 Significantly different than overall mean

‘Regulated’ businesses not only have more privacy employees, but a higher privacy team budget as well

KEY SEGMENT DIFFERENCES

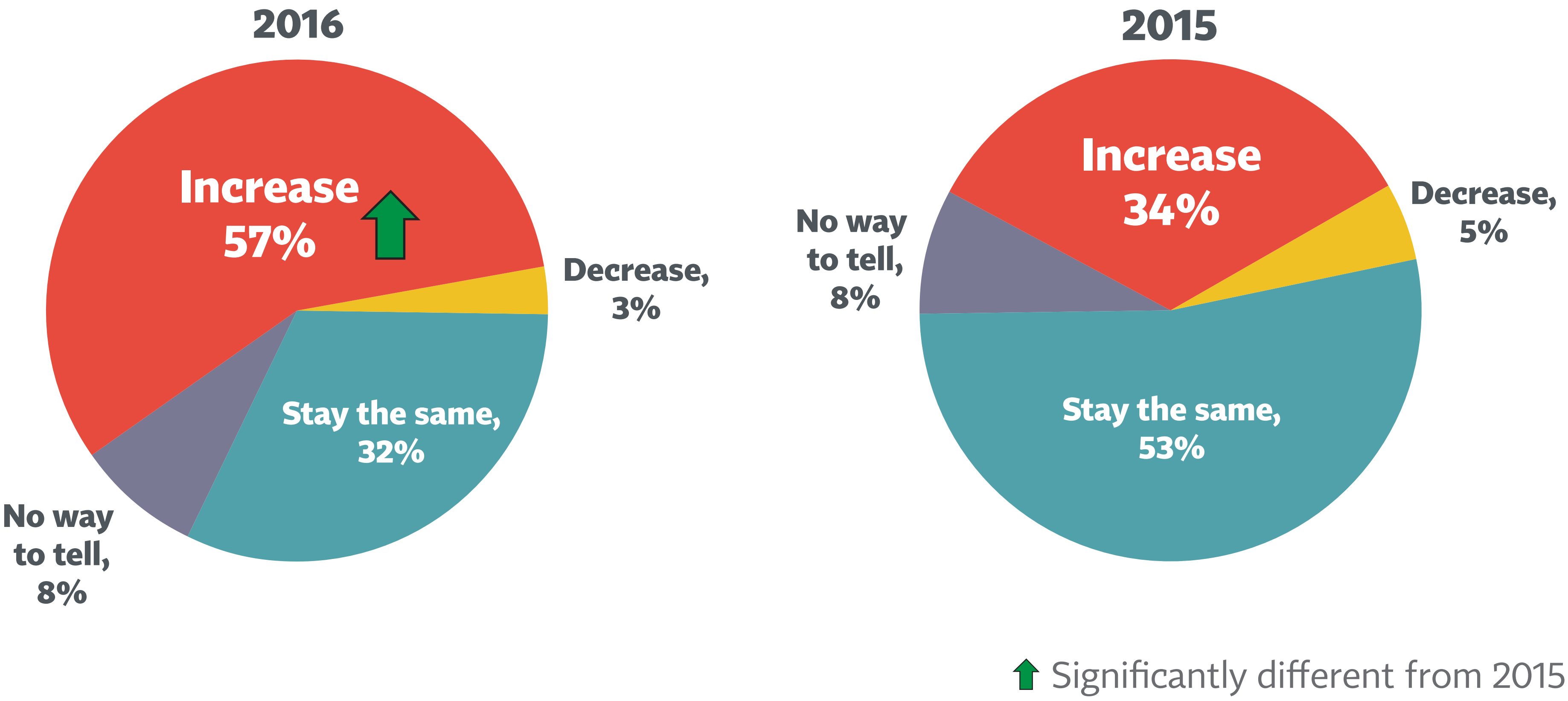
Estimated Privacy Spend, By Industry Category (000)

	BY INDUSTRY CATEGORY			BY CUSTOMER TARGET		
	Regulated	Unregulated	Gov’t	B2B	B2C	Both
Privacy Team Budget, w/o Salaries	$681.4	$348.7	$17.0	$511.6	$196.1	$540.6
Privacy Team Salaries	$675.9	$619.9	$417.2	$386.7	$598.6	$699.6
Spend Outside Privacy Team	$779.1	$728.1	$294.8	$431.9	$327.4	$918.2
Total Privacy Spend (Mean)	$2,136.5	$1,696.8	$729.0	$1,330.2	$1,122.2	$2,158.4

2016 sees a sharp jump in those saying their privacy budget will increase next year

- In 2015, 34% expected an increase; in 2016, it's 57%

In Next 12 Months, Privacy Budget Will…

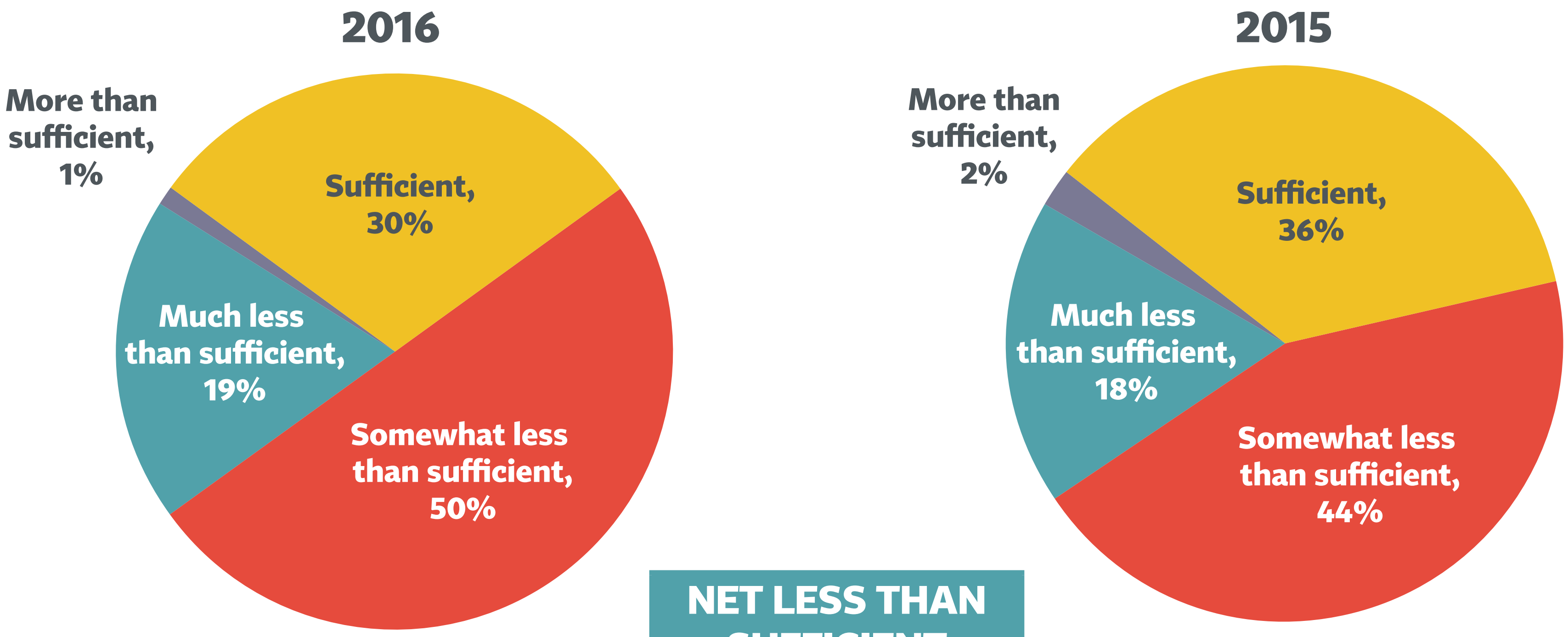


F5: In the next 12 months, you expect your company's privacy budget will …

As in 2015, about two-thirds feel their current privacy budget is not sufficient for their needs

- The “insufficient” proportion is up directionally from 2015, 62% to 69%

Privacy Budget Is…



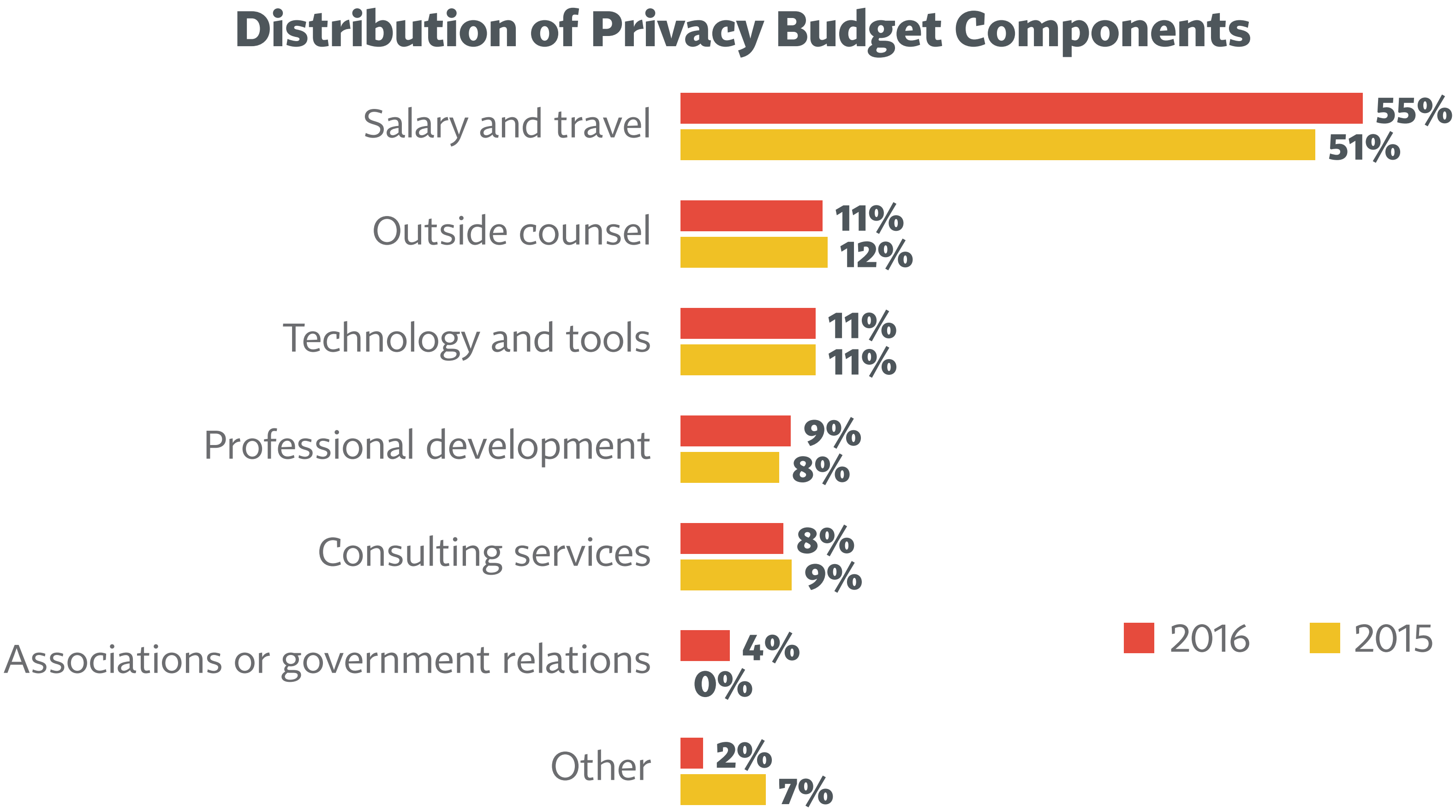
NET LESS THAN SUFFICIENT

2016: 69%
2015: 62%

F6: In your opinion, your company’s privacy budget is … to meet your privacy obligations

There's been little change in how privacy budgets are divvied up by component

- As in 2015, the lion's share goes toward salary and travel, with no statistically significant changes in any category

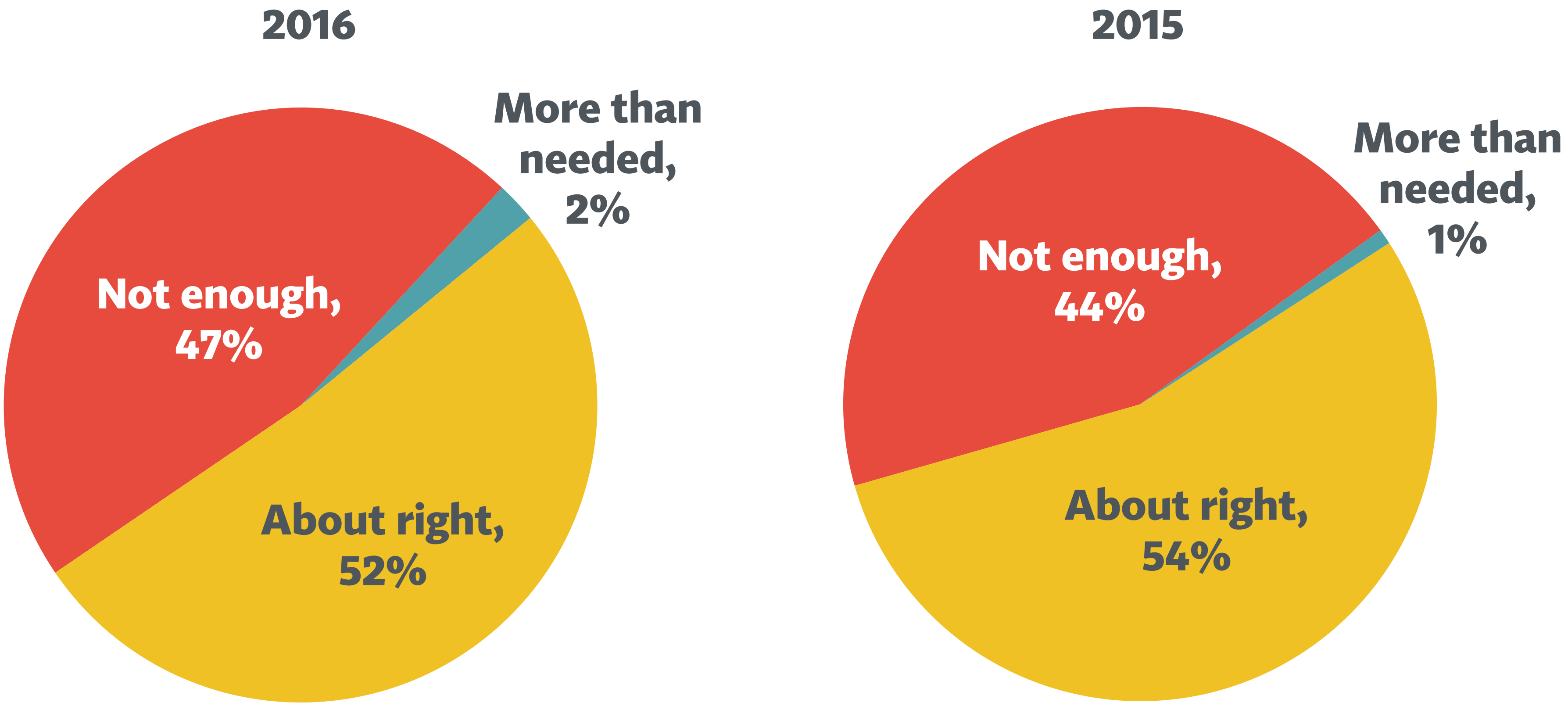


F7: What percent of your company's total privacy budget is allocated to each of the following components?

As with budget generally, there is a strong feeling not enough is spent on training

- 47% say their privacy training budget is inadequate, similar to the 44% last year

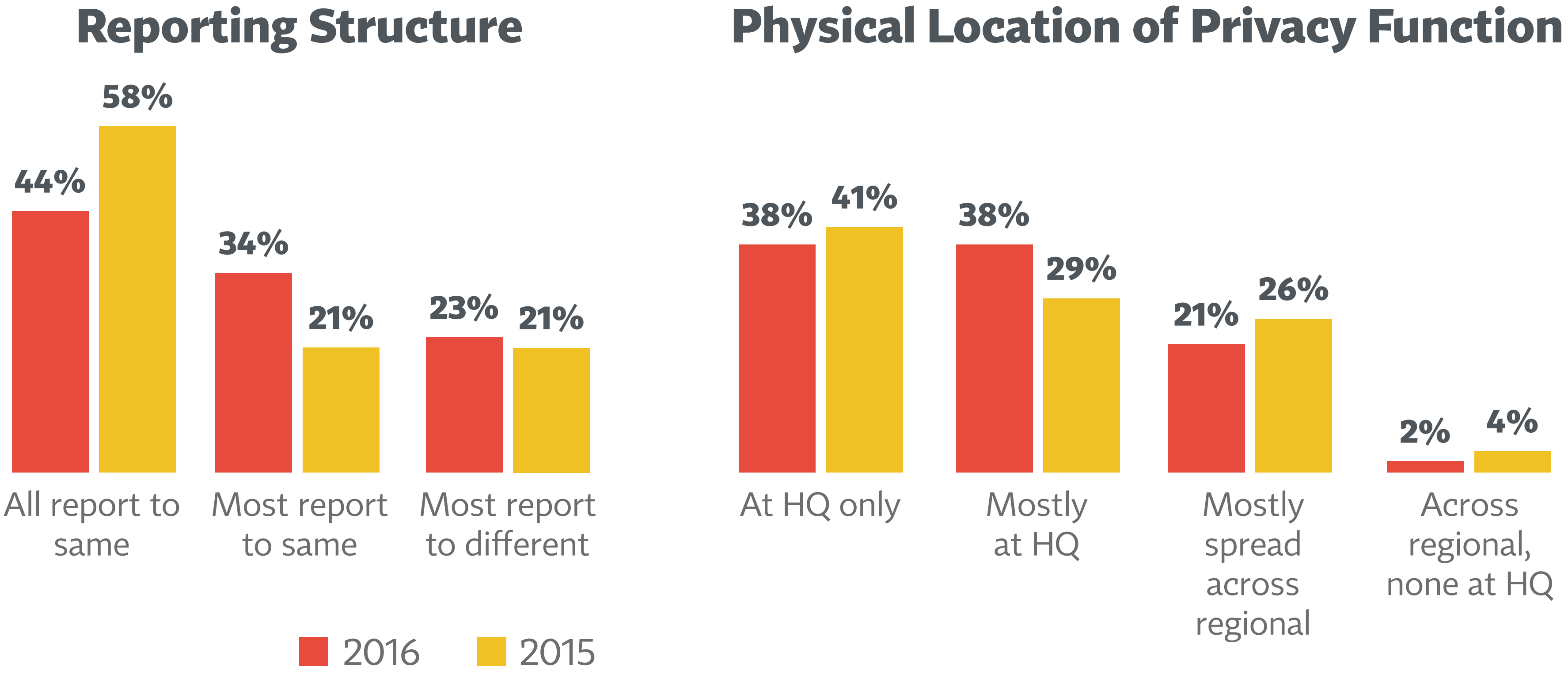
Amount Spent on Privacy Training Is…



F8: The amount your company invests on privacy training of its employees is …

The 2016 results suggest there's less centralization of reporting than there was in 2015

- 44% say privacy employees all report to the same people, vs. 58% last year.
- However, there's been little change in the geographic location of the privacy function: The majority say all or most of it is housed at headquarters

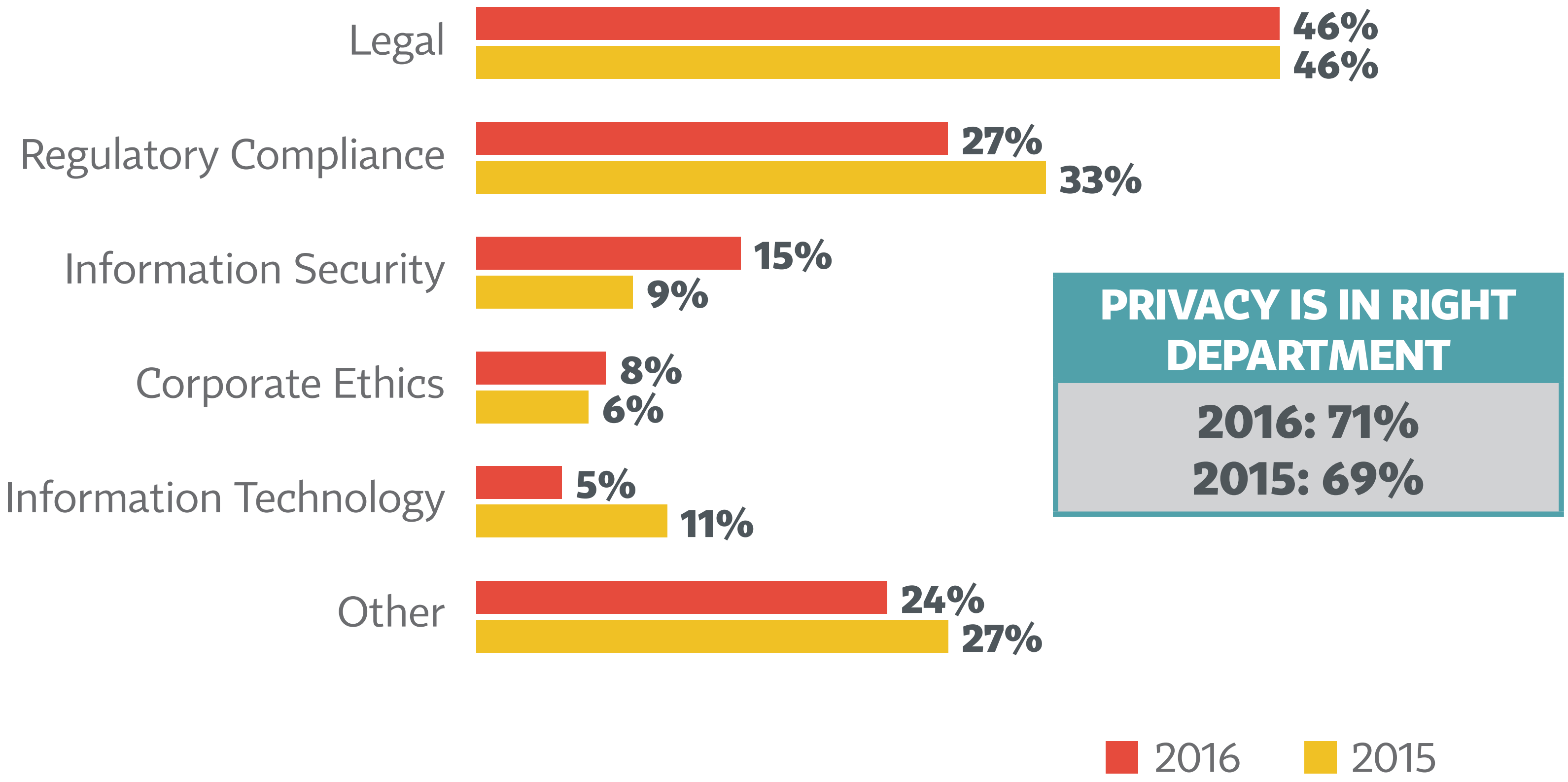


F10: Which of the following best describes the reporting structure for you and the colleagues you work with in privacy?
F11: The privacy function of your company is geographically located ...

Nearly half of respondents say their privacy program is located in their legal department

- As in 2015, a strong majority feel that the function is located in the correct department: 71%

Organizational Location of Privacy Function



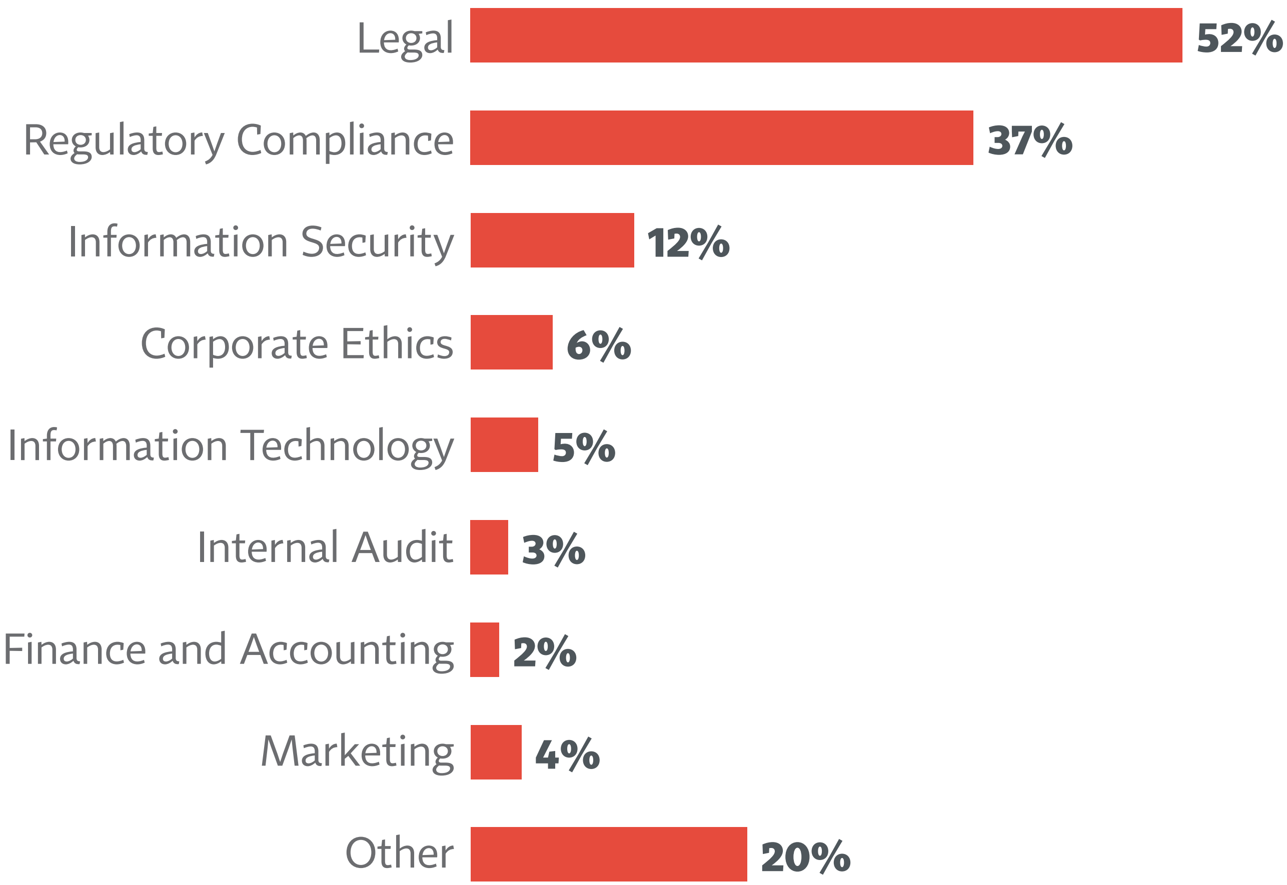
PRIVACY IS IN RIGHT DEPARTMENT

2016: 71%
2015: 69%

F12: Where within your company is the privacy function located?
F13: In your opinion, is the privacy function located in the right department?

