



# **Benchmarking Privacy: An Executive Summary**

---

International Association of Privacy Professionals

Inside Front Cover (blank)

# Benchmarking Privacy: An Executive Summary

---

International Association of Privacy Professionals

## || Welcome

Dear privacy professionals,

We are pleased to present you with the IAPP's newest research on organizational privacy practices. The IAPP has partnered with the Ponemon Institute, a leading research organization in privacy management practices, to develop the first comprehensive benchmark study of the privacy profession.

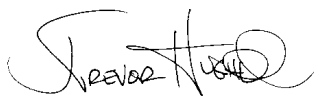
This executive summary presents the key findings of this landmark survey, which measures everything from demographics, jurisdiction and staffing to program maturity, collaboration and success measures.

With the unprecedented growth of the privacy profession, this data is intended to provide you with solid data to support your strategic planning efforts, build your privacy team and plan for future initiatives.

I hope that you find this information valuable. I encourage you to share it your management, staff and colleagues as a means to advance the business and operational needs of your privacy department.

I urge you to visit our Web site, [www.privacyassociation.org](http://www.privacyassociation.org), for additional professional resources and watch for more data, surveys and research from the IAPP over the coming months.

Sincerely,



J. Trevor Hughes, CIPP  
Executive Director  
IAPP



# Table of Contents

## **I. Executive Summary**

1. Privacy office, organizational location, jurisdiction, staffing and leader-staff communications	4
2. Program maturity level and privacy office focus.	5
3. Collaboration & cooperation with other organizational functions	5
4. Measuring success in meeting objectives	6
5. Respondent & organization demographics	6
6. Titles, experience levels and salary ranges	6

## **II. Caveats to our survey's findings**

## **III. Benchmark survey methods**

## **IV. Survey Results**

1. Privacy office location, jurisdiction, budget, staffing and leader-staff communication	9
2. Program maturity level and privacy program objectives	15
3. Collaboration with other functional areas	19
4. Measurements of success in meeting objectives	20
5. Organizational demographics	21

## **Appendix: Privacy Leaders and Staff Audited Survey Results**

Privacy Leader Responses	29
Privacy Staff Survey Responses	42

# I. Executive Summary

---

Ponemon Institute and the International Association of Privacy Professionals (IAPP) are pleased to report this research on the organizational privacy practices for a sample of benchmarked companies. The survey used to collect data included two separate instruments – privacy leaders and staff members. The staff survey was limited to questions about job function and salary, while the privacy leader survey included questions about the company's privacy program structure and characteristics, program goals and activities, and program effectiveness measurement techniques.

In August 2008, benchmark instruments were mailed to a representative cross-section of IAPP member organizations. The research design involved a two-step process. First, an in-depth benchmark survey was sent to privacy leaders in major organizations. After completing this instrument, privacy leaders returned the survey form directly to the researcher. In addition to the primary instrument, privacy leaders were asked to circulate a second short survey to members of their immediate staff. Staff members completed this confidential survey and sent the results directly back to the researcher.

In total, 62 privacy leaders and 104 staff practitioners responded to the two surveys over a five month time period. To preserve confidentiality, no individual or company-identifiable information was captured by the researchers during the analysis of data.

The present study seeks to determine the following important questions about the efficacy of privacy and data protection programs in major organizations:

- How is the privacy office organized and structured?
- How is the privacy office staffed and budgeted?
- Does an organization's size and program maturity make a difference?
- What is the organization's budget and how is it distributed across typical activities?
- What other functions do privacy leaders and staff members perform?
- What are the privacy program's top priorities?
- How important is collaboration and cooperation across the enterprise to program success?
- How do organizations measure program objectives and performance?

In addition to the above questions, the present study seeks to understand the roles, responsibilities and expectations of staff members who work in their organization's privacy office (or program activity). Specifically, we seek to understand:

- What is the breadth of responsibilities of privacy employees?
- What are compensation levels and do they vary for certifications, titles and job responsibilities, organizational size, and organizational reporting relationships?
- What is included in total compensation and what are expectations of compensation?

The key findings of the presented research are summarized in this report. Please note that a small number of responding companies – coupled with non-scientific benchmark methods – make it impossible to apply tests of statistical significance. Hence, this research focuses on description and inference.