For the relatively few who feel privacy is not in the correct department, a majority also feel it should be in legal

Better Organizational Location of Privacy Function
Responding: Think function is in wrong department



F14: Where within your company should the privacy function be located?

There are 2.4 reporting rungs, on average, between the privacy lead and the CEO

- In addition, note that 63% of respondents say that they themselves are the head of privacy

Hierarchical Characteristics

RUNGS BETWEEN PRIVACY LEADER AND CEO	
1 rung: 18%	Mean 2.4
2 rungs: 36%	
3+ rungs: 46%	

FULL-TIME STAFF REPORTING TO RESPONDENT
Mean 4.4

Outliers over 1000 removed

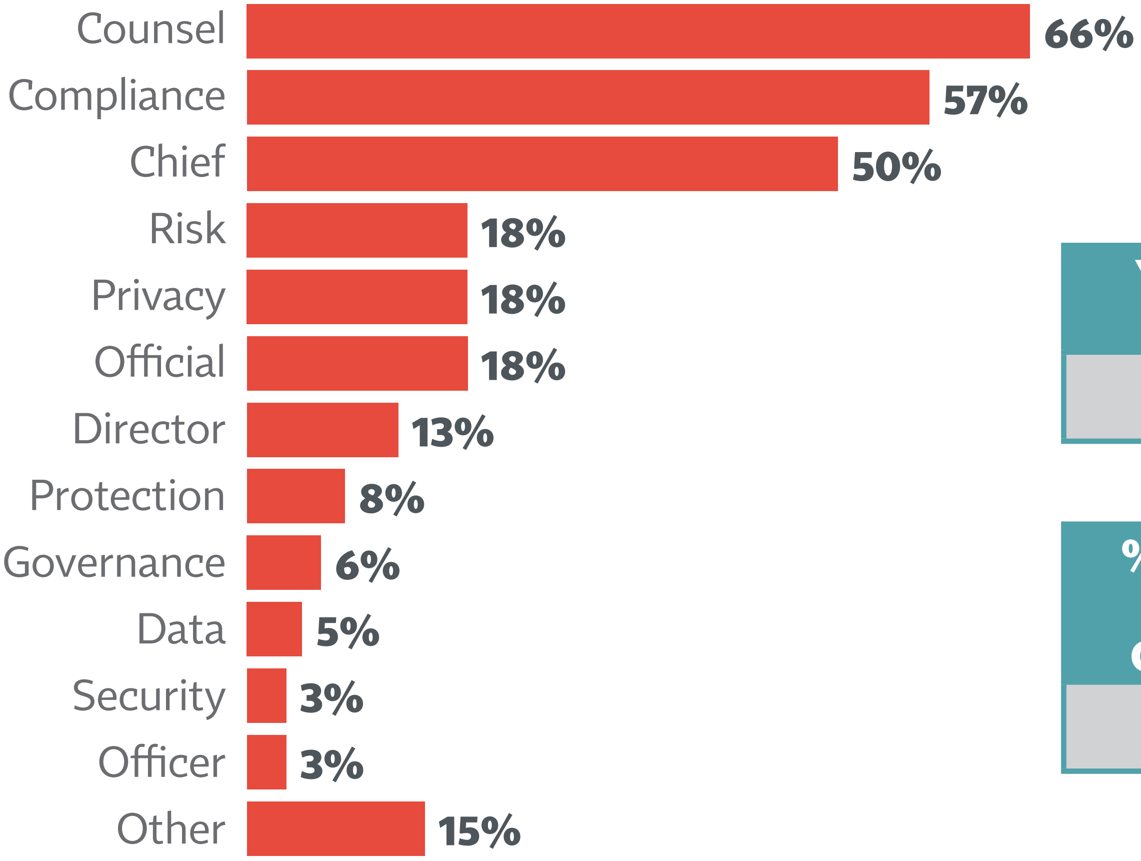
RESPONDENT IS PRIVACY LEAD?
YES: 63%

F15: How many full-time staff report to you?
F19: How many vertical rungs away from the CEO is the privacy leader?
F21: Are you the company's privacy leader, or is that someone else?

With privacy most likely to be in legal, it's not surprising that the most common term in the lead's title is "counsel"

- Only two other terms were cited with reasonable frequency: "compliance" and "chief"

Terms in Title of Privacy Leader



YEARS HAVE HAD PRIVACY LEADER

Mean 6.3

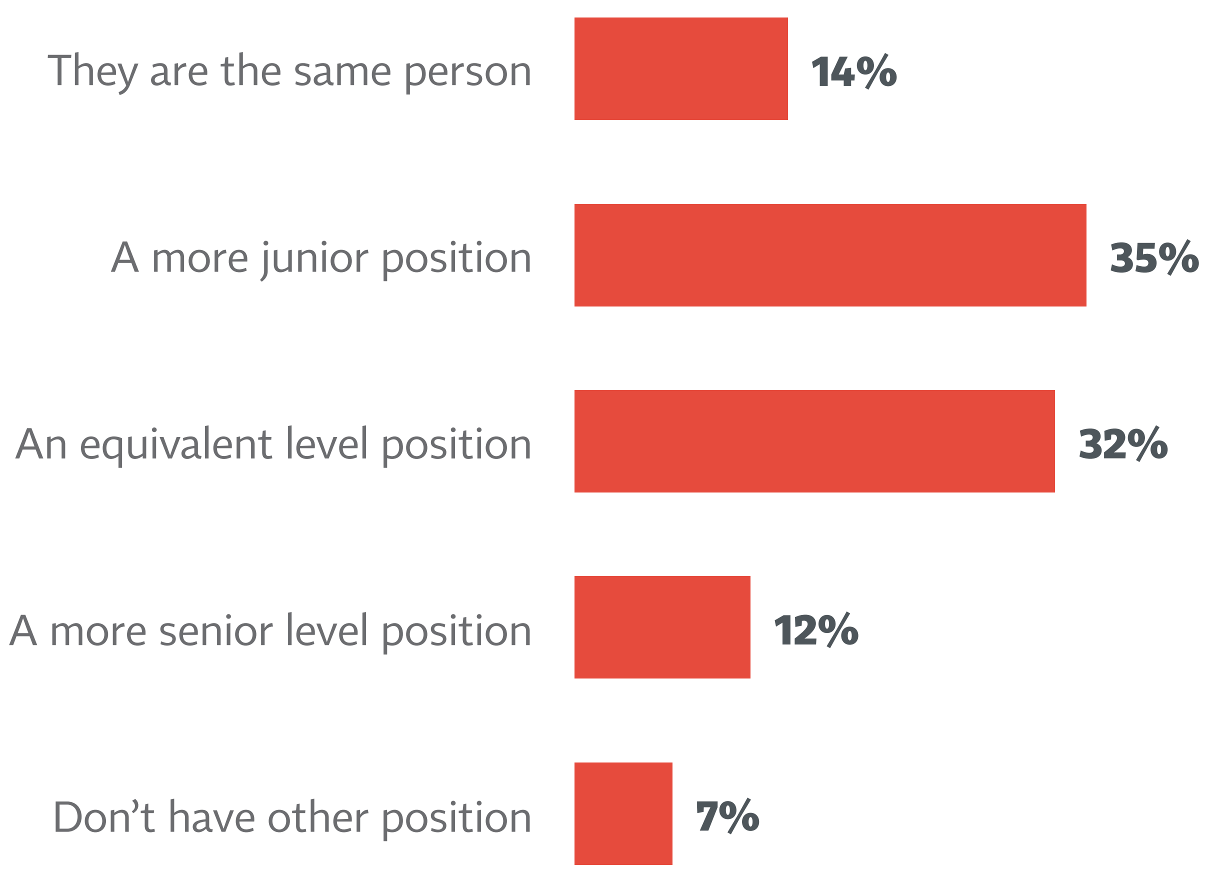
% WHERE PRIVACY LEADER WORKS ONLY ON PRIVACY

36%

F18: Which of the following words occur in the official, formal title of the person in rung #1 [or Privacy lead from F22]?
F20: For how many years has your company had a privacy leader or chief privacy officer?
F23: Does the individual designated as your company's privacy leader have responsibilities other than privacy?

The privacy leader is more likely to be junior to the CISO

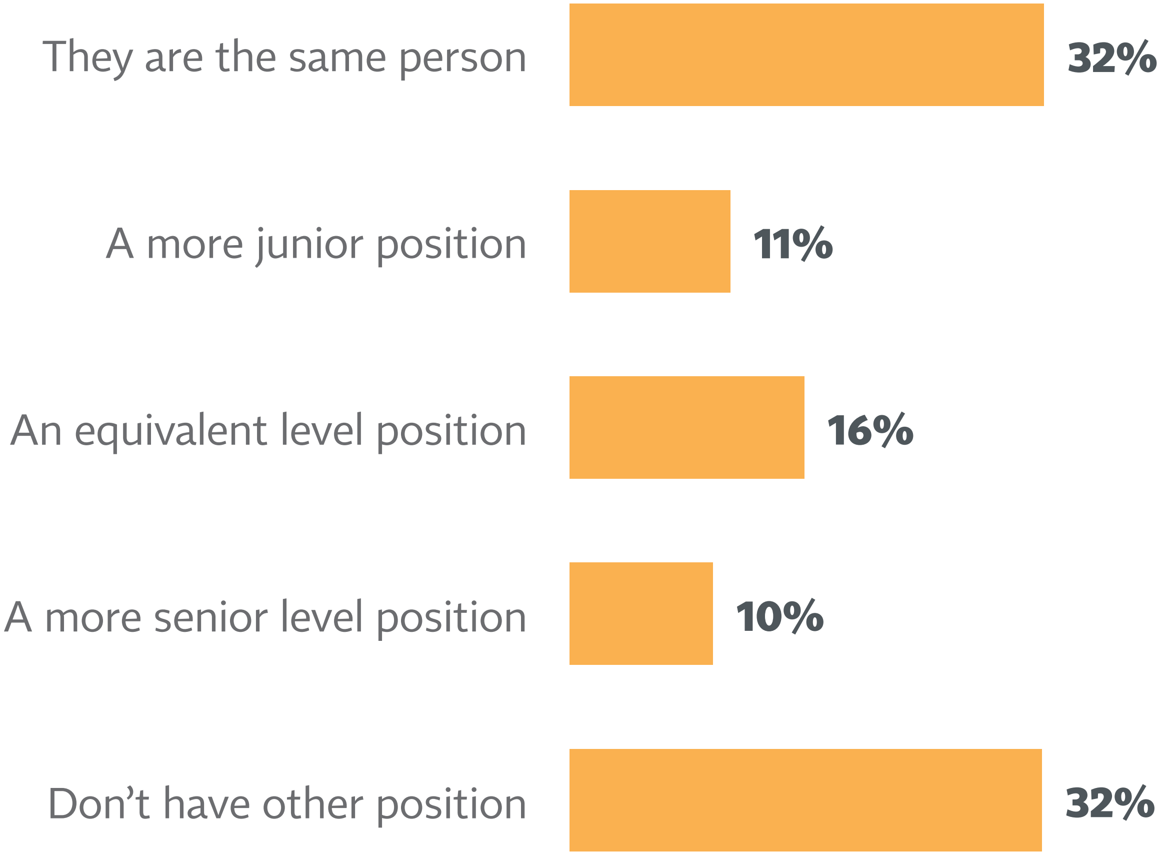
Privacy Leader Relative to CISO



F23a: How does the privacy leader/chief privacy officer compare with your company’s chief information security officer or the highest level information security person in the company? The privacy leader/chief privacy officer is …

However, the privacy leader is probably also the lead privacy counsel or at a similar level

Privacy Leader Relative to 'Chief Privacy Counsel'

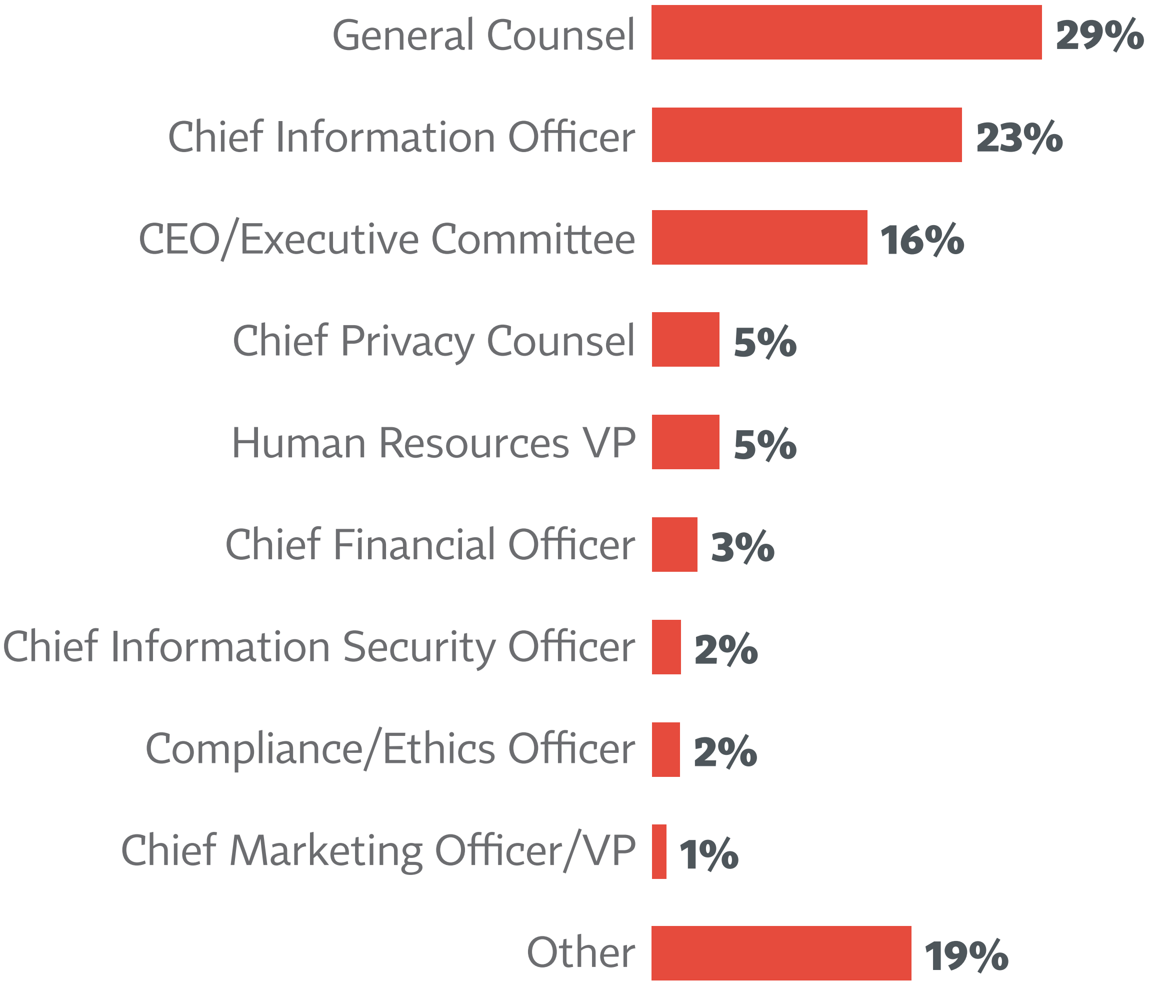


F23b: How does the Privacy Leader compare with your company's chief privacy counsel? The Privacy Leader is …

The privacy lead likely reports to the General Counsel or the CIO

- Next on the list, reported by 16%, is the CEO or Executive Committee

To Whom Top Privacy Person Reports

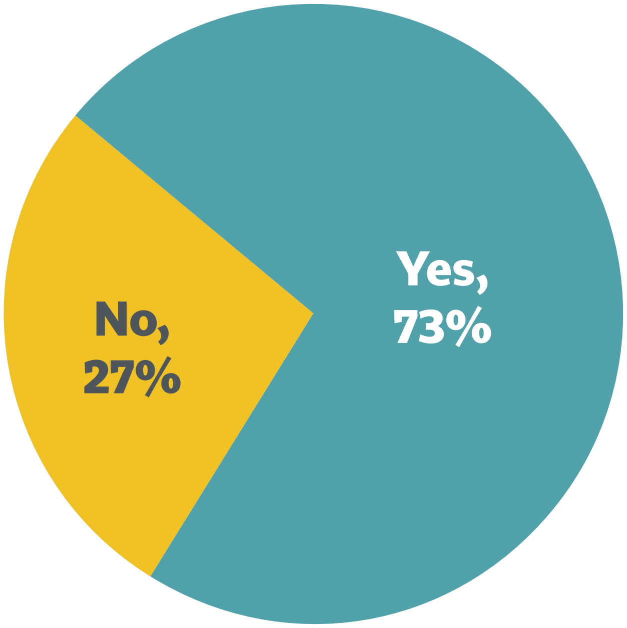


F26: Who does the top privacy person report to?

3 in 4 say privacy matters get reported to the Board of Directors

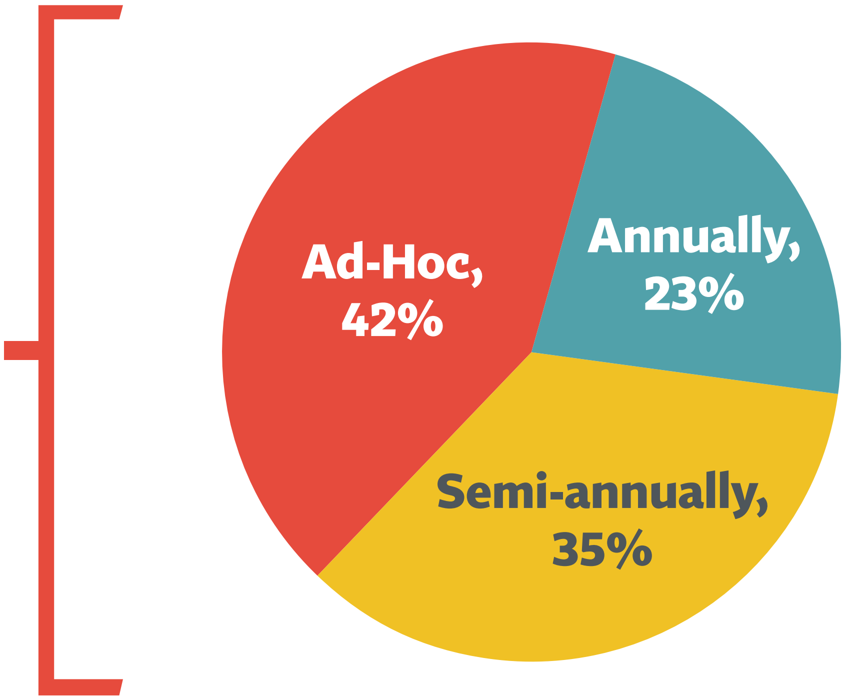
- However, frequency of reporting to the Board is split: 42% report matters ad-hoc, 35% semi-annually, and 23% annually

Privacy Matters Reported to Board?



How Often?

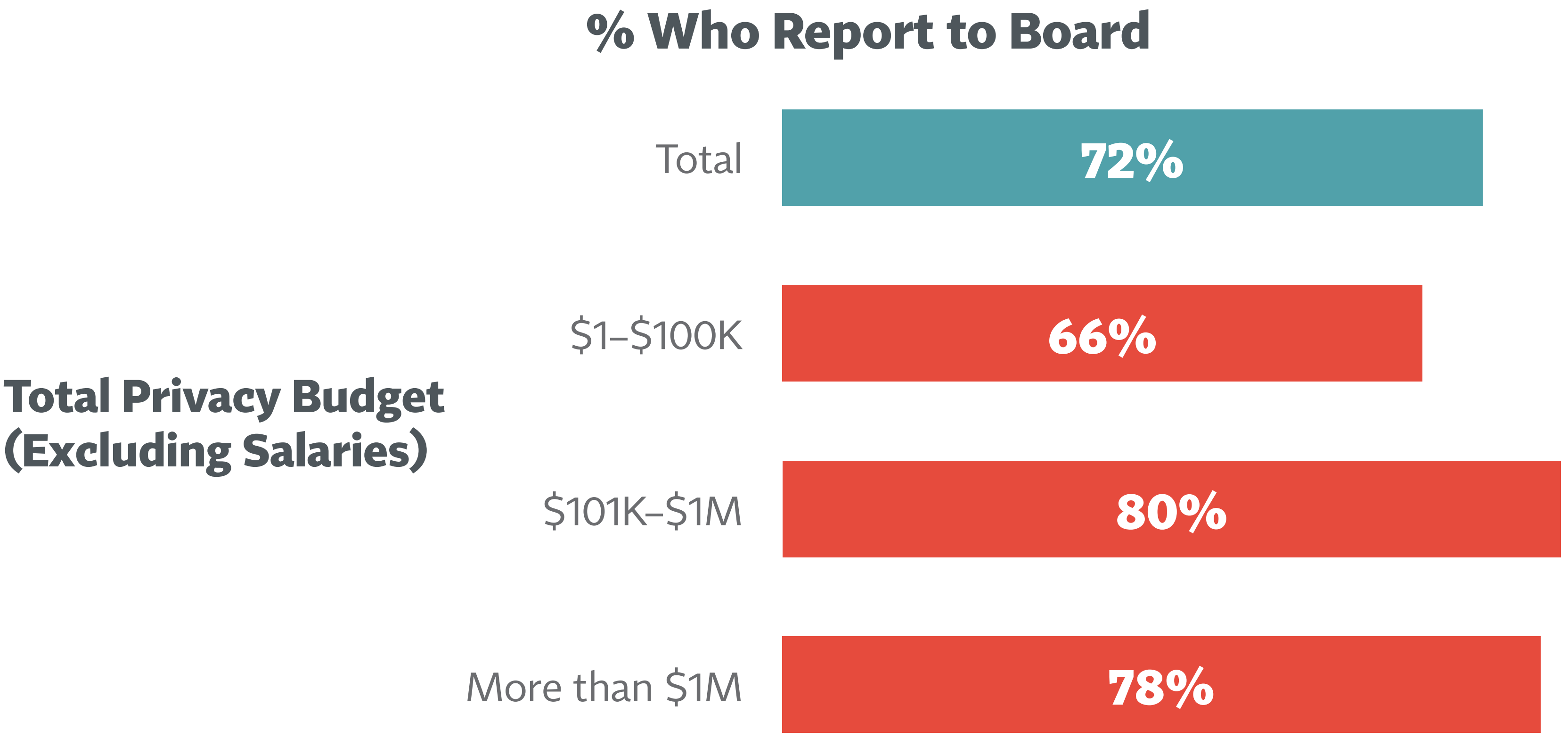
Base: Matters Reported to Board



F27: Are privacy-related matters at your organization reported to the board of directors or the board level generally?
F28: How often are privacy matters reported at the board level?

Companies with the highest privacy budgets are directionally more likely to report to their boards

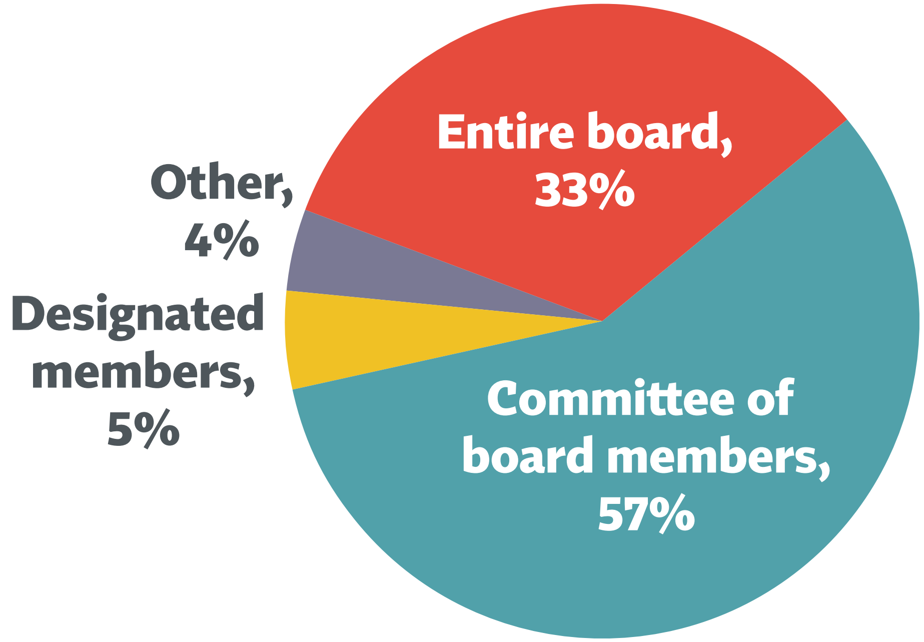
KEY SEGMENT DIFFERENCES



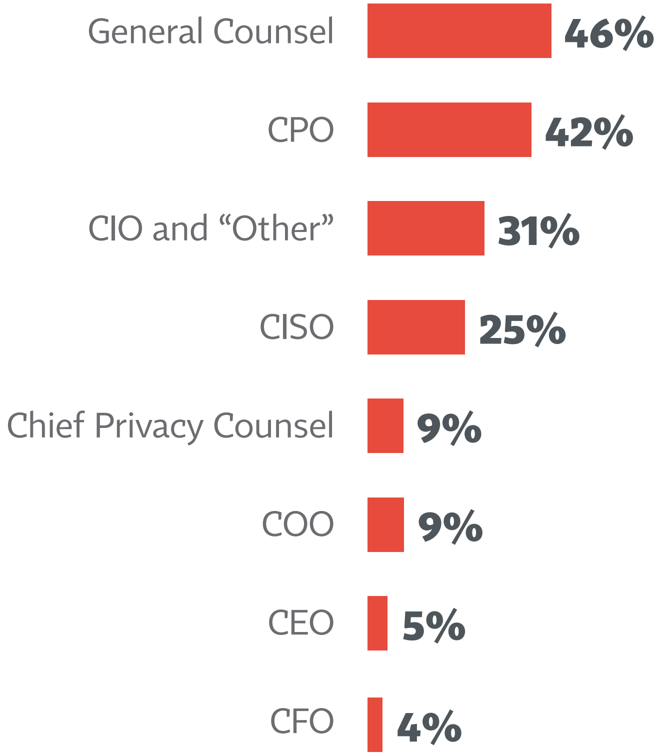
F27: Are privacy-related matters at your organization reported to the board of directors or the board level generally?