## I. Privacy office, organizational location, jurisdiction, staffing and leader-staff communications

Leaders reported that they are fairly high-level in their organizations with 61% at only one or two reporting levels away from their company CEO; 27% are three levels away. Leaders report most often to the General Counsel (19%), the Compliance/Ethics Officer (19%) or the CEO/Executive Committee (18%).

Of the respondents, 89% indicated their privacy offices are located in the United States with jurisdiction across multiple locations – U.S. (96%), Canada (46%), Europe (42%), Asia-Pacific (37%) and Latin America (35%).

The external budgets of participating companies vary considerably. More than 25% of companies report an annual budget of \$500,000 to \$1 million; about 23% are above \$1 million to \$2.5 million; about 18% are less than \$100,000.

---

**Key Finding 1:** Budgets vary disproportionately according to the size of the organization. More than 70% of companies with over \$10 billion in revenue reported privacy budgets between \$500,000 and \$2.5 million.

---

On average, staffing costs represented 56% of the total budget, followed by overhead and administration (5%), policies, procedures and governance (5%), outside legal (4%) and outside consultants (4%).

Approximately 60% of leaders reported two or more full-time employees and 43% reported two or more part-time employees. Twenty-two percent of leaders reported no full-time staff and 42% reported no part-time staff.

Most leaders also reported that they anticipated either no change in headcount (68% for full-time and 80% for part-time) or an increase in headcount (29% for full-time and 15% for part-time).<sup>1</sup>

Fifty-five percent of organizations use indirect staffing resources (a.k.a. privacy liaisons) to fulfill privacy and data protection activities. About 73% of leaders report that privacy liaisons are assigned by business function rather than geography. We believe that privacy leaders recognize the importance of liaisons – especially in data critical areas such as human resources, corporate IT, marketing and information security – for ensuring enterprise compliance. Despite the importance of privacy liaisons, 47% of leaders said they do not control or influence these liaisons through the organization's official chain-of-command.

Seventeen percent of privacy leaders have daily meetings and 50% have weekly meetings with core team members. Communication with privacy liaisons was much less frequent, with 7% having weekly meetings and 37% having monthly meetings.

## 2. Program maturity level and privacy office focus

We asked privacy leaders to rate their organization's privacy initiatives according the following maturity classification:

- Pre-stage – program has not been established as a unit within the company
- Early stage – program is just starting to become staffed and organized
- Middle stage – program is in existence and is starting to launch key initiatives
- Late middle stage – program is starting to evaluate the effectiveness of key initiatives
- Mature stage – program is in maintenance mode focusing on program evaluation and refinement

Thirty-six percent of privacy leaders indicated their programs were at the mature stage, 18% at the late middle stage, 27% at the middle stage, and 18% at the early or pre-program stages.

---

**Key Finding 2:** The scope and function of privacy initiatives change as the program matures. Immature privacy programs tend to have a narrow focus on a particular law, issue or data type. As the program matures, its focus broadens to other related domains including the strategic use of information assets.

---

With respect to data type, privacy programs protect employee records (95%), customer or consumer records (91%), and business customer information (84%).

The majority of privacy programs in this study provide policies, procedures (SOPs) and other guidance to assist the organization's various business units in safeguarding confidential information about people and families. A majority of these privacy programs managed policies or SOPs about consumers and customers (88%), business customers (78%) and employees (78%).

A majority of leader and staff respondents said they perform functions above and beyond their primary privacy role. Such additional functions include regulatory compliance and information security. A large number of leaders also report general management responsibilities beyond privacy program management.

## 3. Collaboration & cooperation with other organizational functions

Privacy leaders were asked about the importance of collaboration or cooperation with other functions. Collaboration with information security (100%), corporate IT (98%), legal (98%), regulatory compliance (93%), and human resources (83%) was deemed to be either very important or important to the success of the organization's privacy mission.

More than half of respondents believed collaboration with corporate ethics, physical security, internal audit, records management, marketing, governmental affairs, public relations and procurement were either very important or important. It is our belief that the need for collaboration increases as the privacy program matures.

---

**Key Finding 3:** Privacy professionals recognize the need for collaboration across the enterprise in order to achieve privacy and data protection objectives.

---

<sup>1</sup> These responses were returned during the financial services crisis but before full recognition of the recession. Thus, the headcount and budget expectations reported may not reflect this economic change.