Board reporting is usually to a committee of members; the General Counsel is most often the messenger

To Whom Matters Reported
Base: Matters Reported to Board



Who Does Reporting
Base: Matters Reported to Board

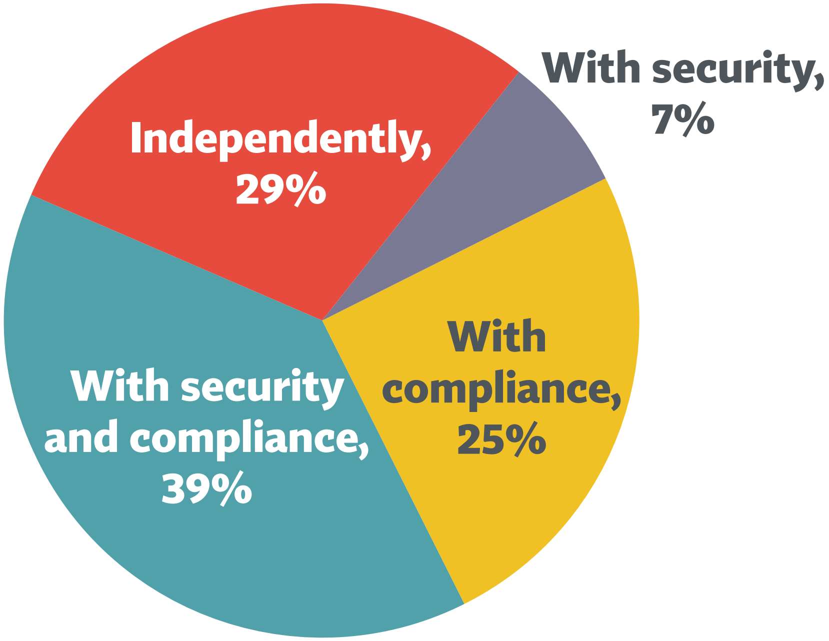


F29: Who at the board level are privacy matters reported to?
F32: Who at least sometimes reports privacy matters at the board level?

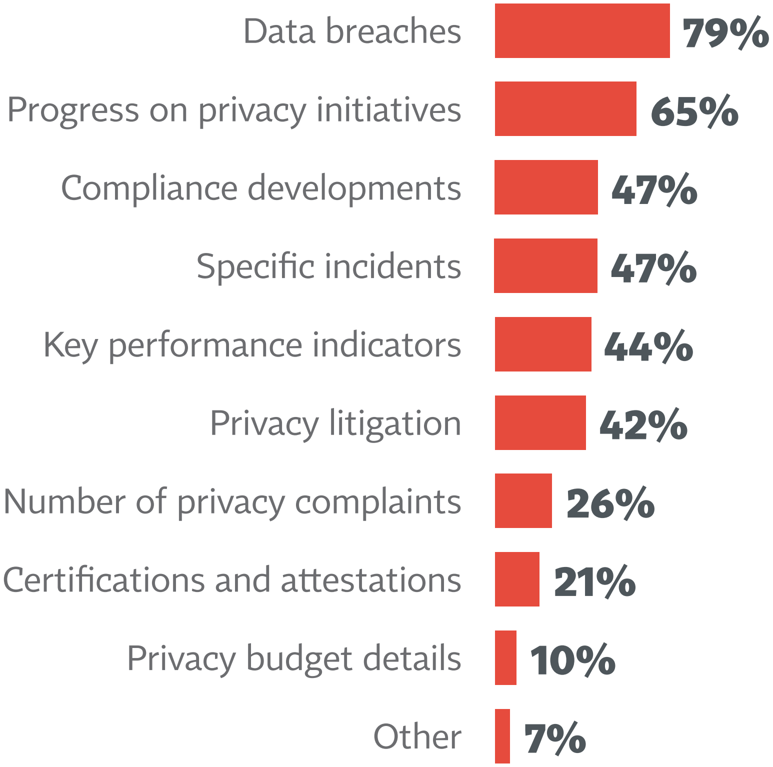
Privacy matters reported to the Board are most likely to be reported along with security/compliance matters

- Just 29% say privacy matters are reported independently, by themselves.
- Moreover, data breaches and privacy program progress are the most common topics shared with the Board

How Privacy Topics Treated with Board
Base: Matters Reported to Board



Specific Topics Reported
Base: Matters Reported to Board



F30: Privacy matters are reported to the board…
F31: What privacy topics are reported at the board level?

Independent reporting of privacy matters to the board is also more common in unregulated firms

KEY SEGMENT DIFFERENCES

- In regulated companies, privacy matters are more likely than average to be reported along with compliance matters

How Matters Reported to Board

	BY INDUSTRY CATEGORY		BY CUSTOMER TARGET		
	Regulated	Unregulated	B2B	B2C	Both
Independently	25%	41%	27%	24%	32%
With Security	5%	9%	4%	22%	3%
With Compliance	34%	12%	28%	15%	28%
With Both	36%	38%	41%	39%	37%

🟥 Significantly different than overall mean

Finance leads sectors in privacy staffing

- But government departments are trying their best to catch up

KEY SEGMENT DIFFERENCES

Privacy Group Structure:
Segments with Higher Than Average Results

BY INDUSTRY

	Gov’t	Finance	Health	Tech
Full or part time employees in privacy program	4	14	10	11
Privacy program budget + salaries (not including outside team) (000)	$463.3	$1,236.3	$1,514.1	$1,107.1
Net change expected in privacy employees	+30%	+11%	+13%	+8%
Privacy budget will increase	59%	62%	55%	67%
Privacy budget less than sufficient	75%	68%	79%	60%

▨ Significantly different than overall mean

Firms with 5–24K employees and those in the early stage are most likely to say their budget isn't enough…

KEY SEGMENT DIFFERENCES

- The largest firms are most likely to say they'll increase their budgets.
- And those early-stage firms expect the largest net increase in privacy employees

Privacy Group Structure:
Segments with Higher Than Average Results

BY EMPLOYEE SIZE

	<5K	5–24.9K	25–74.9K	75K+
Net change expected in privacy employees	+7%	+16%	+13%	+8%
Privacy budget will increase	53%	56%	50%	▨ 74%
Privacy budget less than sufficient	67%	▨ 80%	67%	55%

BY PRIVACY LIFESTAGE

	Early	Middle	Mature
Full or part time employees in privacy program	10	5	▨ 14
Privacy program budget + salaries (not including outside team) (000)	$525.3	$1,019.2	▨ $1,318.8
Net change expected in privacy employees	▨ +21%	+10%	+7%
Privacy budget will increase	51%	54%	62%
Privacy budget less than sufficient	▨ 89%	73%	53%

▨ Significantly different than overall mean

Contents

1 Executive Summary

2 Background and Method

3 How the Job of Privacy Is Done

4 Background on Companies and Individuals

5 Privacy Group Characteristics: Structure

6 **Privacy Group Characteristics: Responsibilities**

7 Privacy Function in the Business Context

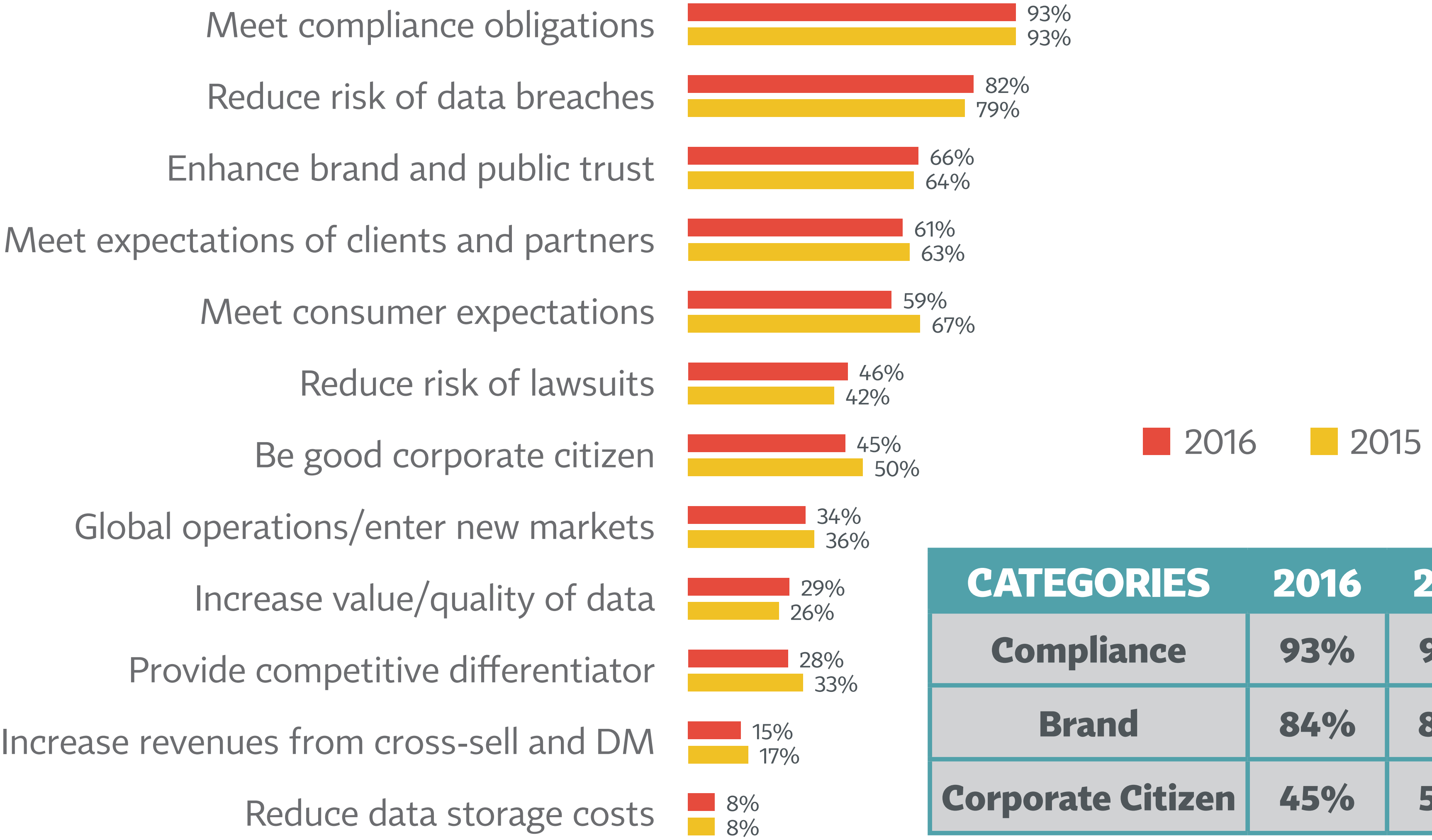
8 Internal and External Resources

9 Thoughts About the Profession

10 Cross Border Data Transfer

As in 2015, the top two reasons for having a privacy function: compliance and reduced risk of data breaches

Reasons for Having Privacy Function



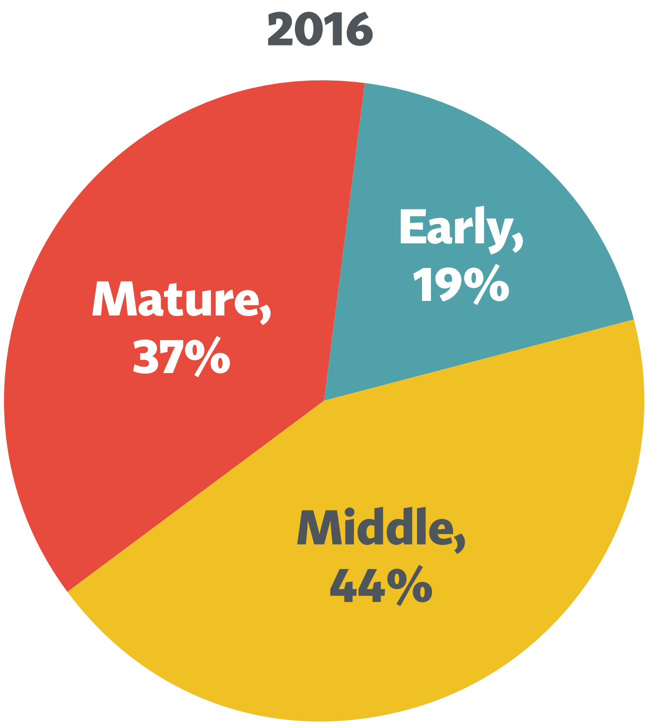
CATEGORIES	2016	2015
Compliance	93%	93%
Brand	84%	88%
Corporate Citizen	45%	50%

E6: Which of the following would you say are the main reasons that the leadership of your company supports and funds a privacy function?

The average privacy function has been in existence for 6 and a half years

- And the distribution of firms by level of privacy maturity has remained the same since last year, with about one-third considering themselves “mature”

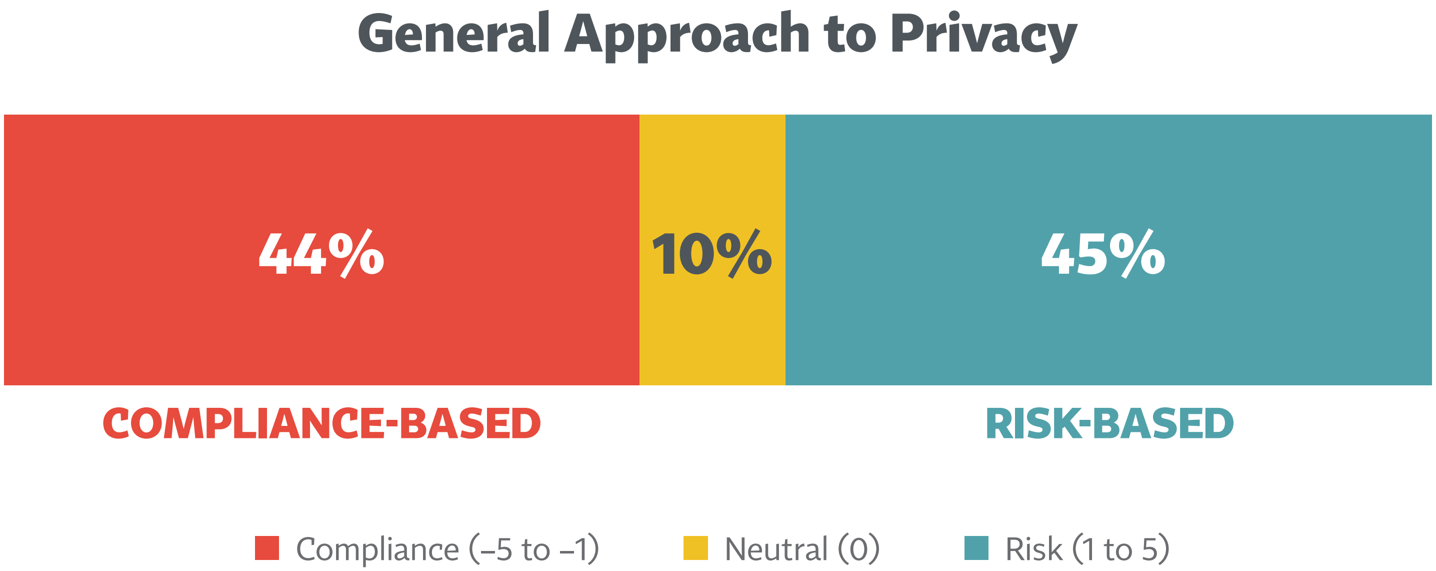
Privacy Function Lifecycle Stage



YEARS WITH PRIVACY (MEAN)
6.5

E1: Please select the maturity stage of your company’s privacy program.
E2: For how many years has your company had a dedicated privacy program?

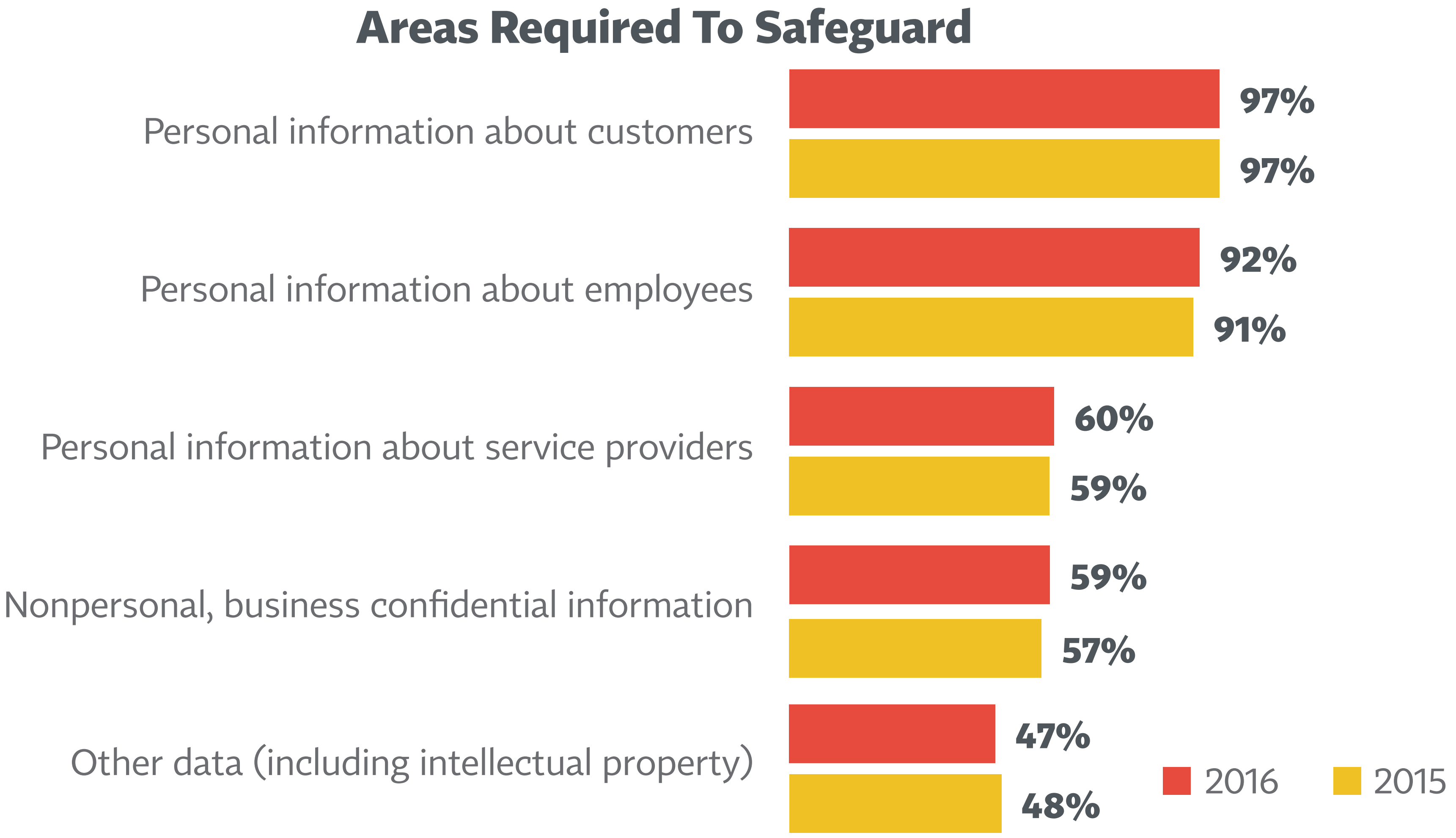
Firms are exactly split in having a compliance-based vs. risk-based approach to privacy



E8: Please use the slider below to indicate where your company falls on this spectrum between compliance-based or risk-based.

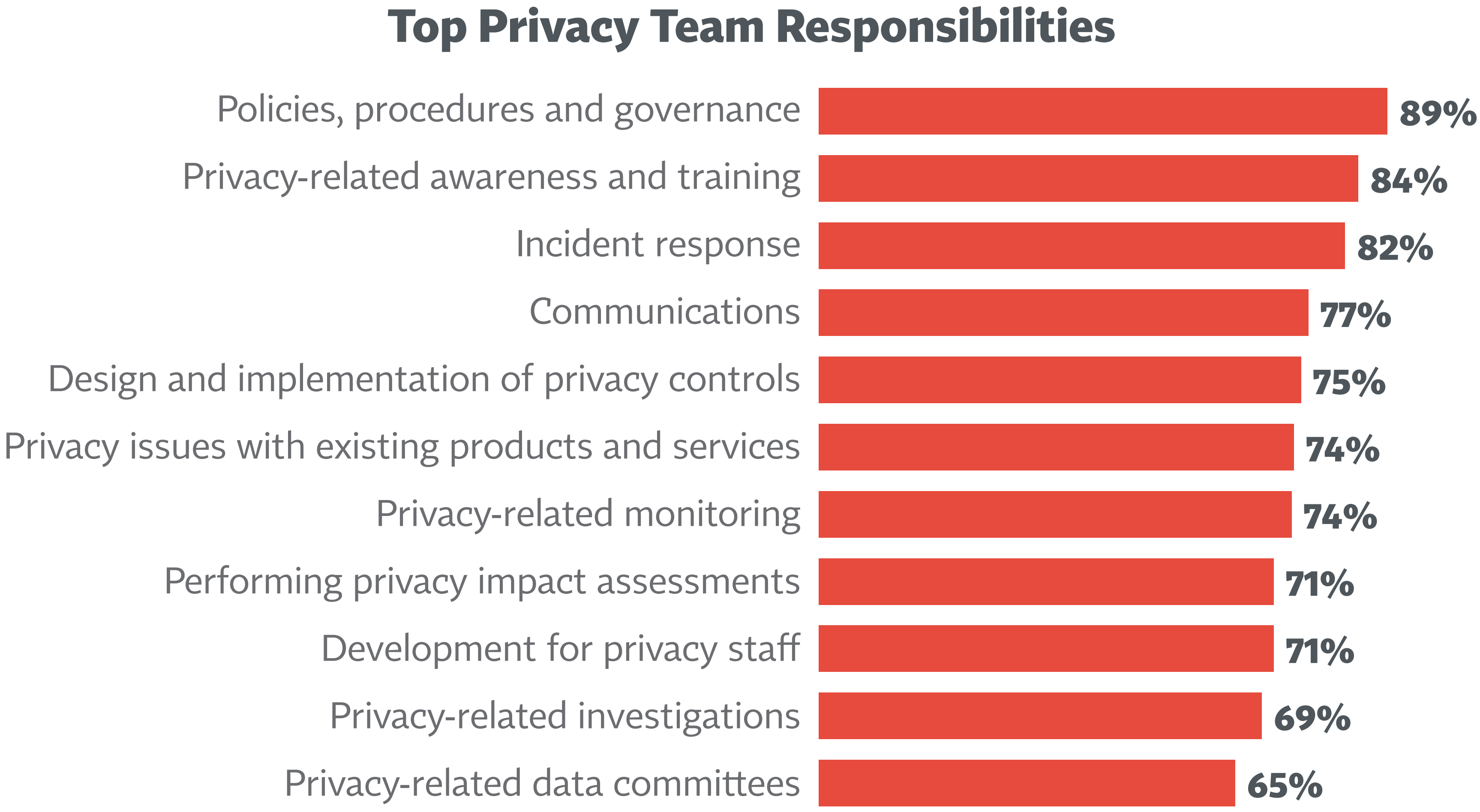
Nearly all privacy programs say they need to safeguard customer and employee information

- As in 2015, about 6 in 10 are also required to safeguard service provider and non-personal business data



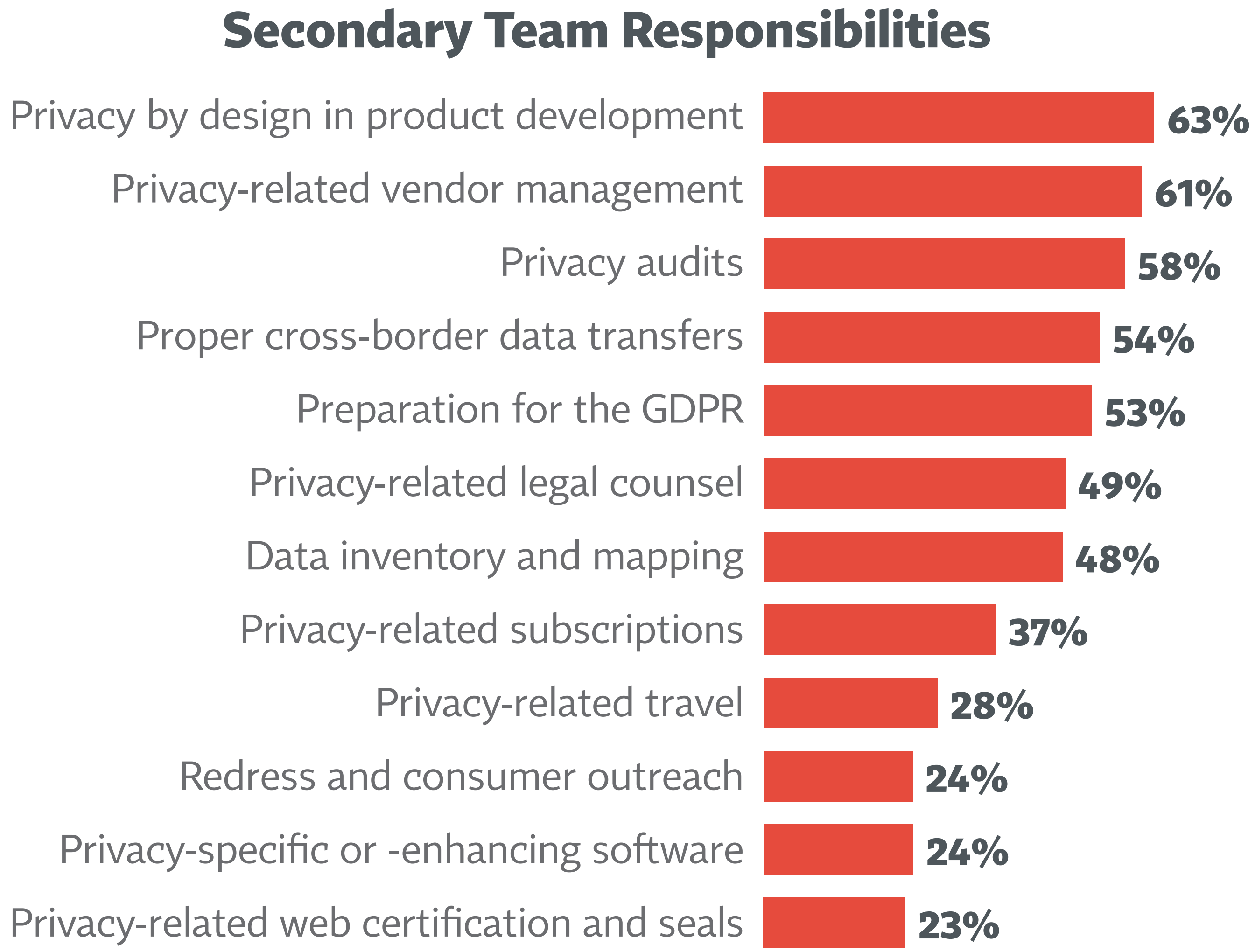
E4: What types of information is your privacy program required to safeguard?

The most common privacy team responsibilities range from policies and governance to data committees



D5: Which of the following is your team responsible for accomplishing on an annual basis?

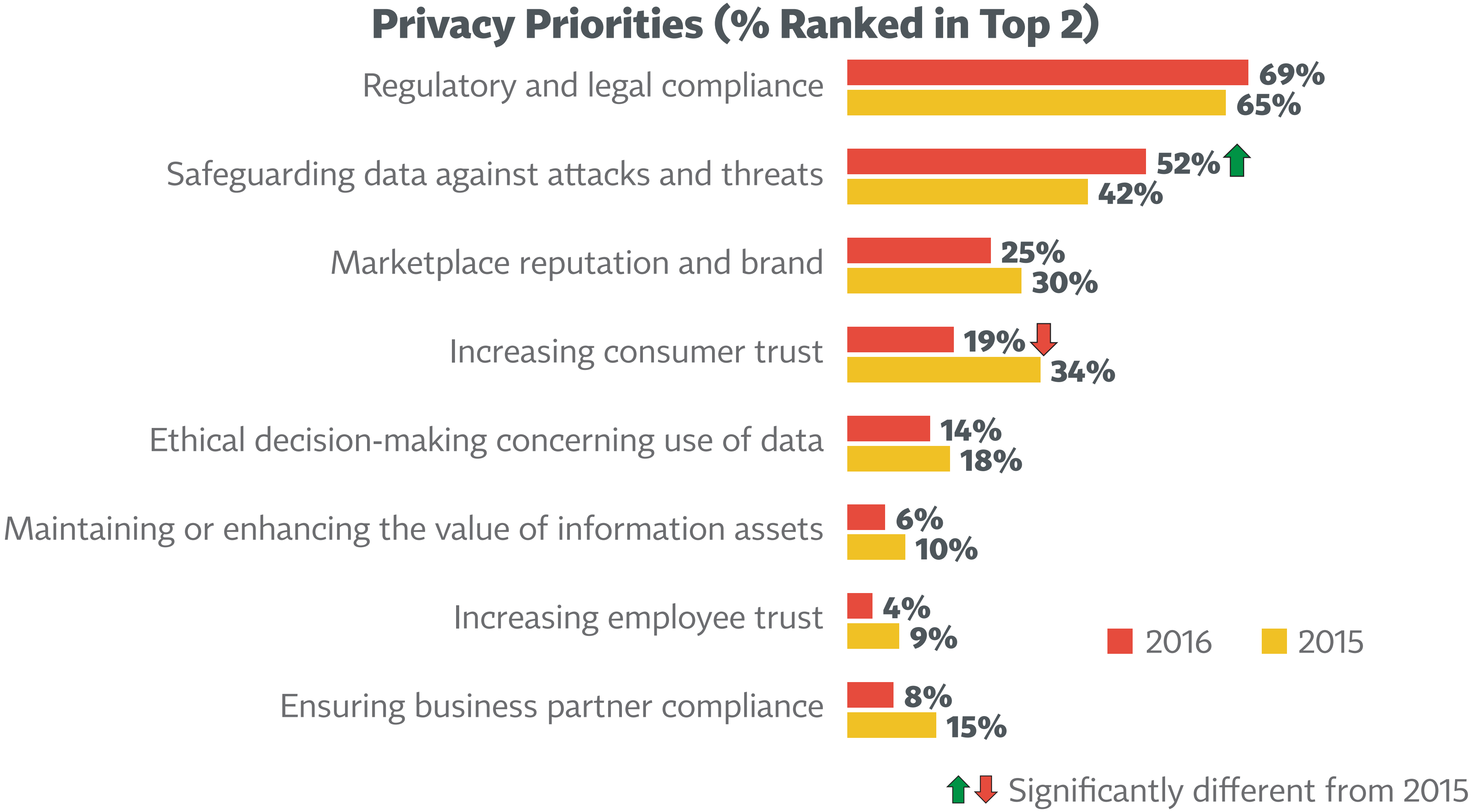
Secondary responsibilities run from privacy by design and vendor management down to web certification



D5: Which of the following is your team responsible for accomplishing on an annual basis?

When asked to narrow down responsibilities to highest priorities, compliance wins out

- Note, however, that safeguarding data has increased as a top priority



E5: Please rank these priorities from 1 = highest to 8 = lowest for your company.
Do not assign any rank for a priority that is not applicable to your company.

Reasons for having a privacy practice differ to some extent by type of firm

KEY SEGMENT DIFFERENCES

- Entering new global markets is a more important reason for finance and tech firms

Privacy Group Responsibilities: Segments with Higher Than Average Results

BY INDUSTRY

	Finance	Health	Tech
Main Reasons for Privacy: Global operations/new markets	▨ 46%	15%	▨ 45%
Main Reasons for Privacy: Compliance	▨ 100%	83%	90%

▨ Significantly different than overall mean

Avoiding lawsuits is a primary reason for having a privacy function among the largest firms

KEY SEGMENT DIFFERENCES

- Mature privacy practices offer a range of reasons, especially focused on enhancing trust and meeting consumer expectations

Privacy Group Responsibilities: Segments with Higher Than Average Results

BY EMPLOYEE SIZE

	<5K	5–24.9K	25–74.9K	75K+
Main Reasons for Privacy: Reduce lawsuits	40%	47%	37%	67%
Compliance-based	39%	44%	30%	72%

BY PRIVACY LIFESTAGE

	Early	Middle	Mature
Main Reasons for Privacy: Enhance brand and trust	62%	59%	76%
Main Reasons for Privacy: Meet consumer expectations	36%	58%	71%
Main Reasons for Privacy: Compliance	83%	93%	99%
Years with privacy program	2.0	5.4	10.2

🟥 Significantly different than overall mean

Companies in regulated industries are significantly more likely to consider their privacy program “mature”

KEY SEGMENT DIFFERENCES

Privacy Maturity Stage

	BY INDUSTRY CATEGORY			BY CUSTOMER TARGET		
	Regulated	Unregulated	Gov’t	B2B	B2C	Both
Early	13%	▨ 28%	20%	29%	22%	13%
Middle	42%	41%	42%	35%	53%	45%
Mature	▨ 45%	31%	38%	36%	26%	42%

▨ Significantly different than overall mean

DIRECTORS AND HIGHER

Companies with the highest privacy budgets are also the most likely to have mature programs

KEY SEGMENT DIFFERENCES

Privacy Maturity Stage

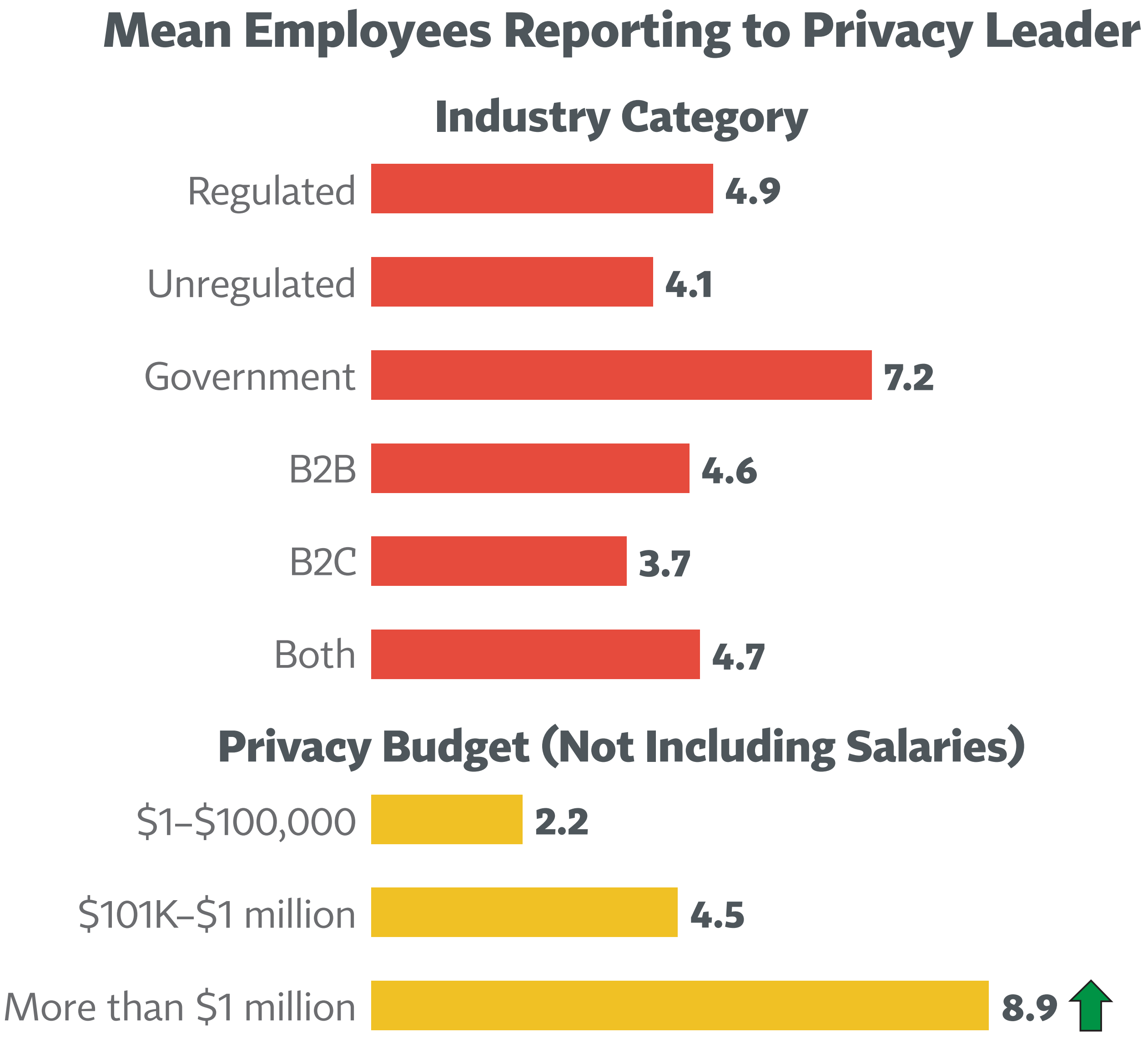
BY PRIVACY BUDGET
(Excluding Salaries)

	$1–$100K	$101K– $1 million	More than $1 million
Early	18%	21%	14%
Middle	40%	50%	31%
Mature	42%	30%	55%

▨ Significantly different than overall mean

Firms with the highest privacy budgets have the highest number of staff reporting to the privacy leader

KEY SEGMENT DIFFERENCES



F15: How many full-time staff report to you?

⬆ Significantly different than overall mean

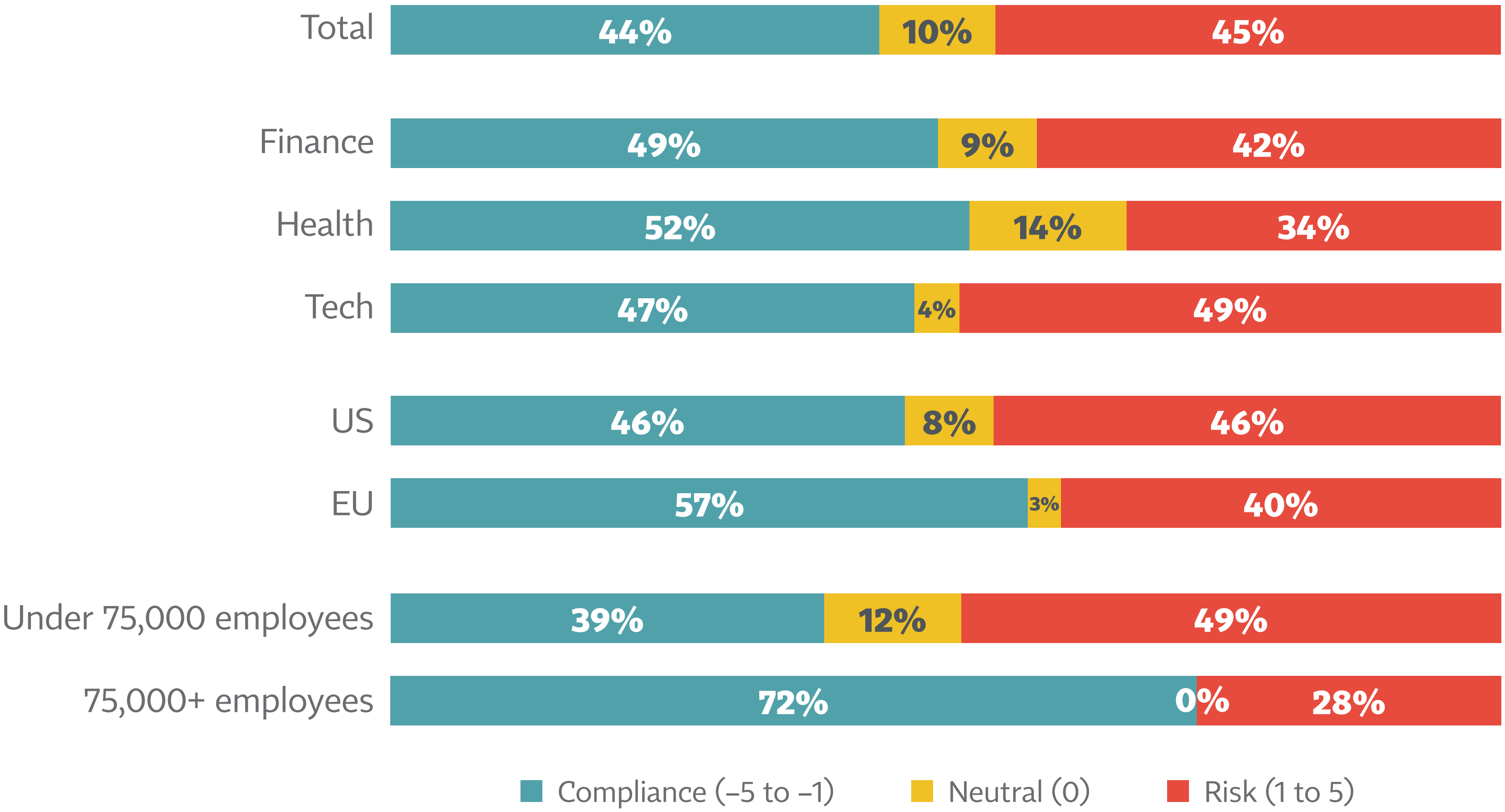
DIRECTORS AND HIGHER

Health care firms are least likely to be risk-focused

KEY SEGMENT DIFFERENCES

- Those with 75,000 or more employees are much more likely to be compliance-based

Compliance versus Risk
Segment differences



E8: Please use the slider below to indicate where your company falls on this spectrum between compliance-based or risk-based.

Contents

1 Executive Summary

2 Background and Method

3 How the Job of Privacy Is Done

4 Background on Companies and Individuals

5 Privacy Group Characteristics: Structure

6 Privacy Group Characteristics: Responsibilities

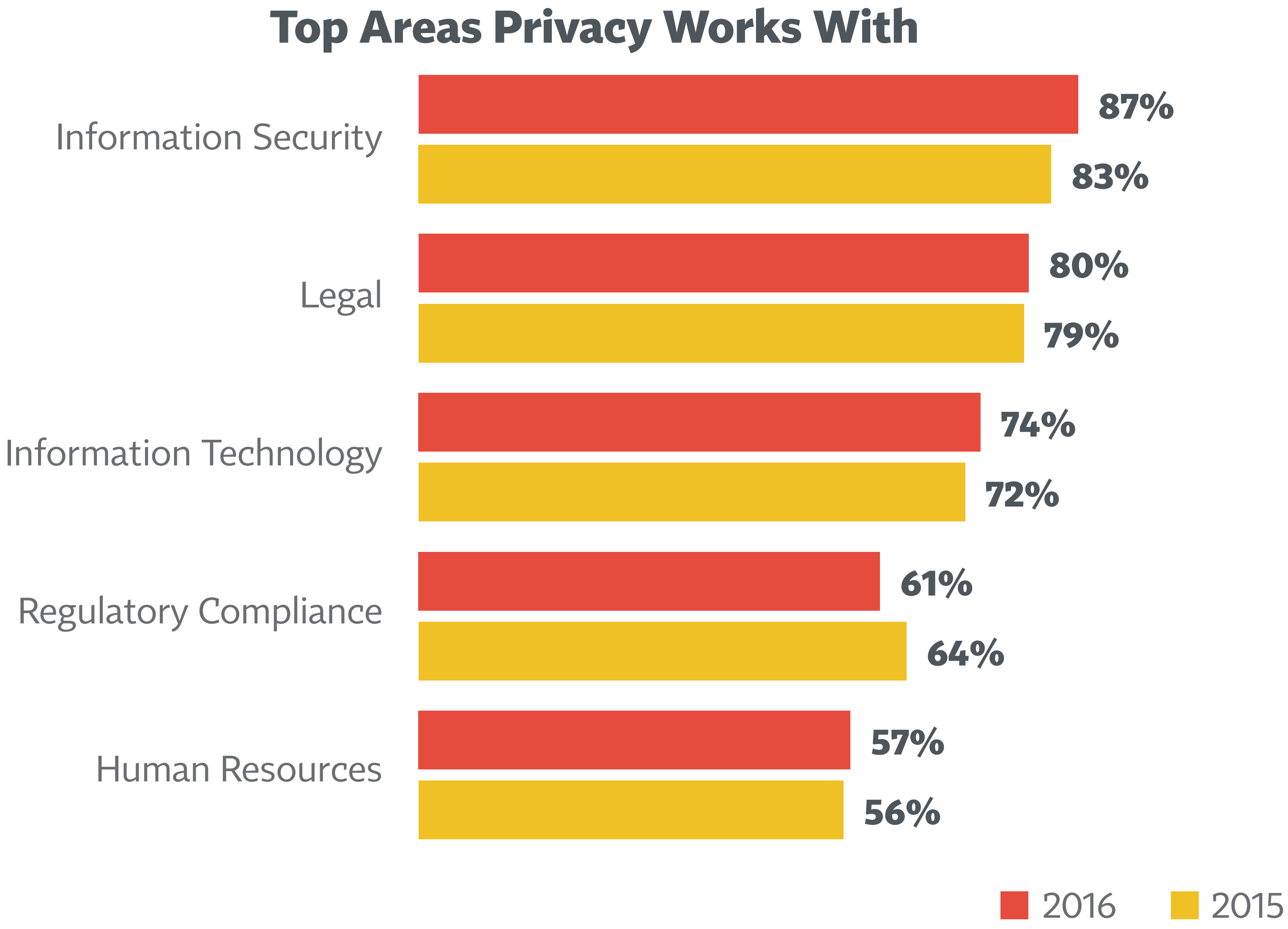
7 **Privacy Function in the Business Context**

8 Internal and External Resources

9 Thoughts About the Profession

10 Cross Border Data Transfer

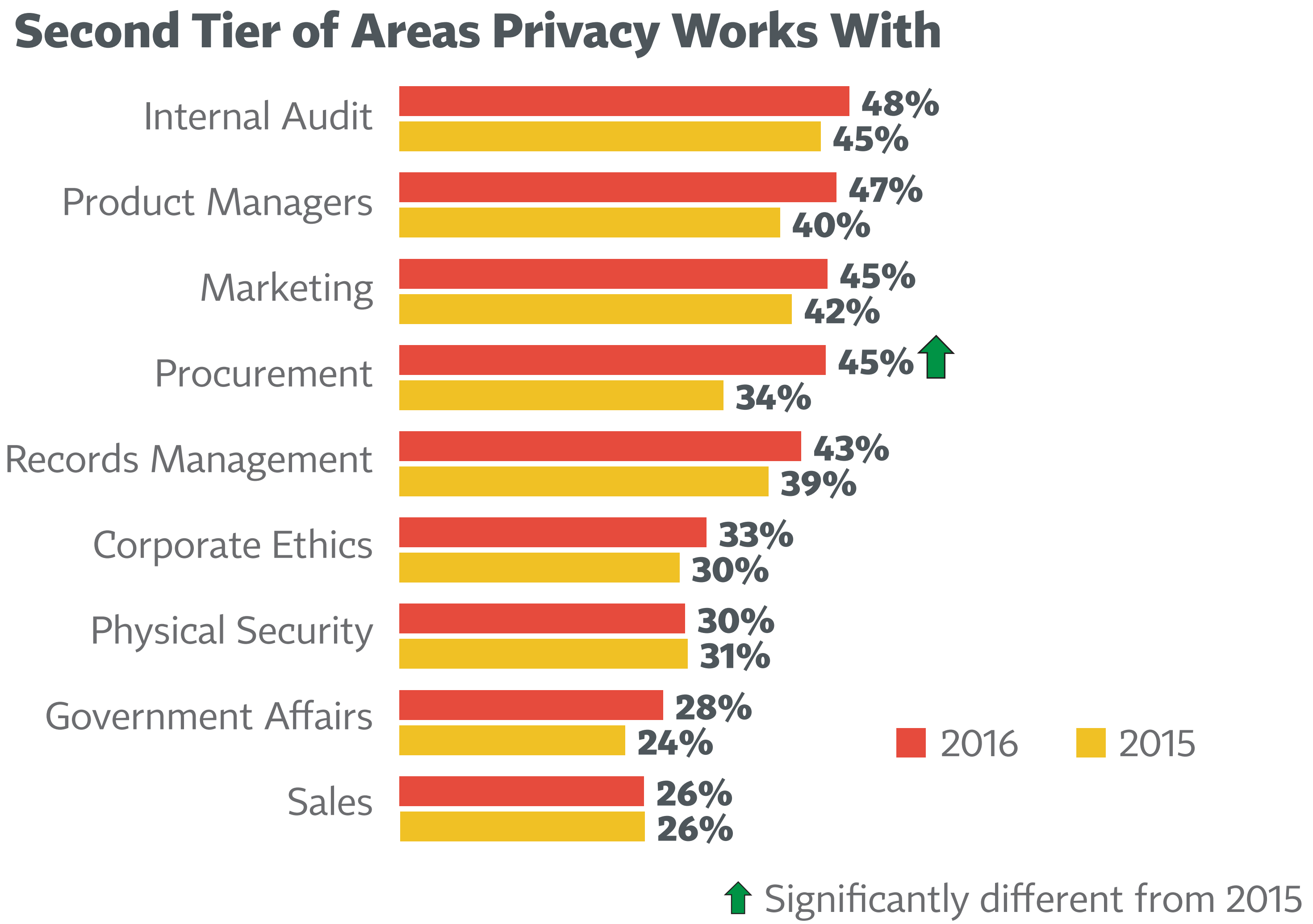
As was the case in 2015, IS, legal, and IT are the departments privacy teams are most likely to work with



G1: First, thinking about your day-to-day work, with which of the following functions do you interact on a regular basis?

Privacy is less likely to work with departments ranging from Internal Audit to Sales

- However, there's been a significant increase in privacy professionals saying they work regularly with procurement

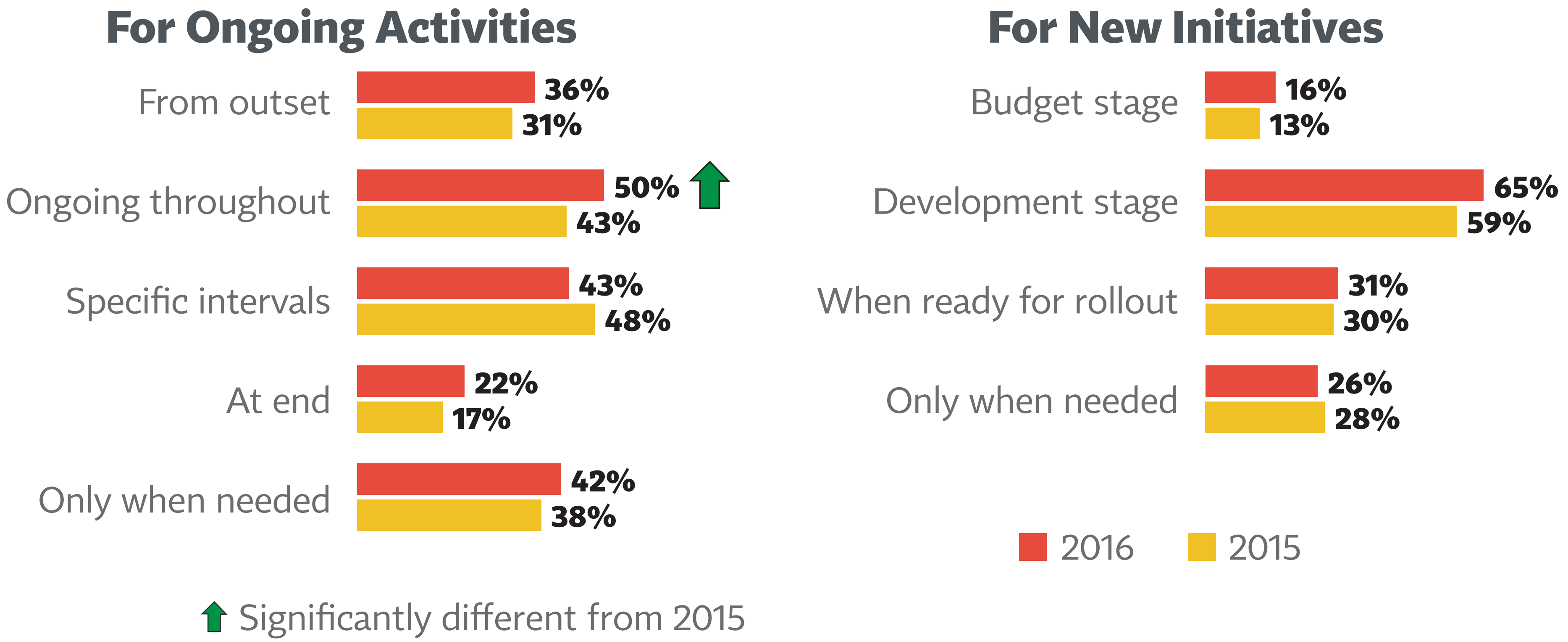


G1: First, thinking about your day-to-day work, with which of the following functions do you interact on a regular basis?