#### 4. Measuring success in meeting objectives

Fifty-five percent of respondents said their organizations have measures in place to evaluate the privacy program's performance (success or failure) in meeting its mission or objectives. A majority of respondents said they measure organizational compliance with policies (90%), coverage of training and awareness to employees (90%), reductions in data breach incidents (74%), and frequency of customer or consumer complaints (71%). Albeit more qualitative, respondents believe the effectiveness of policy and training should be included in program performance evaluation.

---

**Key Finding 4:** A majority of organizations attempt to measure their privacy program's success or failure in meeting objectives.

---

Self-assessment and audit are the two techniques used most frequently. The results of these self-assessments or audits are used to evaluate programs or to provide evidence of the organization's compliance with policies and law.

#### 5. Respondent & organization demographics

Respondents represent 15 industry segments. The largest industry segment is financial services (37%) followed by health care (14%).

The majority of leaders were located in larger-sized companies with 72% at revenues above \$1 billion. Seventy-four percent have more than 25,000 employees. Sixty-two percent of participating companies are publicly traded.

On gender, leaders are split evenly while staff respondents are skewed to female (63%). Most leaders have a high level of relevant credentials and certifications. Eighty-seven percent indicated that either they or someone on their staff has a CIPP, CIPP/G or CIPP/C designation followed by 33% reporting a CISSP certification. Sixty-five percent of leaders also report that either they or someone on their staff earned a JD or LLM. Approximately 55% report staff members with an MBA or MS degree or other advanced degree.

---

**Key Finding 5:** A majority of participating privacy offices have someone on the staff with a CIPP, CIPP/G or CIPP/C designation.

---

#### 6. Titles, experience levels and salary ranges

Approximately 89% of leaders are director level or higher. More than 60% of privacy leaders are within two levels of the CEO (or the highest ranking executive position in the organization). About 76% of leaders have privacy in their title compared with 59% of staff members.

Leaders, on average, have 23.4 years experience in business, 7.5 years in privacy and 4.6 years in their present position. Staff members have 18.5 years in business, 4.7 years in privacy and 2.8 years in their present position. More than 28% of staff respondents have been in their position less than one year.

About 59% of leaders have an annual salary above \$150,000 (U.S. dollars) with 81% expecting a bonus and 56% expecting stock options, warrants, or shares. Sixty-three percent thought their compensation was comparable or above others in their organization with the same experience, education and training while 30% thought their compensation was lower than others in their organization.

About 73% of staff reported salaries between \$60,001 and \$150,000 with 72% expecting a bonus and 23% expecting stock options, warrants, or shares. Of staff, 59% thought their compensation was comparable or above others in their organization with the same experience, education and training while 25% thought it was lower than others.

---

**Key Finding 6:** Male respondents were 10 percentage points more likely than females to believe their compensation was comparable or above others in their organization.

---



## II. Caveats to our survey's findings

---

The current findings are based on voluntary survey returns. Surveys were mailed to individuals at selected IAPP member companies. Usable responses from the mailing totaled 62 leaders and 104 staff members. It is always possible that individuals who chose not to participate are substantially different in terms of their compensation, roles, and other job-related functions from those who completed the instrument.

Because the sampling frame is selected IAPP membership, the quality of the results is influenced by the accuracy of member contact information and the degree to which the list is representative of the population of privacy professionals being studied. It is our belief that the IAPP list was reasonably accurate at the time of mailing the survey. Although the IAPP is the largest association dedicated to privacy, we acknowledge that the results may be biased in three important respects:

- Not all IAPP members received the survey.
- Survey results are skewed to financial services and healthcare organizations, which are the largest industry sectors in the IAPP today.
- The IAPP membership is primarily located in North American-based organizations. While Canadian, European and Asia-Pacific members exist within the association today, results of this study should not be generalized to other nations or regions of the world.

To keep the survey concise and focused, we decided to omit other normatively important variables from the analyses. The extent to which omitted variables might explain salary cannot be estimated at this time.

The sample size is small, hence the ability to generalize segmented findings about organizational size, program maturity and industry is limited. Great care should be exercised before attempting to generalize findings.

The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide a truthful response.

Surveys were mailed during the crisis in the financial services sector before the recession was fully recognized. Since that time, many companies have been reducing budgets and staffs as part of restructuring and cost pressure. Hence, the headcount and budget expectations reported here may not reflect privacy program cuts among participating companies.