Privacy involvement in established activities is split between ongoing, at regular intervals, and ad hoc

- For new initiatives, privacy is most likely to be involved at the development stage—and that's even more the case than it was in 2015 (65% vs. 59%)

Privacy Involvement in Initiatives



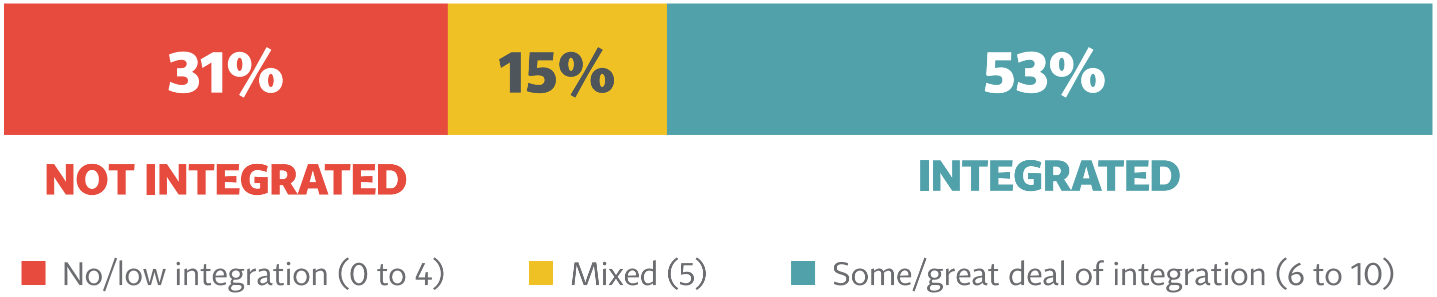
G5: In a general sense, for ongoing activities within your company that may involve privacy-related information, representatives of the privacy function are involved …

G6: Now thinking about new projects or initiatives established by your company that may involve privacy-related information, representatives of the privacy function are involved …

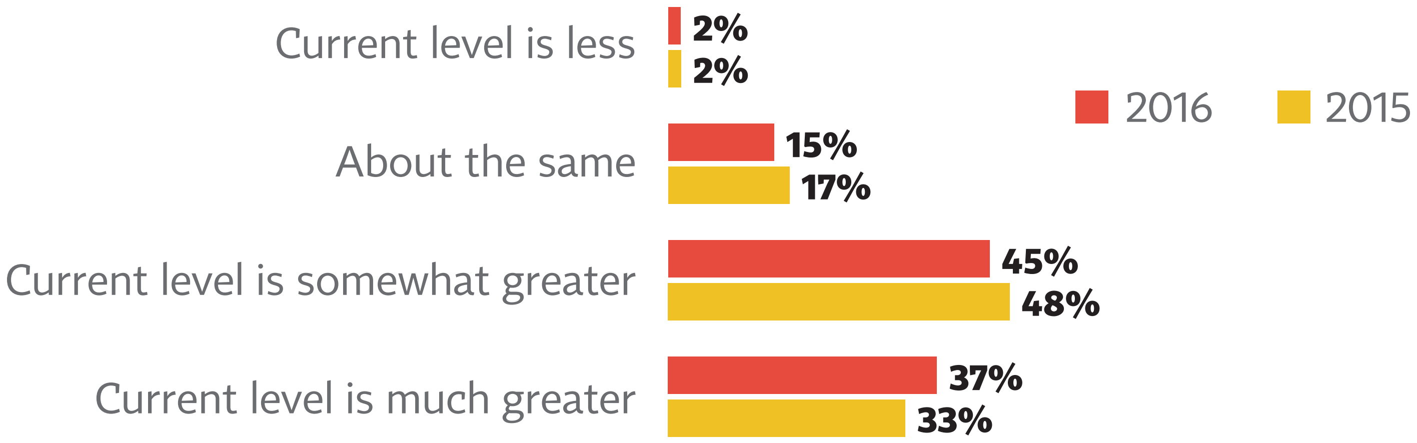
53% give a high rating to the level of integration privacy has in initiative planning and implementation

- That percentage has increased directionally from 2015 (49%), as has the percentage saying integration has been “much greater” than in the past (37%, vs. 33% in 2015)

Privacy Integration in Planning and Implementation



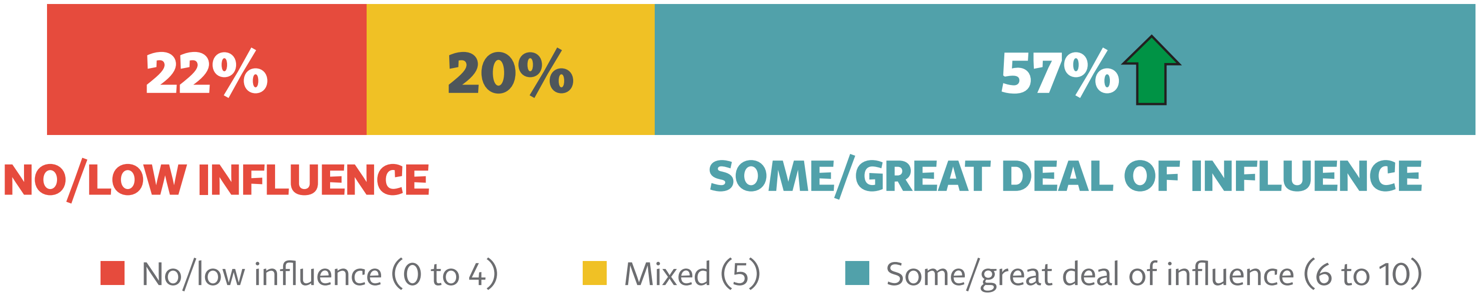
Current Integration Level vs. a Few Years Ago



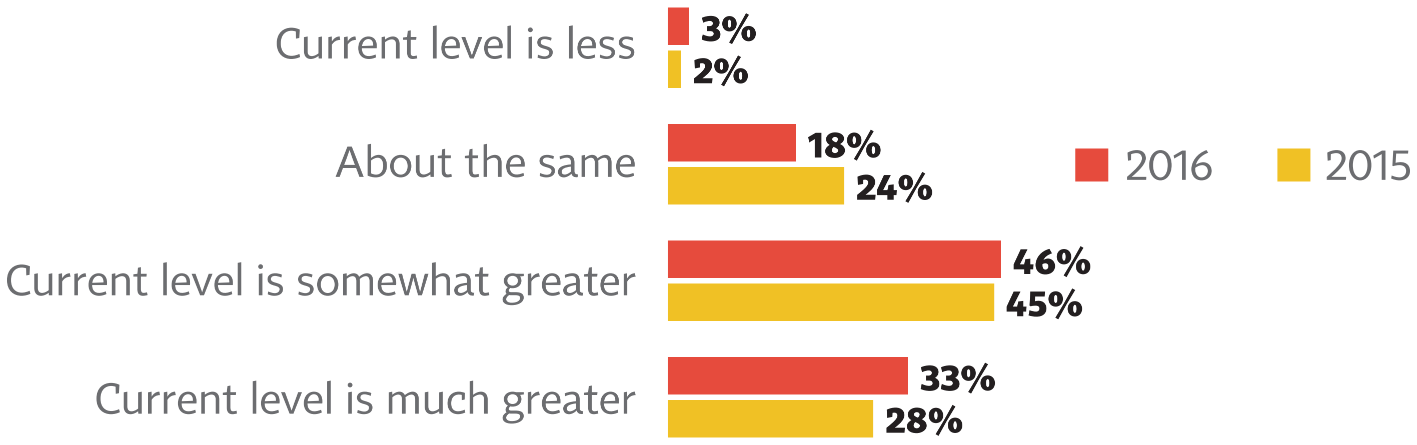
G7: To what extent would you say those in the privacy function of your company are integrated into the planning and implementation of initiatives that involve privacy-related information?
G8: This level of integration is …

The results are even stronger for privacy's influence on initiatives: 57% give a positive rating, up from 49%

Privacy Influence on Planning and Implementation



Current Influence Level vs. a Few Years Ago



⬆ Significantly different from 2015

G9: How would you describe the degree of influence those in the privacy function of your company have over planning and implementation of initiatives?
G10: This level of influence is ...

US privacy professionals are more likely than average to get involved with new initiatives at rollout

KEY SEGMENT DIFFERENCES

Privacy Group in Business Context: Segments with Higher Than Average Results

BY GEOGRAPHY

	US	EU
New initiatives: involved at rollout	35%	22%
Strong integration in planning and implementation	24%	24%

🟥 Significantly different than overall mean

As in 2015, mature privacy programs are likely to be involved, and influence, initiatives across the board

KEY SEGMENT DIFFERENCES

Privacy Group Responsibilities:
Segments with Higher Than Average Results

BY EMPLOYEE SIZE

	<5K	5–24.9K	25–74.9K	75K+
Ongoing activities: involved at specific intervals	34%	43%	47%	57%
Moderate integration in planning and implementation	42%	48%	51%	63%

BY PRIVACY LIFESTAGE

	Early	Middle	Mature
Ongoing initiatives: involved from outset	15%	24%	55%
New initiatives: involved at development stage	55%	63%	76%
Strong integration in planning and implementation	0%	16%	41%
Strong influence on planning and implementation	9%	16%	43%

■ Significantly different than overall mean

Contents

1 Executive Summary

2 Background and Method

3 How the Job of Privacy Is Done

4 Background on Companies and Individuals

5 Privacy Group Characteristics: Structure

6 Privacy Group Characteristics: Responsibilities

7 Privacy Function in the Business Context

8 Internal and External Resources

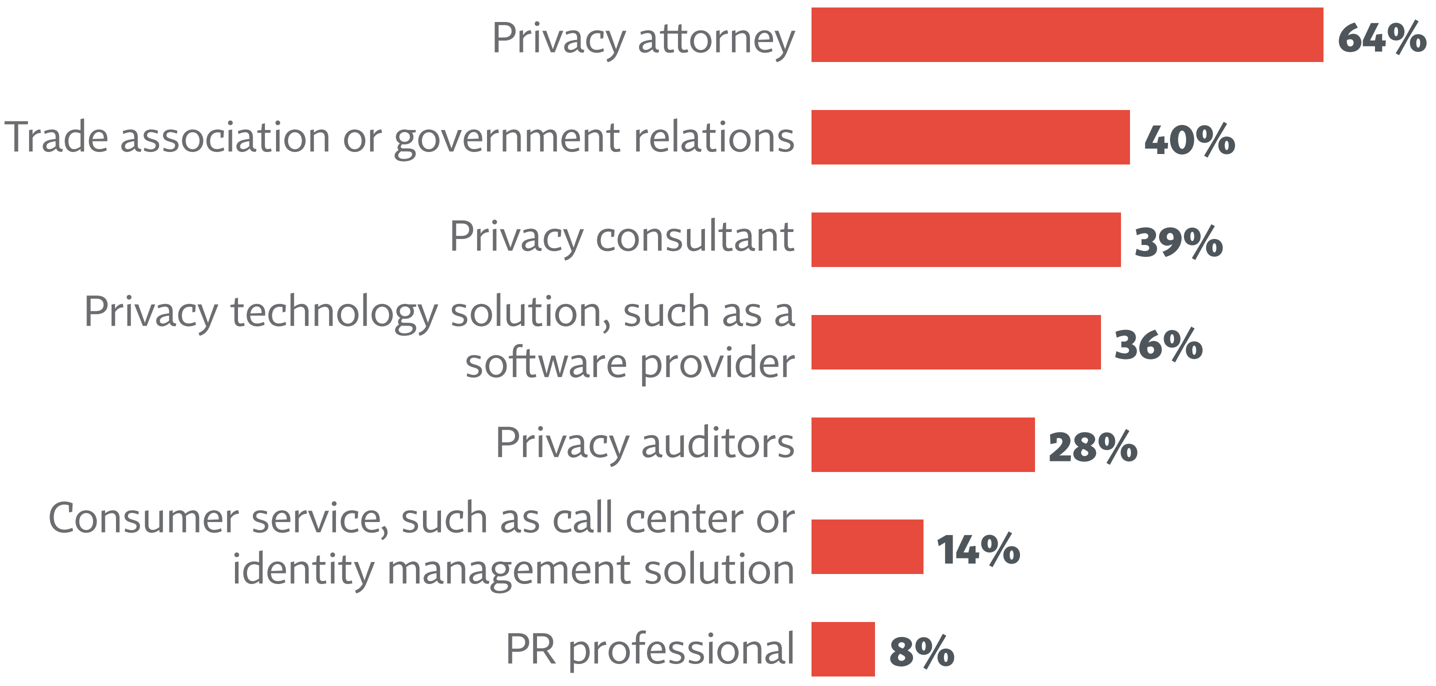
9 Thoughts About the Profession

10 Cross Border Data Transfer

Outside privacy attorneys continue to be the most often used external service

- Forming a next tier: trade associations/government relations, privacy consultants, and privacy technology solutions

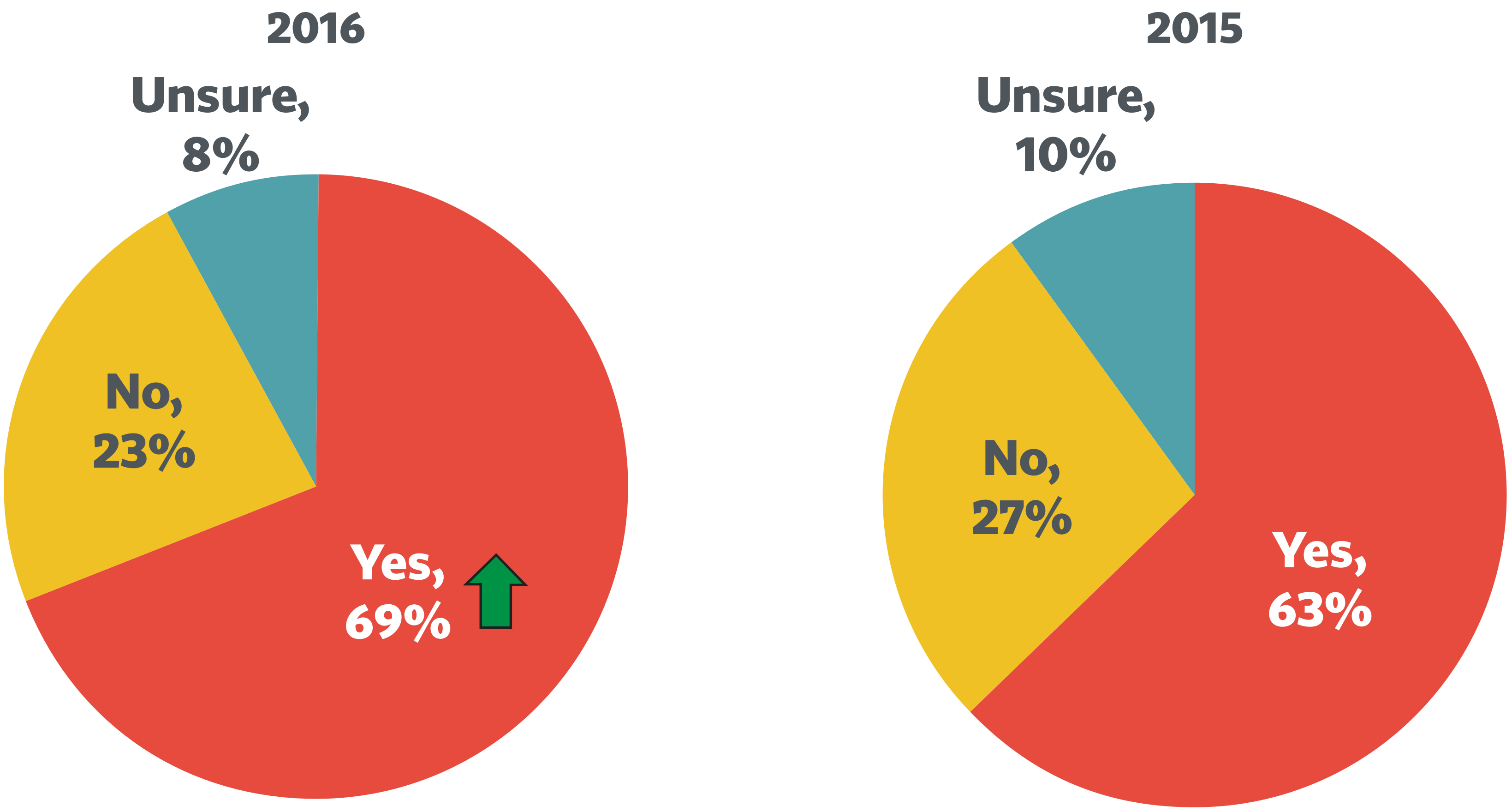
External Services Used in Past Year



H1: Which of the following external privacy services have you worked with directly within the past year?

Close to 7 in 10 privacy pros use internal audits, up from 63% in 2015

Use of Internal Audit



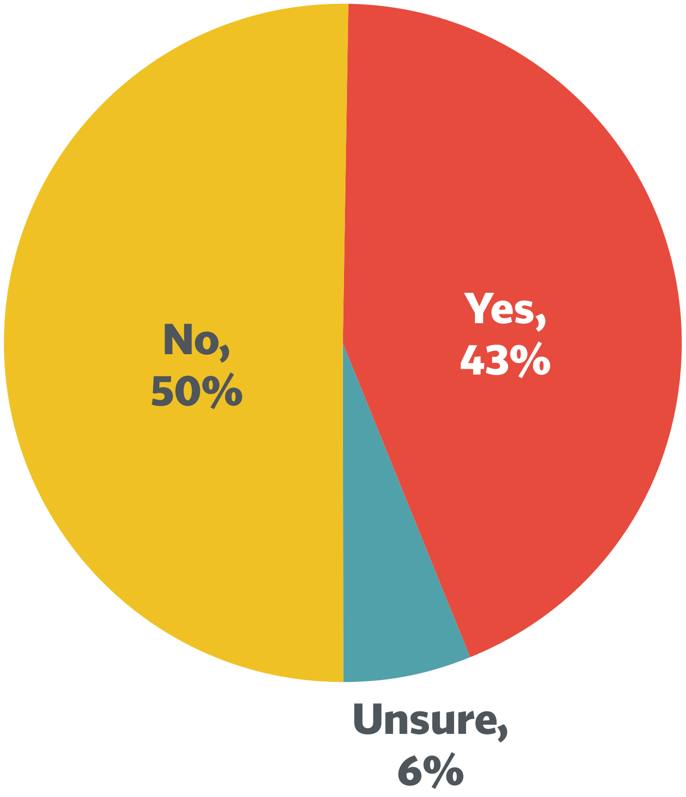
⬆ Significantly different from 2015

H2: Does your company use internal audit for privacy audits?

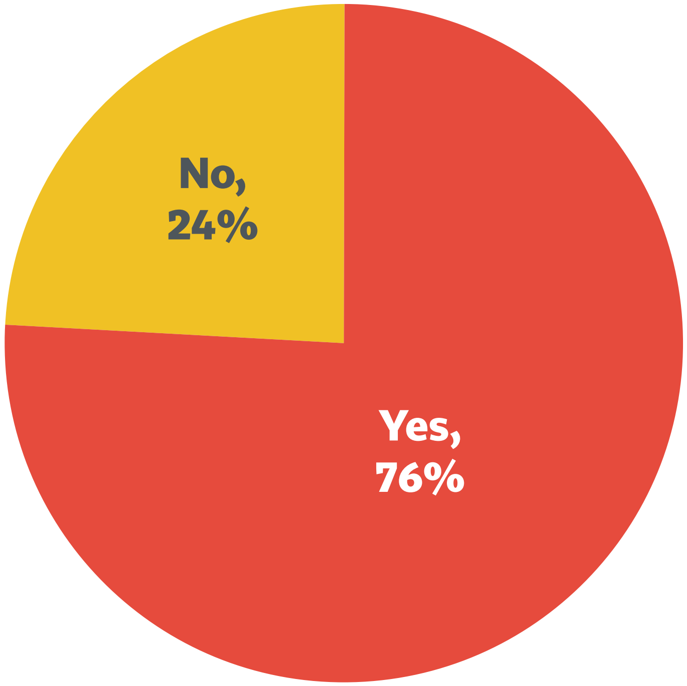
Over 4 in 10 use privacy working groups, similar to the proportion in 2015

- As was also the case in 2015, most survey respondents say they themselves are part of the working group

Have Privacy Working Group



Respondent Part of Working Group?



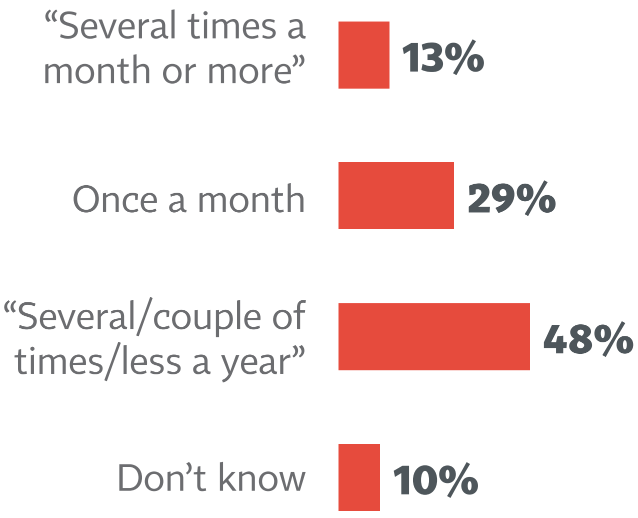
H3: Does your organization have a committee of executives ("privacy working group") from a cross section of departments that regularly oversees the privacy office's activities?
H4: Are you part of the privacy working group?

‘Several times a year’ continues to be the most common meeting frequency for working groups

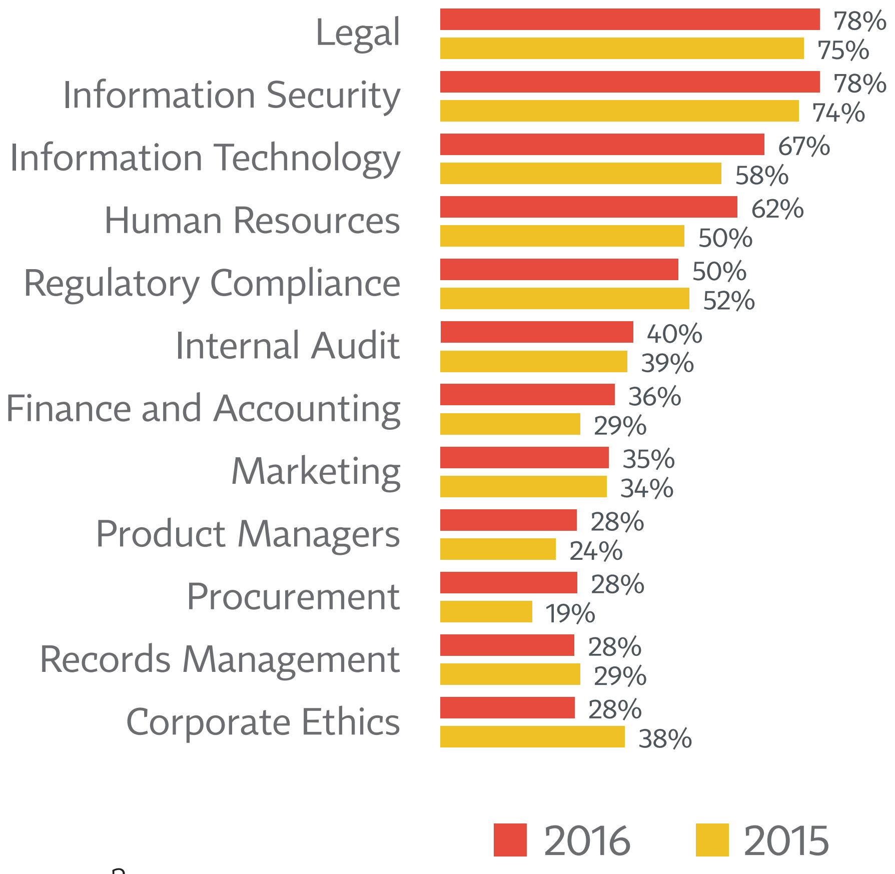
- While legal, IS, and IT are still the most common participants, HR and procurement are more likely to be part of the working groups than was the case a year ago

Among Those With Privacy Working Group

How Often Meet



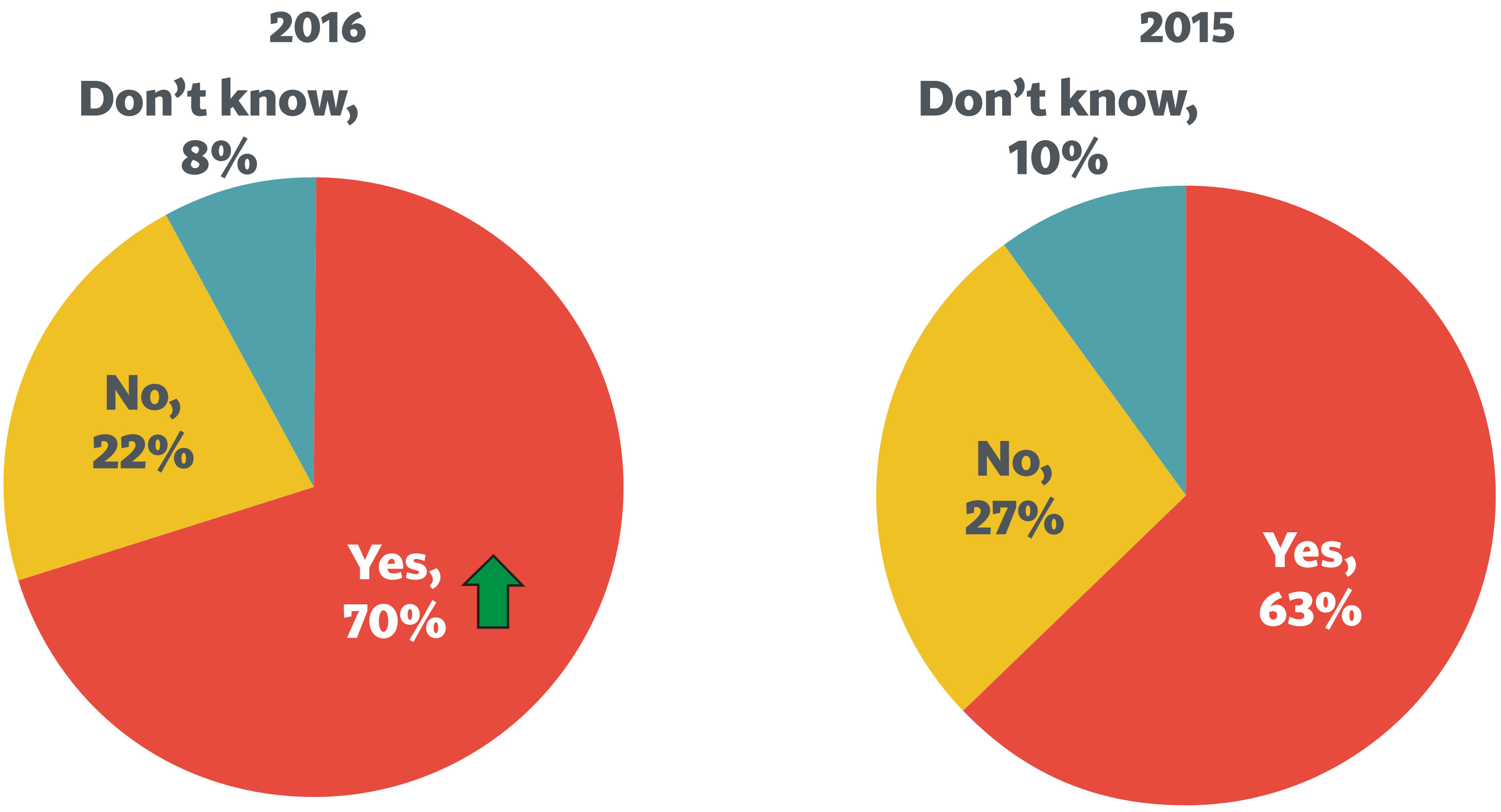
Common Representatives



H5: How often does this working group meet?
H6: What departments are represented as part of the privacy working group?

We also see a significant uptick in the proportion with a vendor management program

Have Vendor Management Program



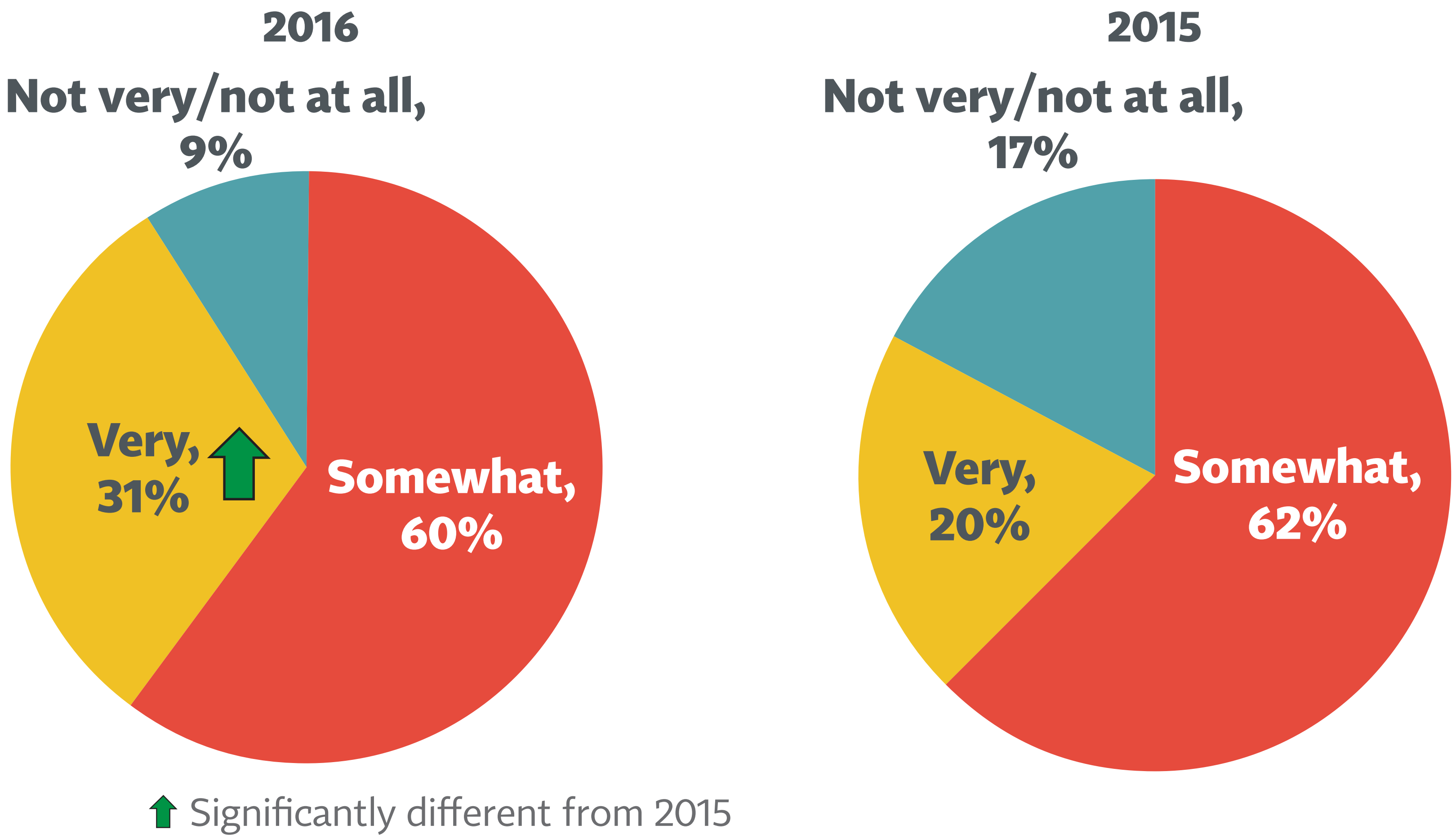
⬆ Significantly different from 2015

H7: Does your company have a vendor management program designed to ensure the privacy and/or security practices of vendors will not threaten the integrity of your company’s privacy standards?

And there's been an 11-point increase in the proportion calling their program "very thorough"

Thoroughness of Vendor Management Program

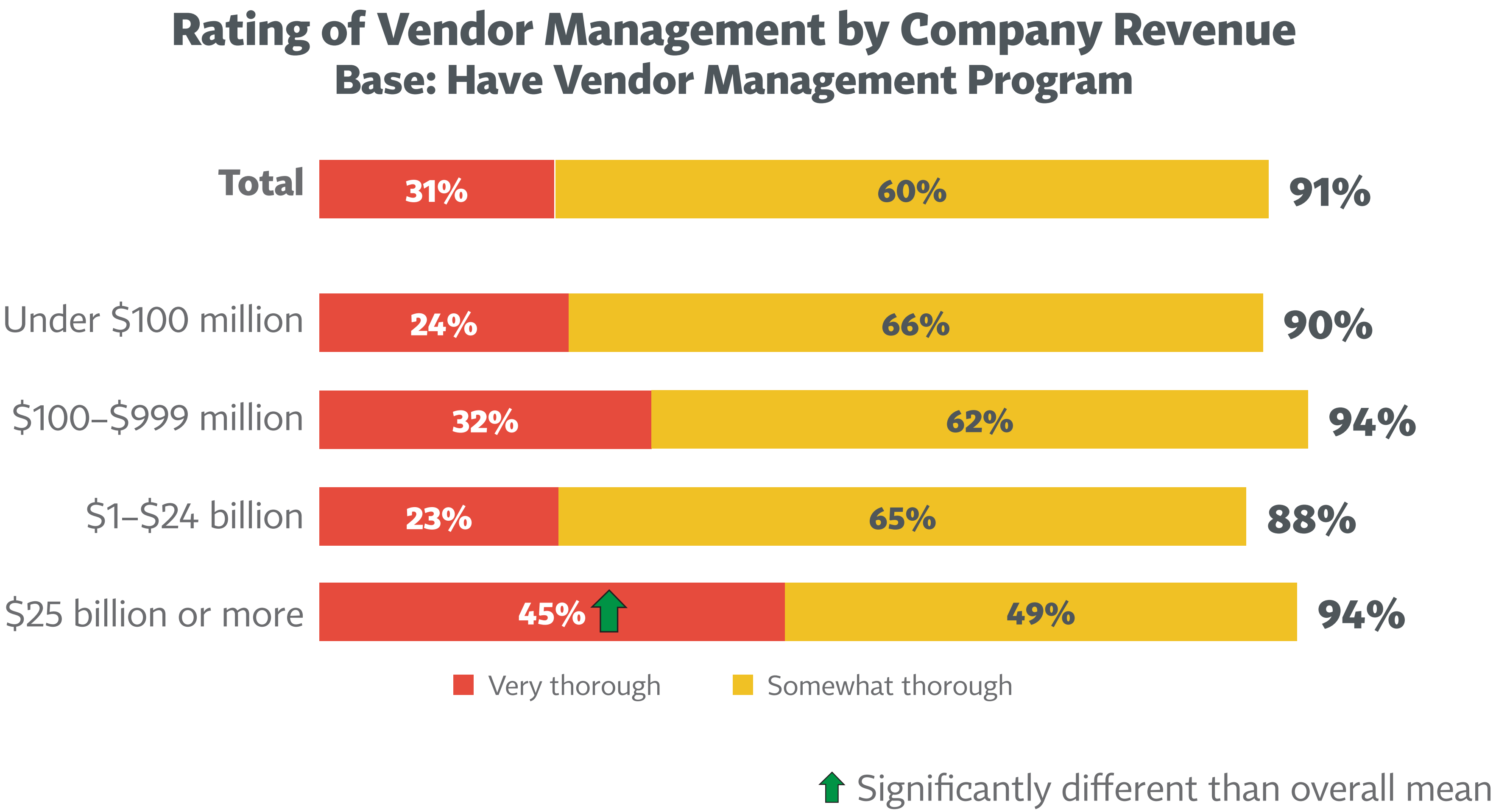
Base: Have Vendor Management Program



H7a: Does your organization's vendor management program include contract management functions?
H8: How would you describe this vendor management program?
H9: Does your vendor management program include on-site audits by your company's internal resources?

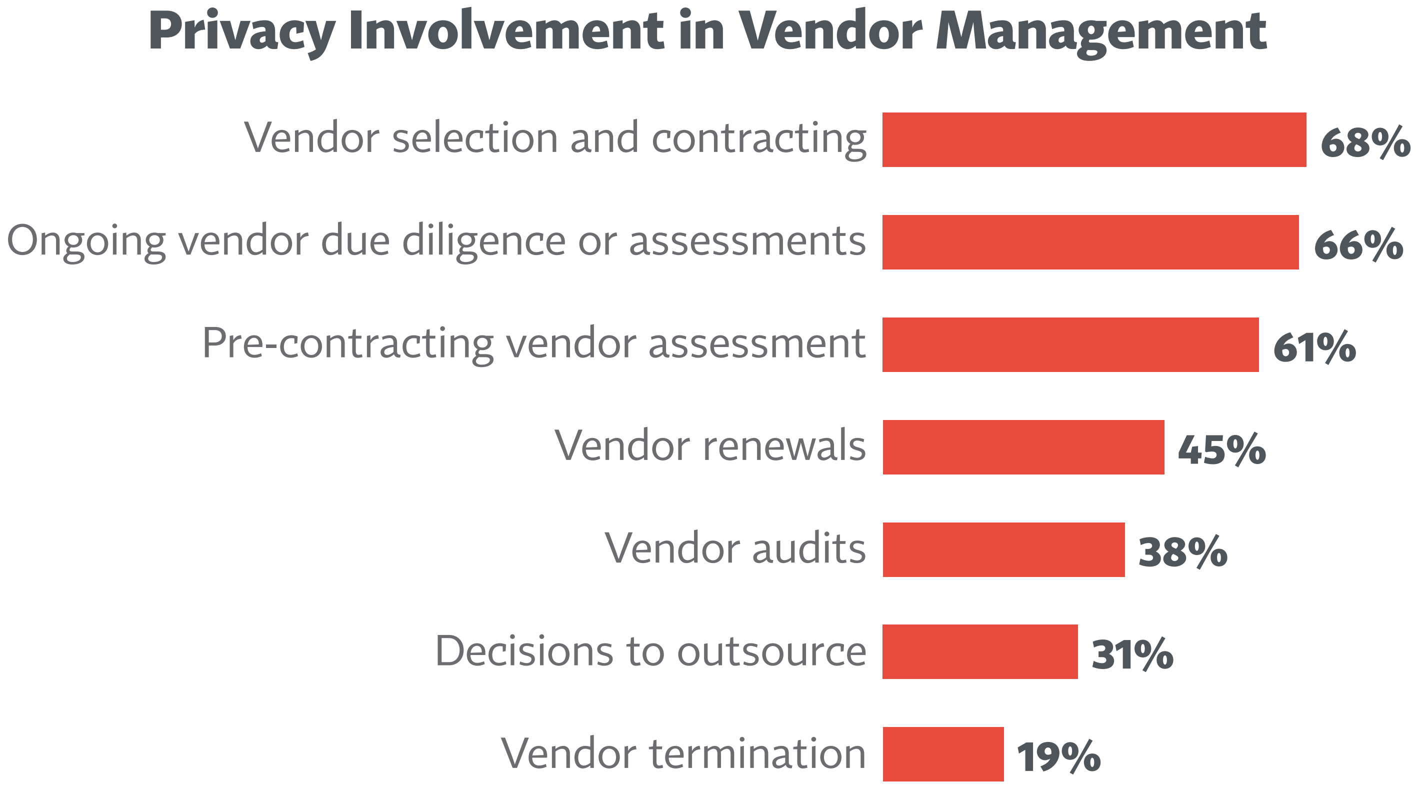
The largest companies, based on revenue, are much more likely to call vendor management 'very thorough'

KEY SEGMENT DIFFERENCES



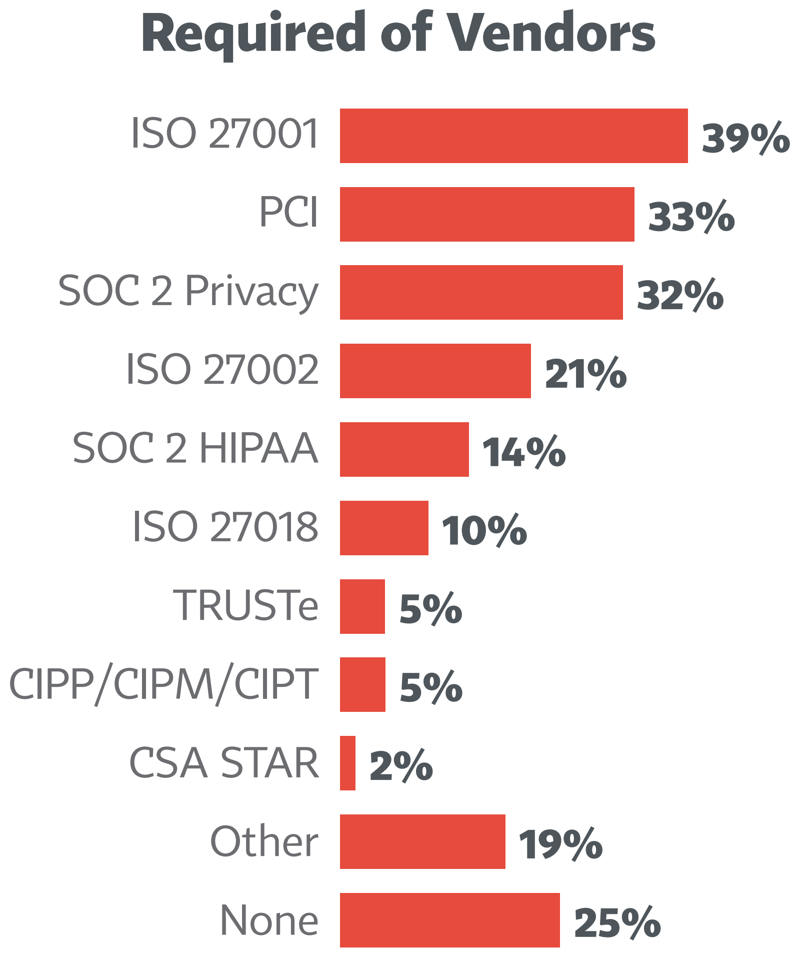
H7a: Does your organization's vendor management program include contract management functions?
H8: How would you describe this vendor management program?
H9: Does your vendor management program include on-site audits by your company's internal resources?

Privacy is most often involved with contracting, due diligence, and assessments



H7d: Which stages of the vendor management lifecycle is the privacy function involved in?

The most common requirements for vendors are ISO 27001, PCI, and SOC 2 privacy certifications

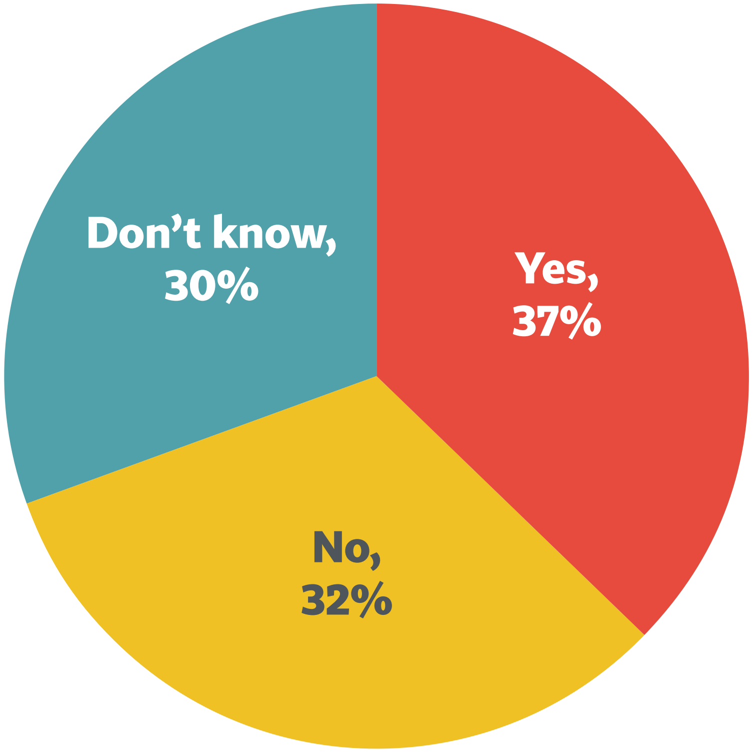


H7g: Which, if any, third party audits or certifications does your organization require from vendors?

Privacy professionals are split on whether they have self-renewing vendor contracts

- That includes nearly a third who don't know

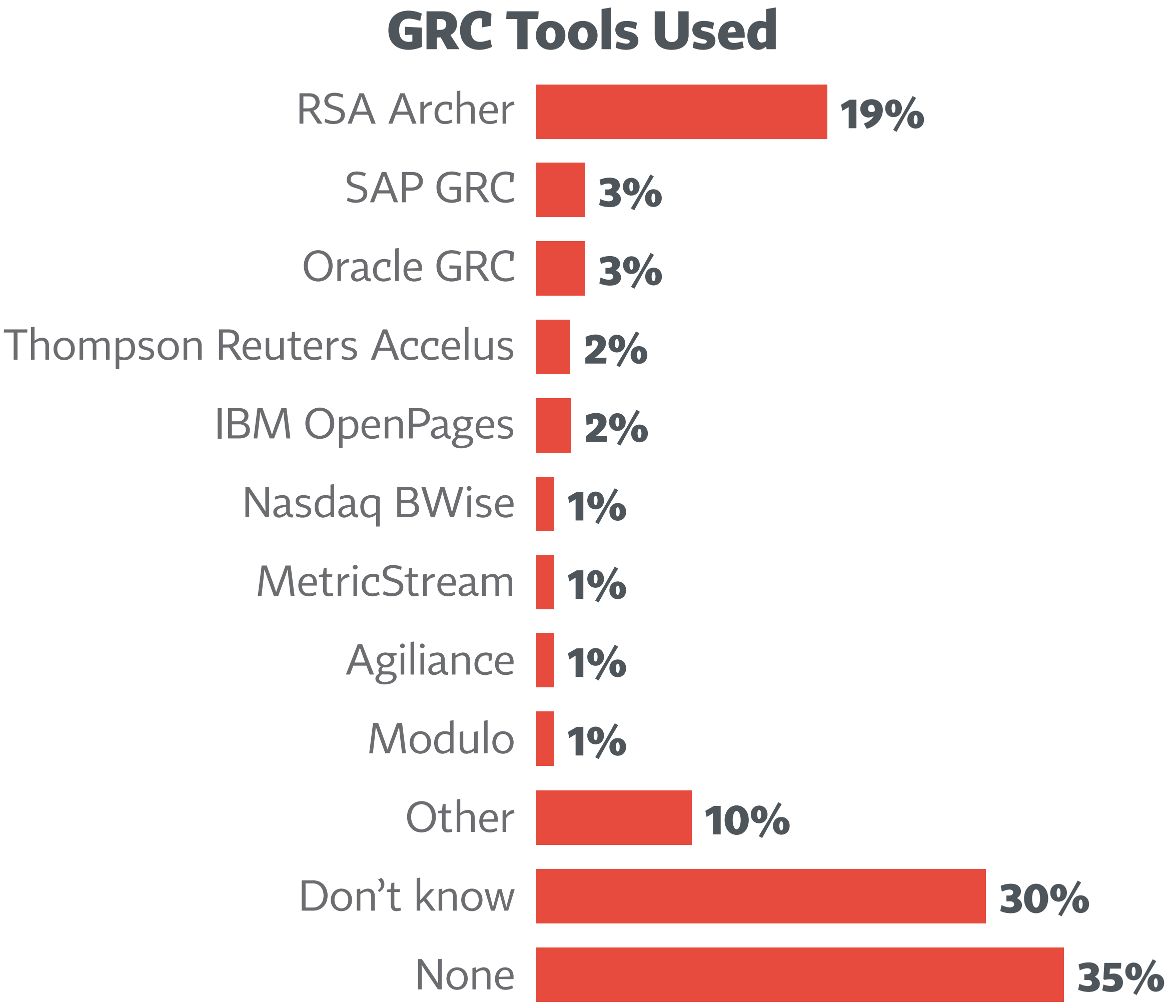
Have Self-Renewing Vendor Contracts
Base: Have Vendor Management Program



H7h: Does your organization have self-renewing or "evergreen" contracts with vendors that handle personal information on your behalf?

GRC tools are also a bit of a mystery to privacy pros: 35% say they don't use them and 30% aren't sure

- Among those who do use them, RSA Archer is the most commonly mentioned by far

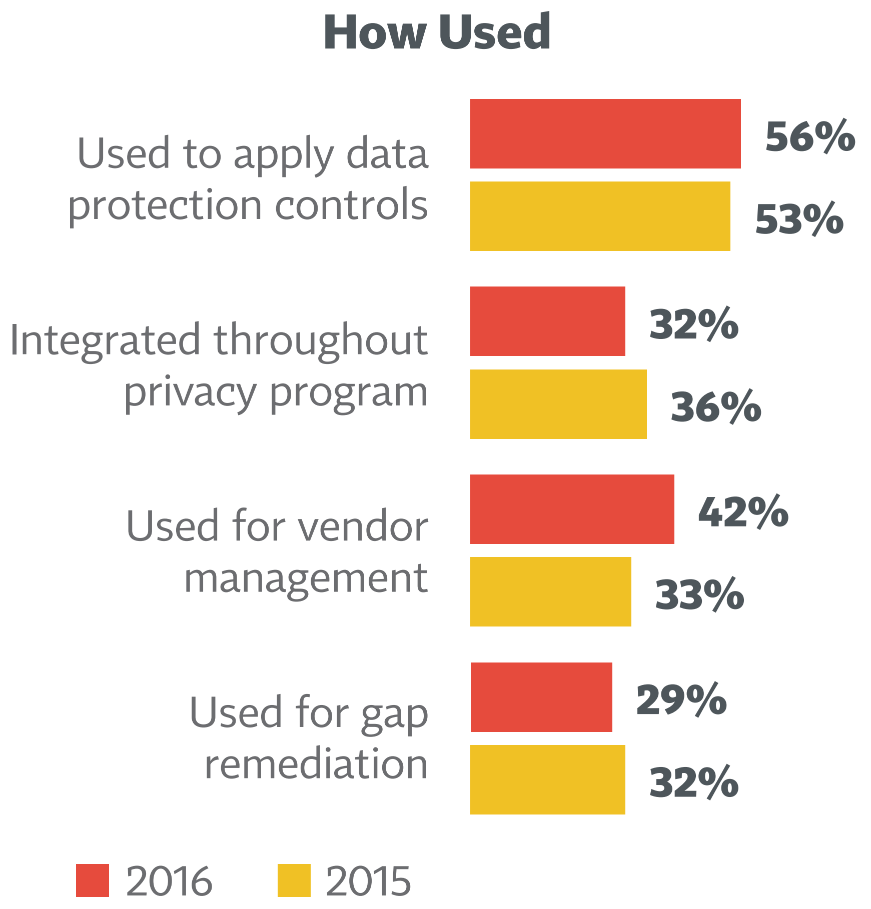


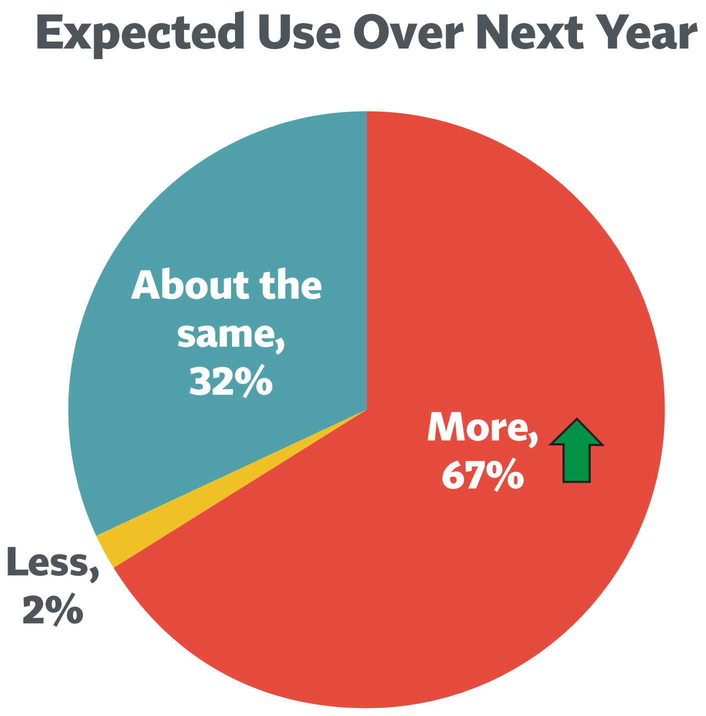
H13: Please select which, if any, of the following governance risk and compliance (GRC) tools your company uses on a regular basis.