### III. Benchmark survey methods

---

In total, 336 IAPP member organizations, each with a privacy officer or equivalent plus staff members within that group, were selected for participation. The member list was focused on senior positions, both private and public sector, and organized according to title.

The survey was fielded over the course of five months starting August 1, 2008. After an initial response window ending November 1, 2008, we re-announced the survey at that year's Privacy Academy event and accepted responses through mid-January 2009.

The detailed privacy leader survey and smaller staff-level survey were mailed as a package to the privacy leader (IAPP member) at each of the 336 organizations. Each package contained a cover letter addressed to that member from IAPP Executive Director Trevor Hughes along with a leader survey form plus a selection of staff survey forms for redistribution. All forms were completed and returned individually to the IAPP through pre-posted/pre-addressed

envelopes provided by the IAPP. Additional forms were made available upon request – particularly if the organization required more than the 10 staff forms typically included.

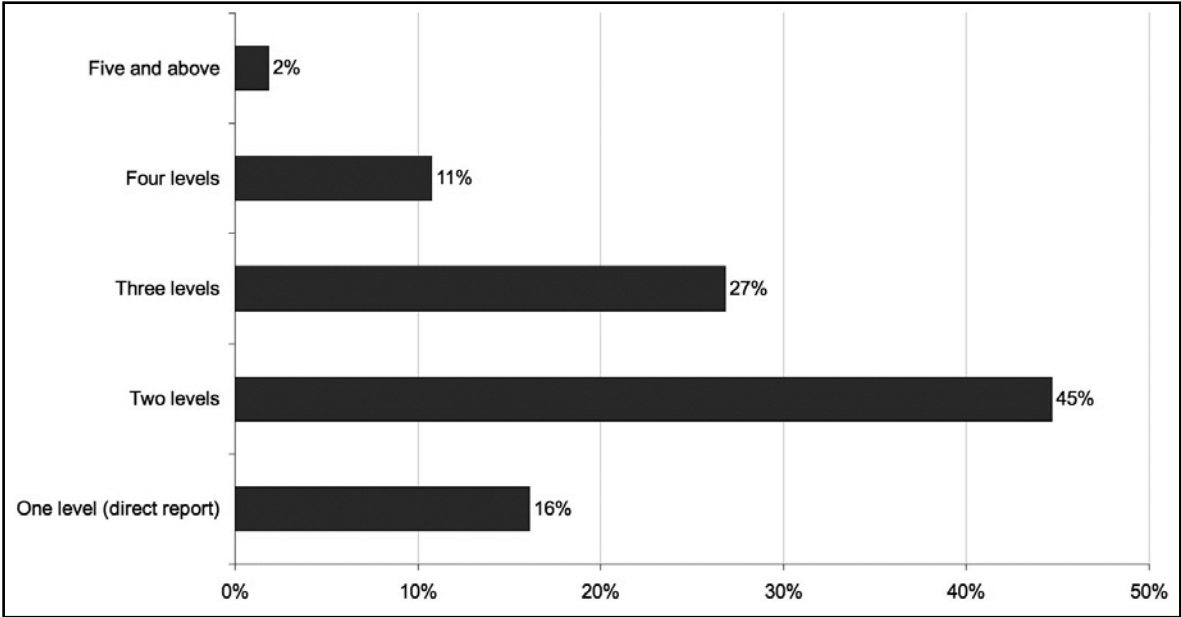
Responses were anonymous though batches of responses were identified to organization based upon a three-digit code assigned to that mailing. The survey forms were gathered by the IAPP and sent to Newburyport, MA-based Data Capture Solutions who scanned the forms, tabulated the data and exported them to Excel for analysis by the Ponemon research team. Tabulation was completed in January, 2009 and analysis began in February, 2009.

# IV. Survey Results

## I. Privacy office location, jurisdiction, budget, staffing and leader-staff communication

This section describes how privacy leaders reported their program or office structure, including reporting relationships, budget, staffing and ongoing communication. Bar Chart 1 shows that 16% of privacy leaders are a direct report to the CEO. Sixty-one percent of the leaders are only two or three reporting levels away from their company’s CEO with another 13% four or more levels from the chief executive.

Bar Chart 1: Levels between the privacy leader and the organization’s CEO



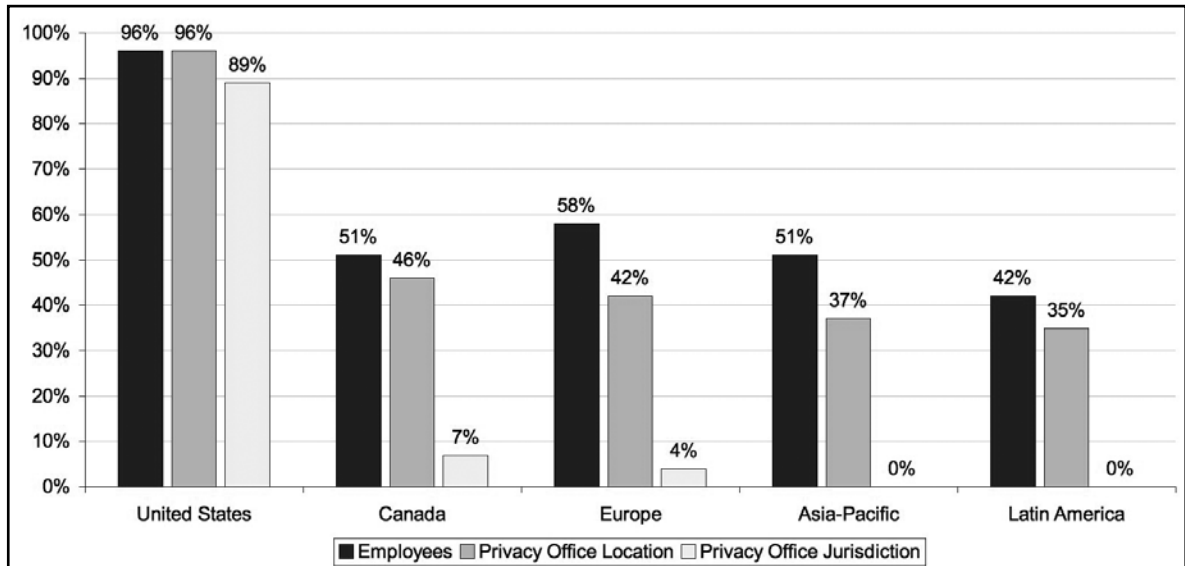
Privacy leaders stated their line of report (chain-of-command) as follows:

- General Counsel (19%)
- Compliance/ethics officer (19%)
- CEO/executive committee (18%)
- Chief information officer (11%)
- Chief Risk officer (11%).

Respondents identified the corporate law department as the most frequent department for locating the privacy office (29%), followed by the compliance department (23%).

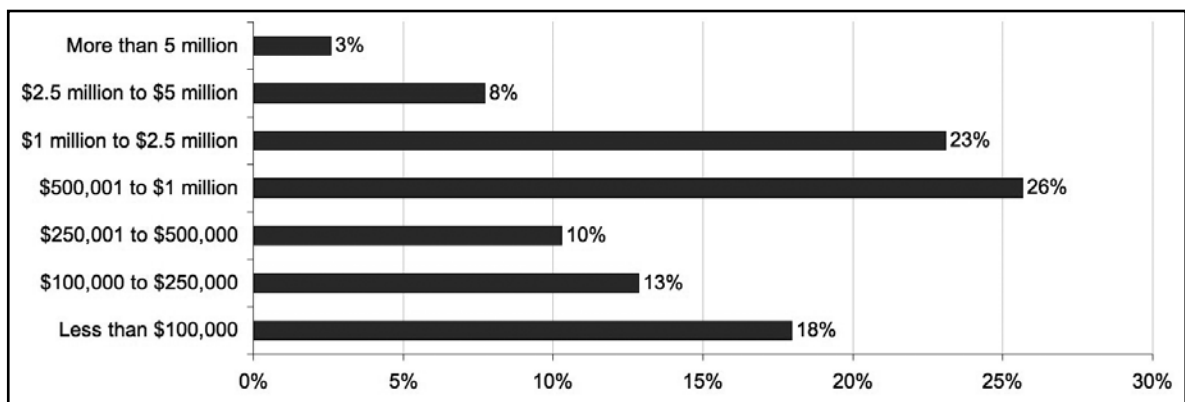
As shown in Bar Chart 2, respondent companies have employees in multiple locations. The U.S. is the top geographic location for the privacy office (89%) followed by Canada (7%) and Europe (4%). The jurisdiction of the privacy office is broader and aligned with company employee locations.