At the same time, two-thirds of those using GRC tools expect to use them more next year

- That's double the proportion who said that in 2015

Among Those Using GRC Tools



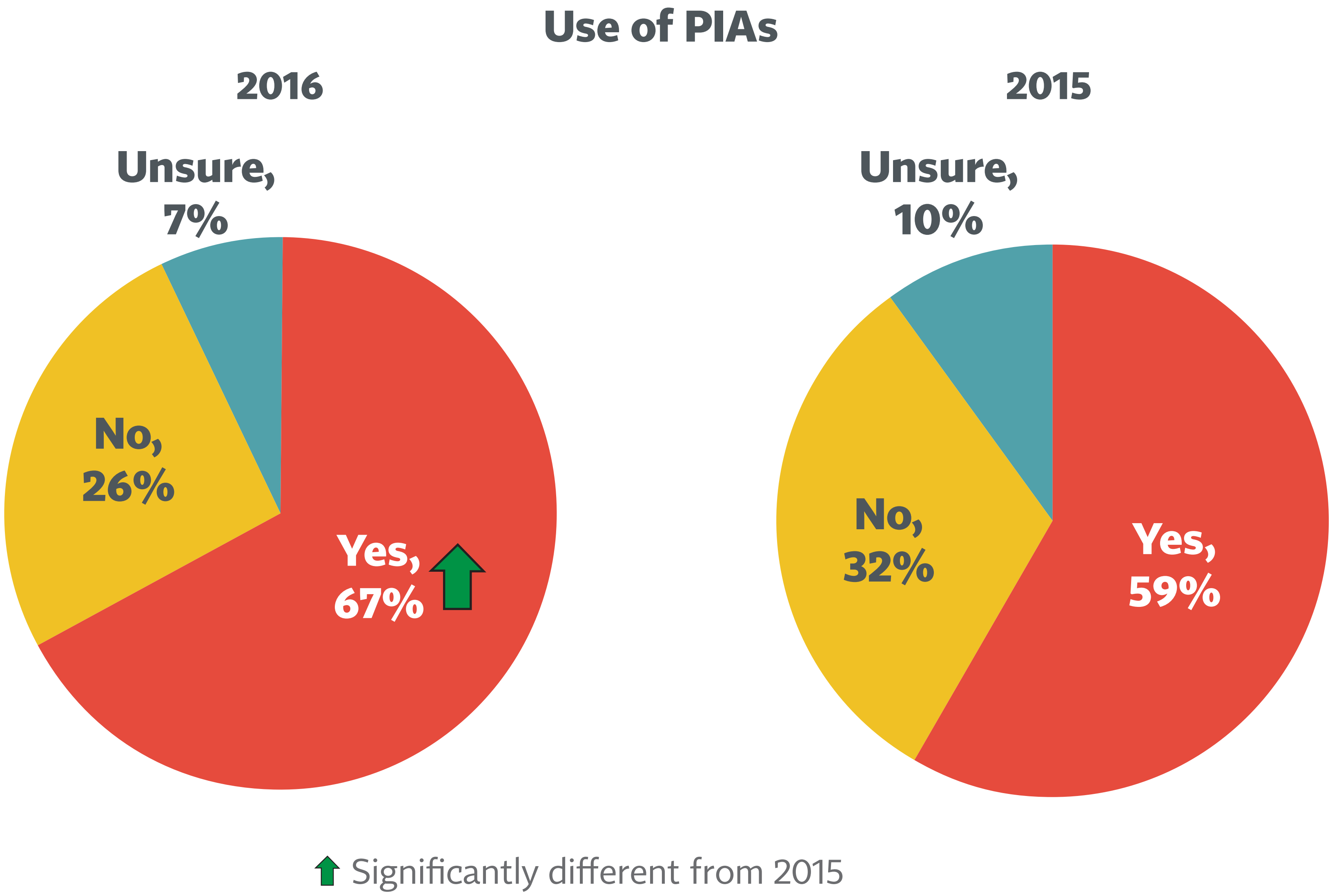


⬆ Significantly different from 2015

H14: Your company's GRC tools are…

H15: Over the course of the next year, you expect privacy-related activities to be integrated into a GRC tool …

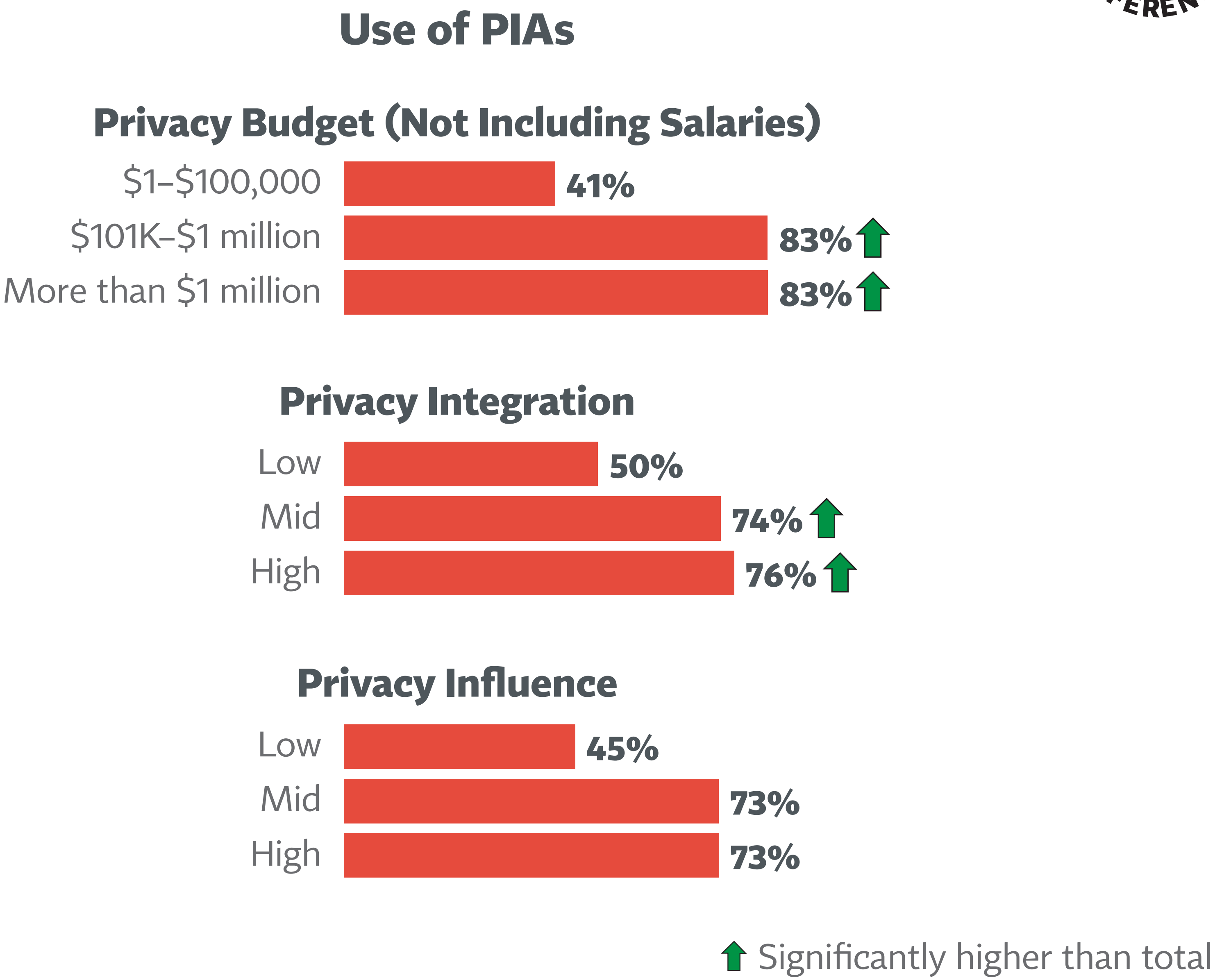
We see a significant increase in the use of Privacy Impact Assessments



H16: Does your company use Privacy Impact Assessments (PIAs)?

PIAs are also common in firms with larger privacy budgets, and in firms with strong privacy integration

KEY SEGMENT DIFFERENCES



H16: Does your company use Privacy Impact Assessments (PIAs)?

By industry, the most notable finding is the robustness of financial firms' resource use

KEY SEGMENT DIFFERENCES

Internal and External Resources:
Segments with Higher Than Average Results

BY GEOGRAPHY

	US	EU
No privacy working groups	51%	38%
Vendor management program	**74%**	62%
Privacy Impact Assessments	63%	70%
Stages of vendor management cycle privacy is involved in		
Decisions to outsource	29%	27%
Vendor selection and contracting	66%	**80%**

BY INDUSTRY

	Gov't	Finance	Health	Tech
Internal audit	61%	**80%**	70%	71%
Vendor management program	46%	**83%**	64%	**82%**
GRC tools	18%	**51%**	37%	39%

🟥 Significantly different than overall mean

As you’d expect, resources are most available to the largest firms and the most mature privacy programs

KEY SEGMENT DIFFERENCES

Internal and External Resources:
Segments with Higher Than Average Results

BY EMPLOYEE SIZE

	<5K	5–24.9K	25–74.9K	75K+
Internal audit	64%	61%	▨ 78%	▨ 83%
Privacy working group	32%	41%	49%	▨ 66%
Vendor management program	60%	69%	▨ 77%	▨ 81%
GRC tools	21%	32%	48%	▨ 54%
Privacy Impact Assessment	61%	68%	66%	▨ 77%

BY PRIVACY LIFESTAGE

	Early	Middle	Mature
Internal audit	39%	75%	▨ 86%
Privacy working group	25%	35%	▨ 51%
Vendor management program	62%	76%	▨ 89%
Stages of vendor management cycle privacy is involved in			
Decisions to outsource	19%	25%	▨ 46%

▨ Significantly different than overall mean

Contents

1 Executive Summary

2 Background and Method

3 How the Job of Privacy Is Done

4 Background on Companies and Individuals

5 Privacy Group Characteristics: Structure

6 Privacy Group Characteristics: Responsibilities

7 Privacy Function in the Business Context

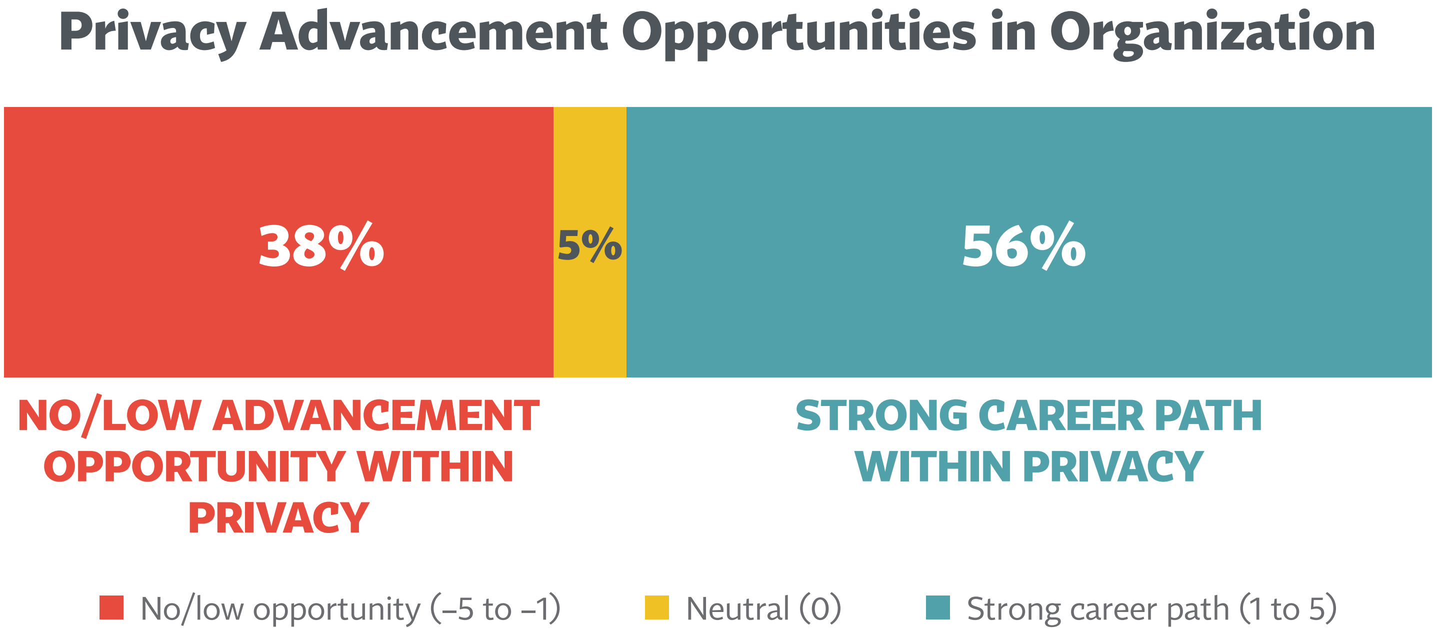
8 Internal and External Resources

9 **Thoughts About the Profession**

10 Cross Border Data Transfer

2016 sees a directional increase in the proportion saying privacy is a strong career track in their group

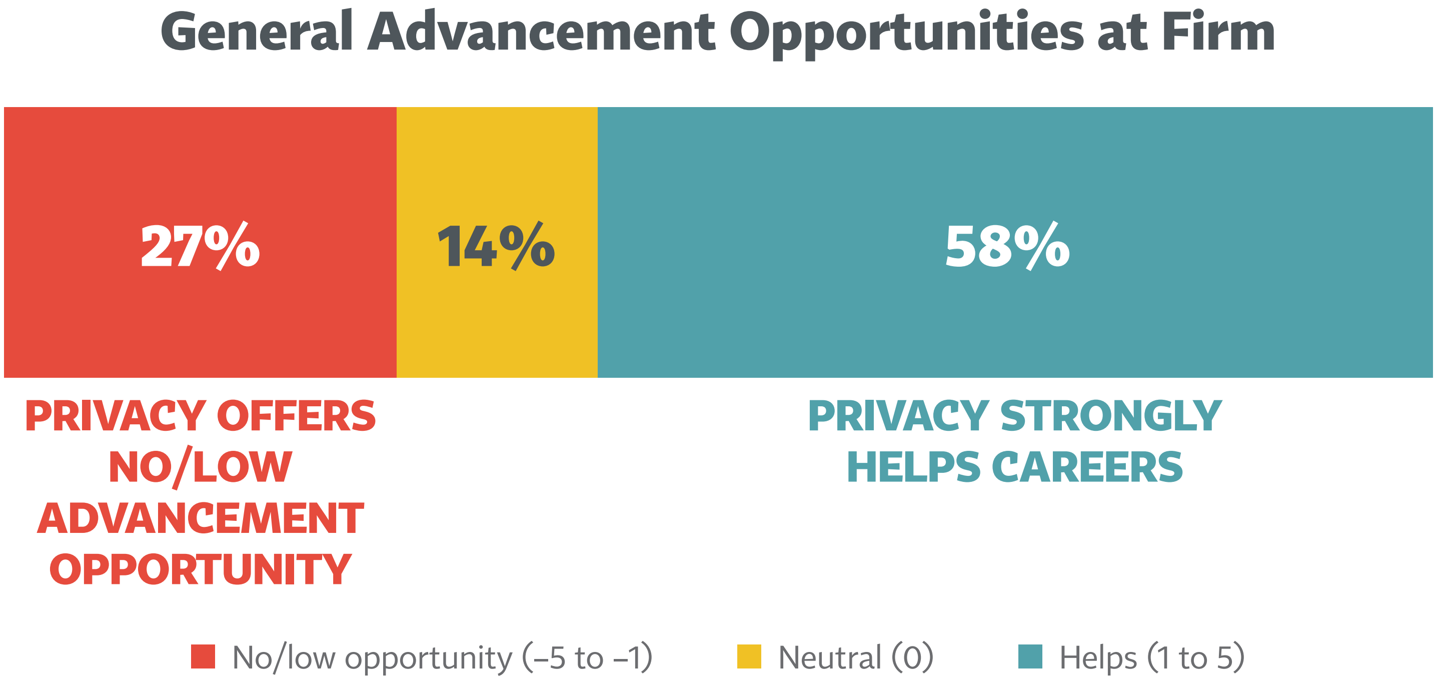
- 56% give a positive assessment, up from 48% in 2015



E9: Please use the slider below to indicate the extent to which you view privacy as a career track at your organization.

There's also been an increase in the proportion saying privacy offers opportunities at their firm generally

- 58% give a positive rating, up directionally from 52% in 2015

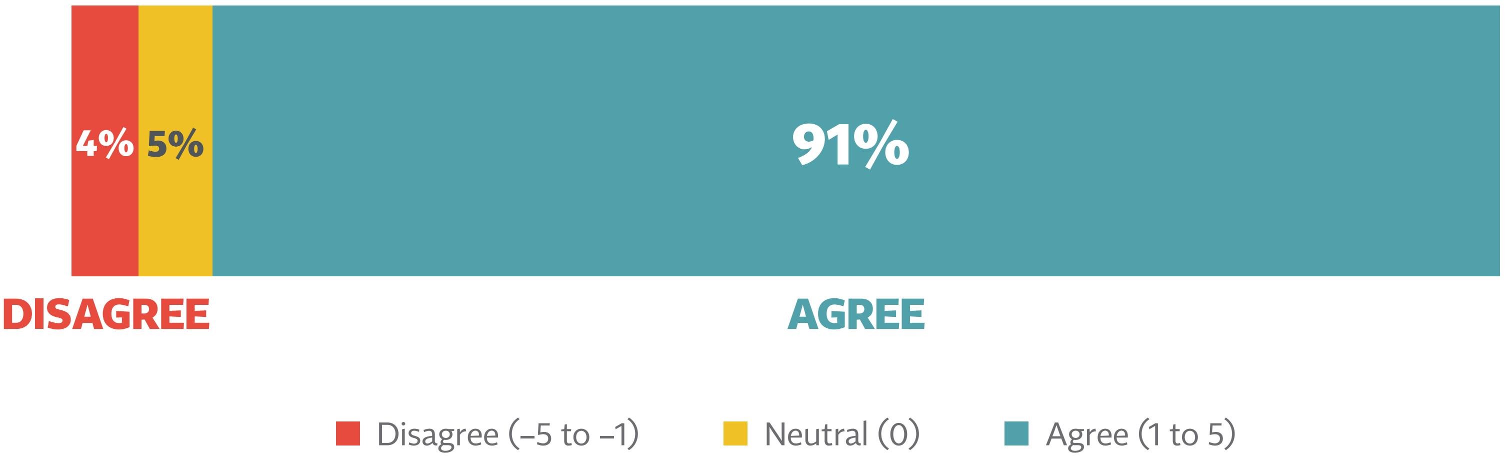


E10: Again, please use the slider below to indicate the extent to which privacy roles can advance careers at your company in general (that is, not necessarily within the privacy program).

Finally, nearly all say that privacy opens doors for opportunities in the marketplace generally

- 91% feel that way, also up directionally from 2015

Privacy Helps Open Career Doors?



E11: Please indicate the degree to which you agree or disagree with the following statement: Doing well in privacy will open doors for better and better job opportunities in the marketplace.

Contents

1 Executive Summary

2 Background and Method

3 How the Job of Privacy Is Done

4 Background on Companies and Individuals

5 Privacy Group Characteristics: Structure

6 Privacy Group Characteristics: Responsibilities

7 Privacy Function in the Business Context

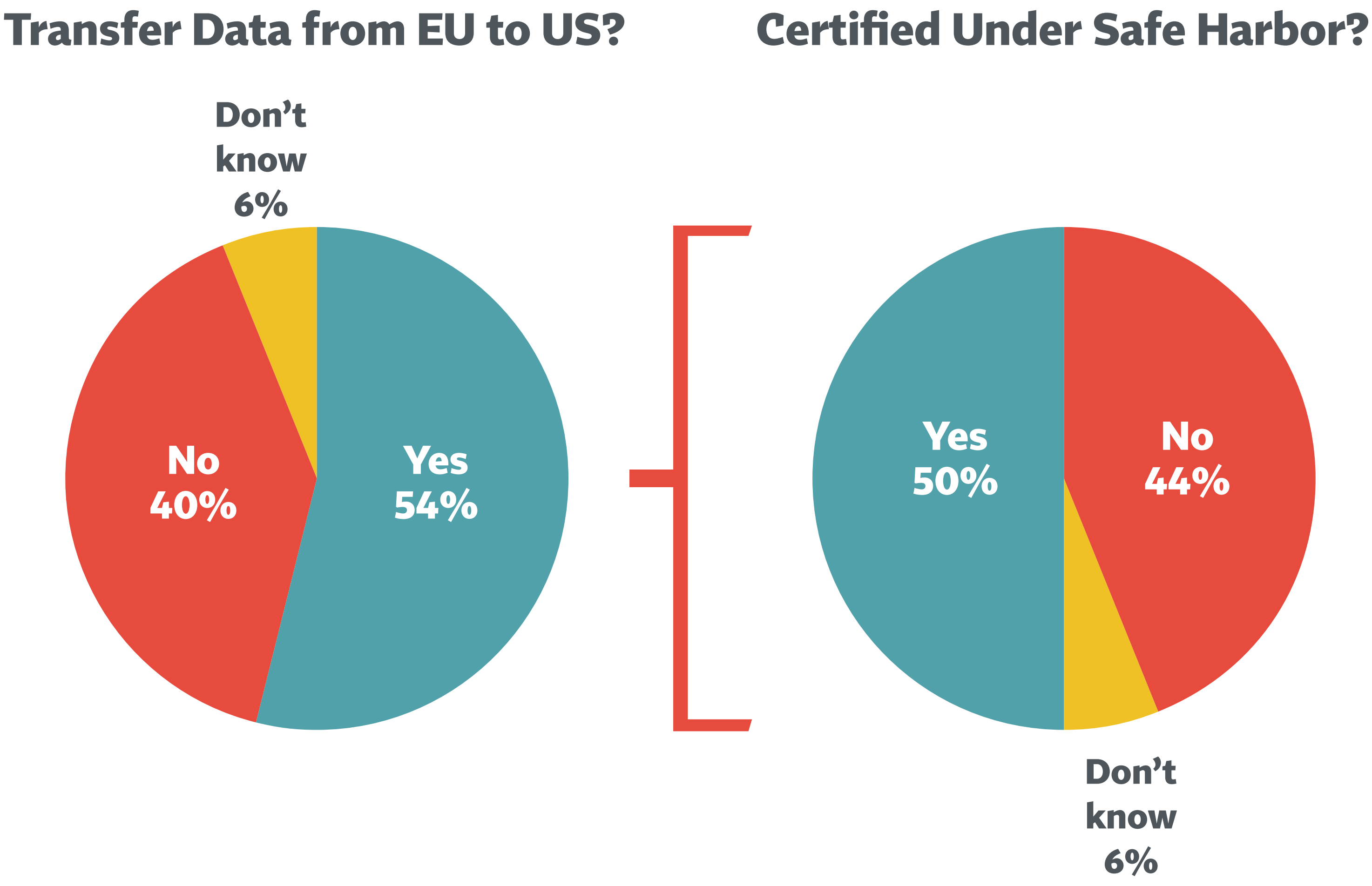
8 Internal and External Resources

9 Thoughts About the Profession

10 **Cross Border Data Transfer**

More than half of the organizations surveyed transfer data between the EU and the US

- In addition, half of those transferring certified under Safe Harbor in the past

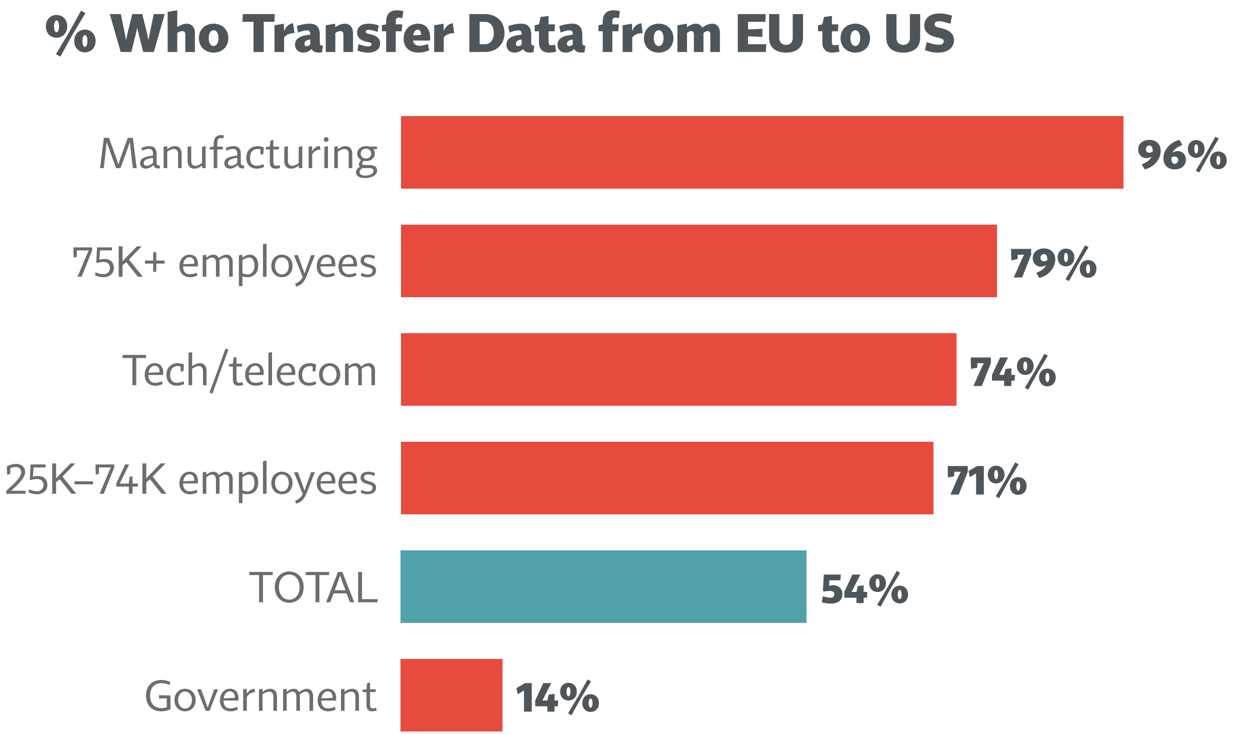


J1: Does your organization transfer personal information from the European Union to the United States?
J2: Did your company certify under Safe Harbor?