**Bar Chart 2: Geographic footprint of participating organizations by employees, jurisdiction of the privacy office and the location of privacy program offices**



**Bar Chart 3: Total external budget of the organization's privacy program**

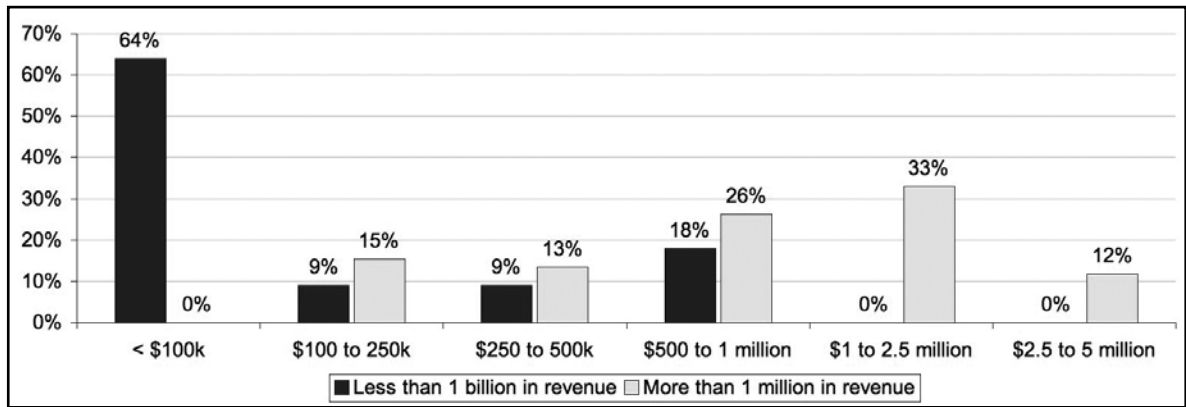
We surveyed leaders on their external budget levels (not including staff compensation or liaison cost), anticipated changes to budget levels, and the primary uses of the budget. Bar Chart 3 shows the distribution of the total external budget.



Twenty-six percent of privacy leaders reported program budgets between \$500k and \$1 million. About 23% reported budgets between \$1 million and \$2.5 million, and 11% are above \$2.5 million. More than 18% reported a budget less than \$100k, 13% at \$100k to \$250k and 10% are above \$250k to \$500k. At the time of the survey, 67% of respondents expected no change in their budget for 2009, 19% expected an external budget increase and 13% expected an external budget decrease.

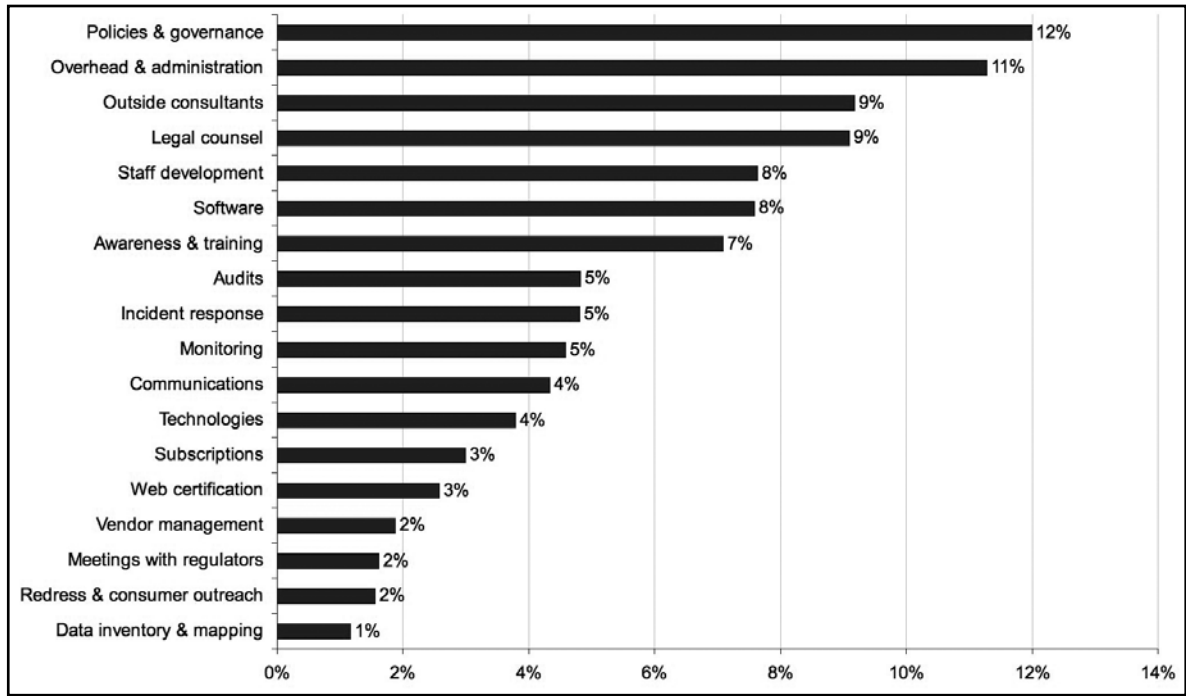
As shown in Bar Chart 4, 64% of companies with revenues less than \$1 billion reported an external budget of less than \$100k. About 33% of companies with total revenues greater than \$1 billion reported an external budget between \$1 million to \$2.5 million. Not shown is that 56% of the company's total budget is compensation and benefits for employees dedicated to the privacy program.

**Bar Chart 4: Total external budget range for smaller and larger-sized organizations**



The largest budget categories include policies and governance, overhead and administration, outside consultants and legal counsel (Bar Chart 5).

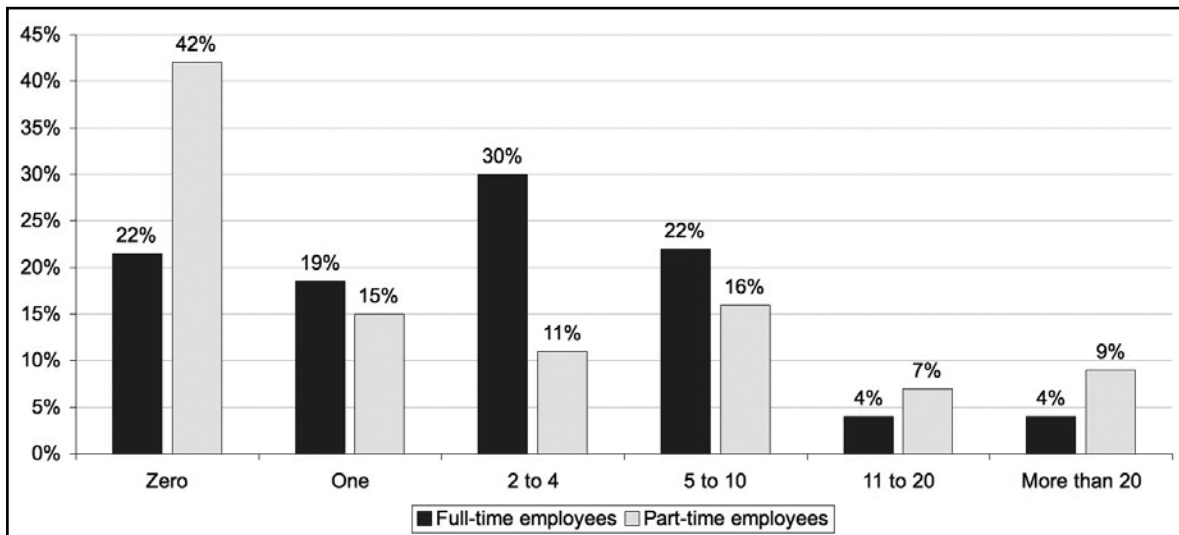
**Bar Chart 5: Allocation of external budget dollars by earmarked program category**



Bar Chart 6 shows staffing levels for full-time and part-time employees. Seventy-one percent indicated they had four or fewer full-time employees. Twenty-two percent indicated they had no full-time dedicated employees.