Manufacturing and tech firms are significantly more likely than average to transfer data across borders

- In addition, cross-border transfer is the norm for organizations with 25K employees or more

KEY SEGMENT DIFFERENCES



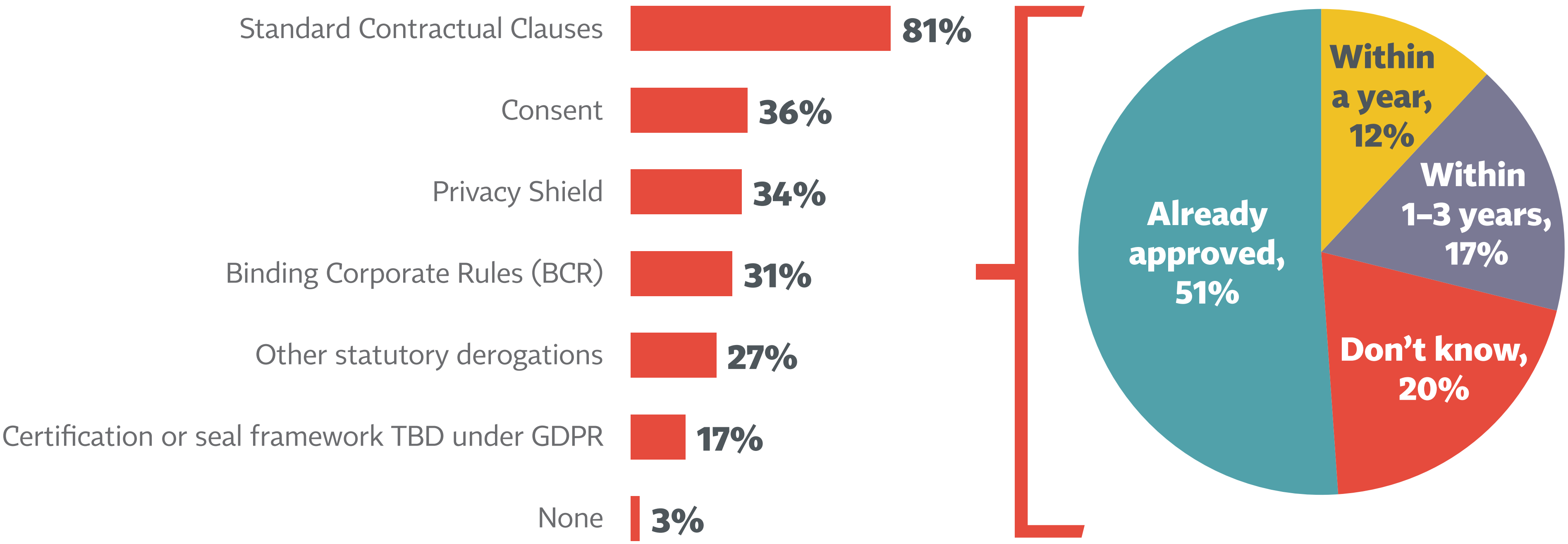
J1: Does your organization transfer personal information from the European Union to the United States?

The vast majority of those transferring data rely on standard contractual clauses as the main mechanism

- However, about one-third rely, or intend to rely, on Privacy Shield or BCR (including 55% for BCR among those with 75K employees or more). And half of those say their BCR application has already been approved

Mechanism for Data Transfer, Among Those Who Transfer

Expected BCR Approval

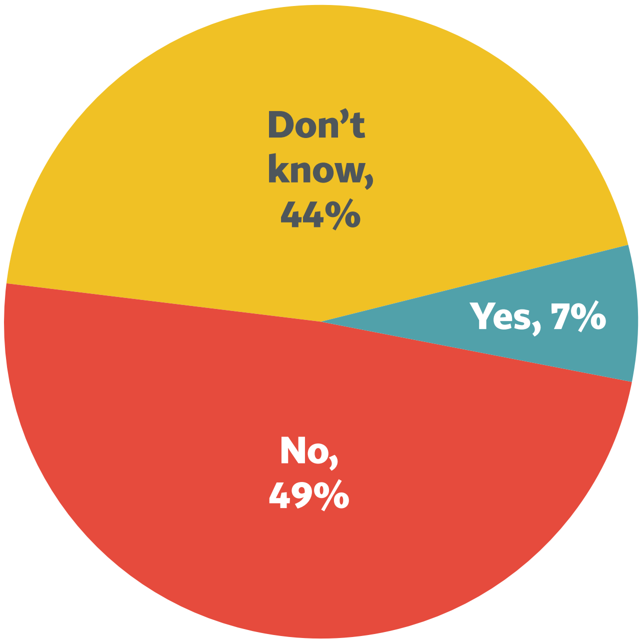


J5: What mechanism(s) does your company intend to use to transmit data to the U.S.?
J6: When do you expect your BCR application to be approved?

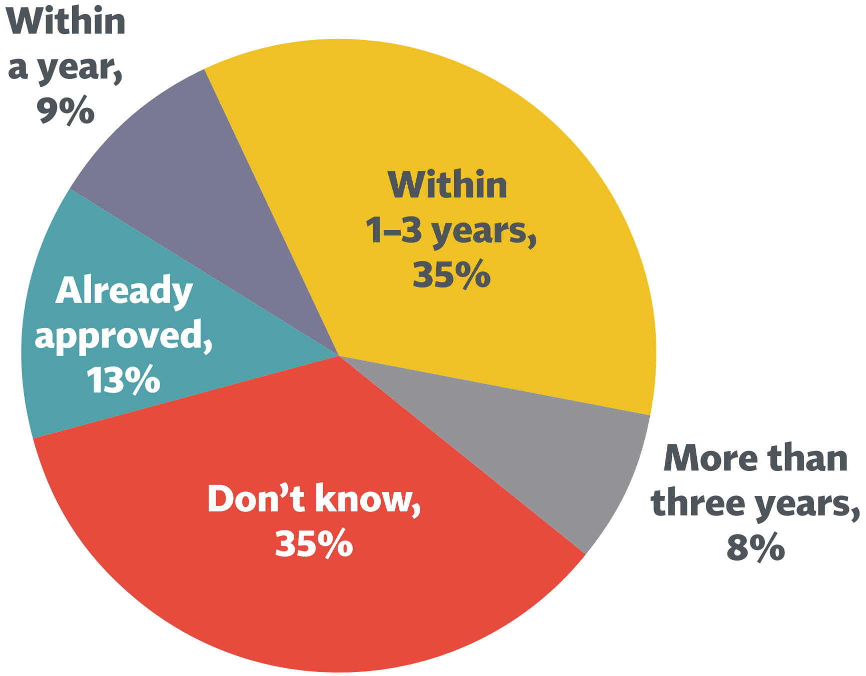
Very few organizations have definitive plans to apply for CBPR in the Asia Pacific region

- Among the few who do intend to apply, most don’t expect approval until at least a year from now—or they aren’t sure

Will Apply for CBPR?



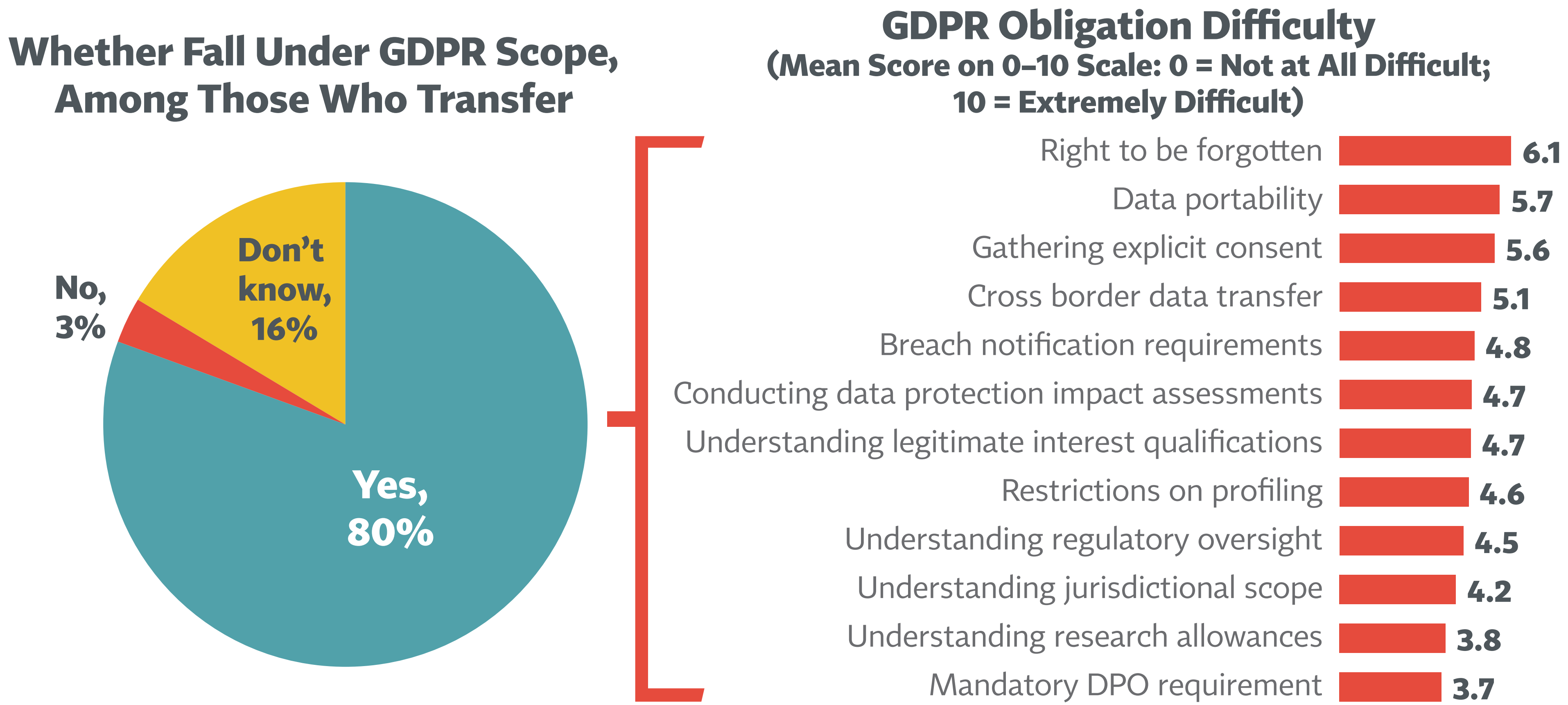
Expected CBPR Approval



J9: Will your organization apply for Cross Border Privacy Rules (CBPR) to transfer data in the APEC region?
J10: When do you expect your CBPR application to be approved?

8 in 10 organizations who transfer data say they fall under GDPR

- Three aspects of GDPR are considered most difficult: right to be forgotten, plus data portability and explicit consent requirements



J7a: Does your organization fall under the scope of the General Data Protection Regulation (GDPR)?
J7b: Please rate each of the following legal obligations of the General Data Protection Regulation on a scale from 0-to-10

Several GDPR obligations are of higher-than-average concern to certain segments

KEY SEGMENT DIFFERENCES

GDPR Obligation Difficulty: Higher Than Average Concerns

(Mean Score On 0–10 Scale: 0 = Not At All Difficult; 10 = Extremely Difficult)

Financial Services:
Data Portability
(6.4)

Manufacturing:
Right to be Forgotten
(7.5)

Hospitality:
Gathering Explicit Consent
(8.3)

25K–74K Employees:
Mandatory DPO Requirement
(4.6)

Revenue < $100 Million:
Understanding Regulatory Oversight
(5.5)

Privacy Spend < $10K:
Breach notification requirements
(6.2)

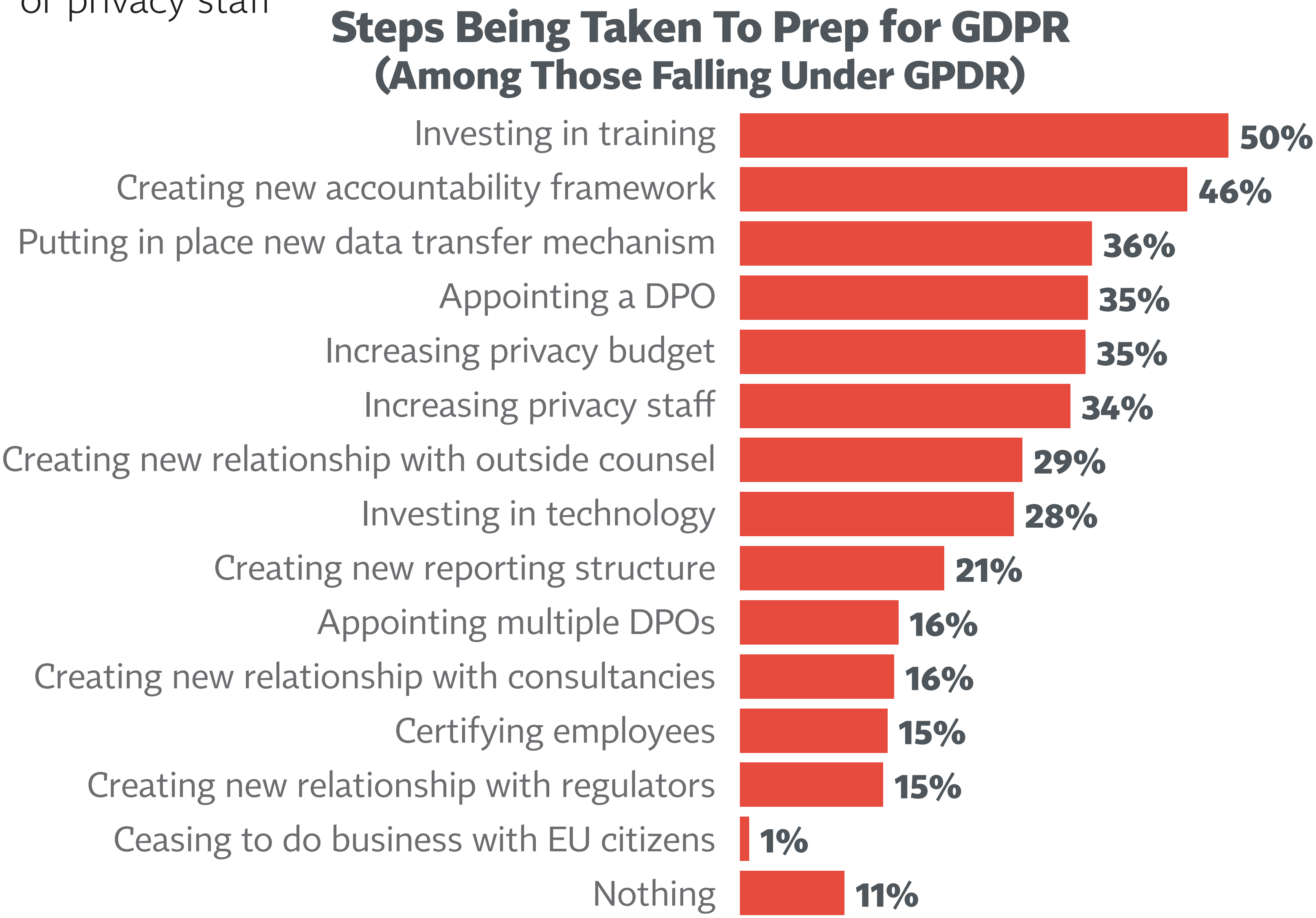
Privacy Spend < $10K:
Understanding Research Allowances
(5.6)

Privacy Spend < $10K:
Understanding Regulatory Oversight
(6.2)

J7b: Please rate each of the following legal obligations of the General Data Protection Regulation on a scale from 0-to-10

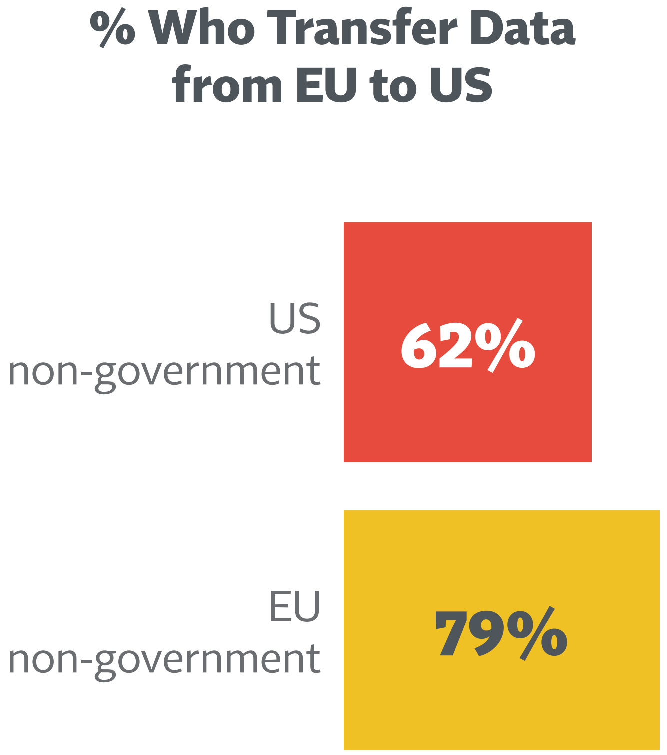
The most commonly taken steps to prepare for GDPR are developing training and accountability frameworks

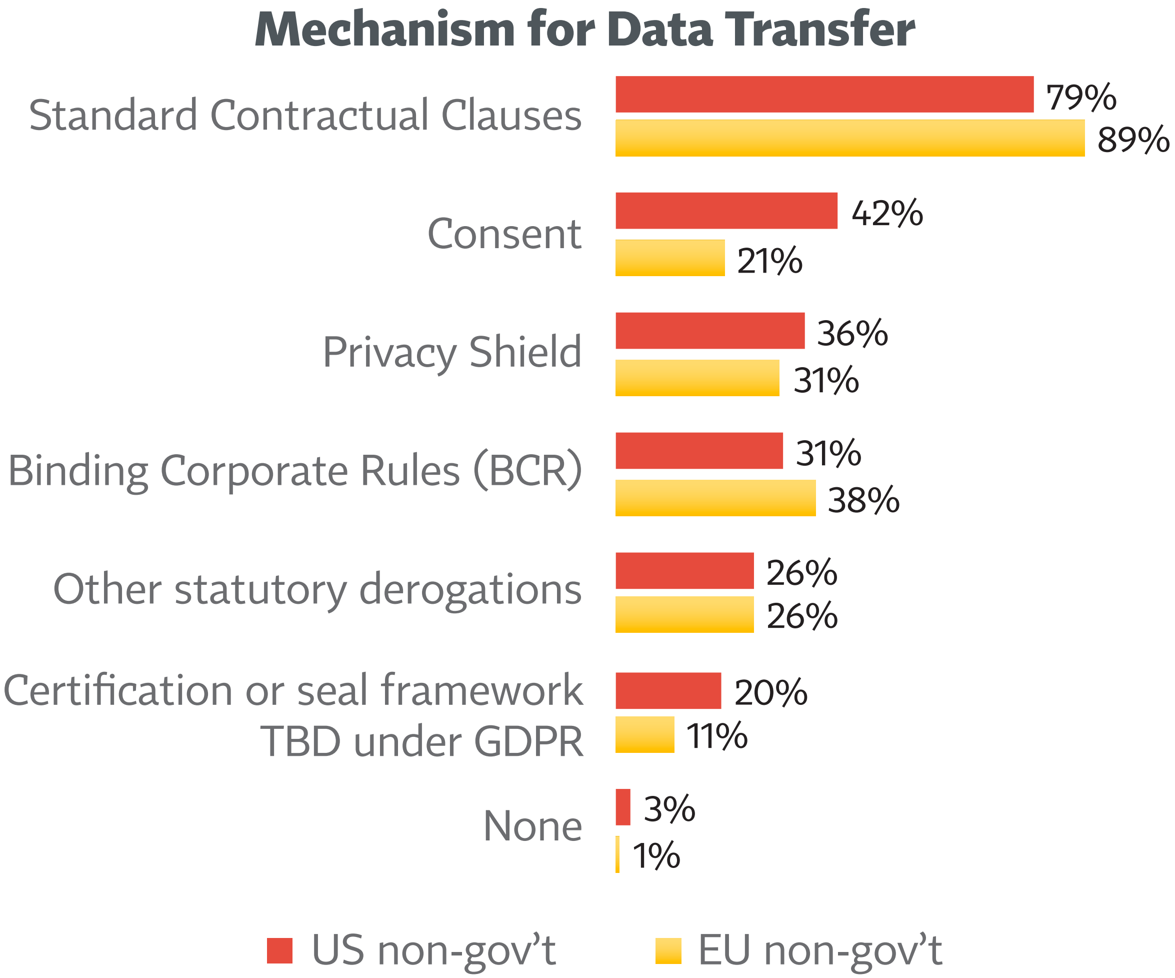
- About a third each say they're preparing by boosting their privacy budget or privacy staff



J8: What, if anything, is your organization doing to prepare for the GDPR?

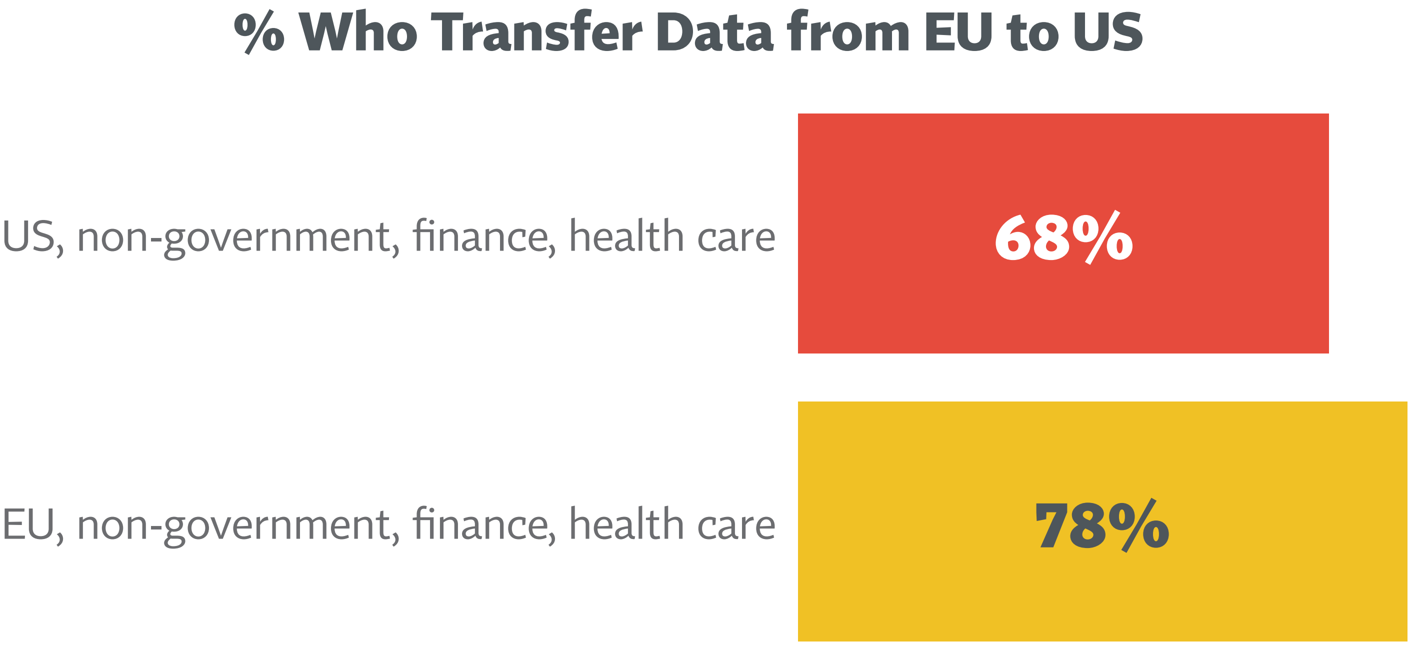
Looking specifically at non-government, EU firms are more likely than US to transfer data and use BCR





J1: Does your organization transfer personal information from the European Union to the United States?
J5: What mechanism(s) does your company intend to use to transmit data to the U.S.?

EU firms are also more likely to transfer data when we exclude finance/health care, along with government



J1: Does your organization transfer personal information from the European Union to the United States?

US firms are much more likely to have certified under Safe Harbor, but only 42% intend to use Privacy Shield

KEY SEGMENT DIFFERENCES

Safe Harbor and Mechanism for Data Transfer

	US w/o Gov't, Finance, Health	EU w/o Gov't, Finance, Health
Certified Under Safe Harbor	73%	37%
Mechanisms		
Standard Contractual Clauses	81%	92%
Privacy Shield	42%	32%
Consent	41%	16%
Binding Corporate Rules (BCR)	31%	31%
Other statutory derogations	25%	27%
Certification or seal framework TBD under GDPR	23%	10%

J2: Did your company certify under Safe Harbor?
J5: What mechanism(s) does your company intend to use to transmit data to the U.S.?

The gap between Safe Harbor and Privacy Shield is especially big for companies with 25K–75K employees

KEY SEGMENT DIFFERENCES

Safe Harbor and Mechanism for Data Transfer

	Employee Size, US and EU, Without Gov't, Finance, Health			
	Under 5K	**5K–24.9K**	**25K–74.9K**	**75K+**
Certified Under Safe Harbor	61%	59%	75%	65%
Mechanisms				
Standard Contractual Clauses	86%	78%	96%	78%
Privacy Shield	43%	44%	26%	43%
Consent	36%	44%	37%	24%
Binding Corporate Rules (BCR)	8%	29%	26%	53%
Other statutory derogations	36%	24%	26%	19%
Certification or seal framework TBD under GDPR	24%	22%	15%	18%

J2: Did your company certify under Safe Harbor?
J5: What mechanism(s) does your company intend to use to transmit data to the U.S.?

That gap is mostly a US phenomenon, with much higher numbers using Safe Harbor vs. Privacy Shield

KEY SEGMENT DIFFERENCES

Safe Harbor and Mechanism for Data Transfer

	Employee Size, US only, Without Gov't, Finance, Health			
	Under 5K	**5K–24.9K**	**25K–74.9K**	**75K+**
Certified Under Safe Harbor	77%	69%	80%	67%
Mechanisms				
Standard Contractual Clauses	88%	69%	96%	75%
Privacy Shield	52%	41%	29%	47%
Consent	38%	55%	42%	28%
Binding Corporate Rules (BCR)	8%	28%	29%	52%
Other statutory derogations	34%	28%	25%	17%
Certification or seal framework TBD under GDPR	22%	31%	17%	20%

J2: Did your company certify under Safe Harbor?
J5: What mechanism(s) does your company intend to use to transmit data to the U.S.?