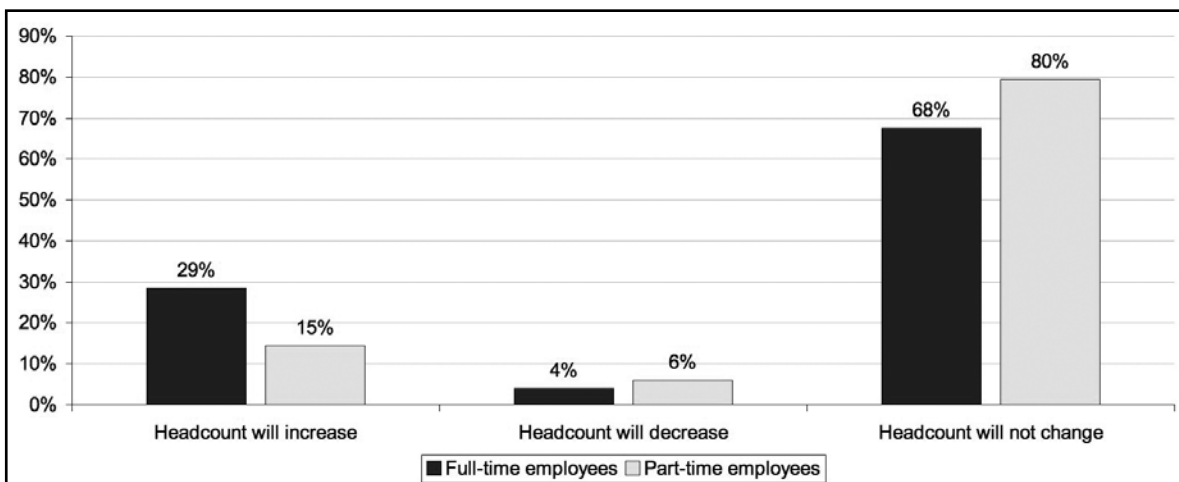
Forty-two percent reported no part-time employees and 32% reported they had five or more. While not shown here, contract or temporary employees accounted for 13% of full-time and 12% of part-time employees.

**Bar Chart 6: Employees dedicated to privacy programs**



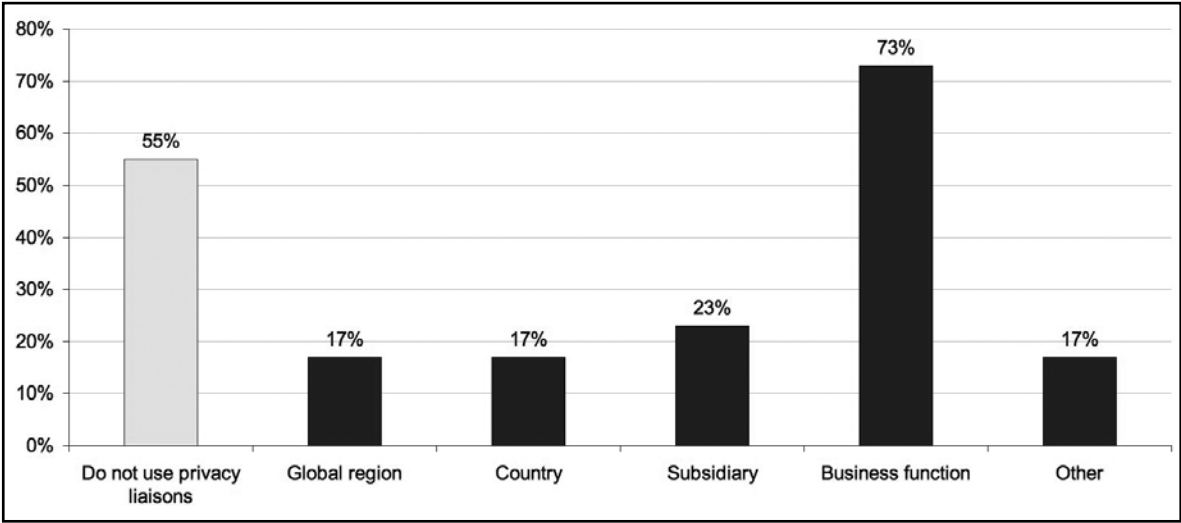
As shown in Bar Chart 7, many respondents anticipated no change in employee headcount in the 2008 fiscal year (68% for full-time and 80% for part-time) or an increase in headcount (29% for full-time and 15% for part-time). A small percentage of respondents anticipated headcount to decrease (4% for full-time and 6% for part-time). Please note that this survey was taken prior to full recognition of the recession that resulted in cost-cutting efforts at many companies.

**Bar Chart 7: Anticipated headcount changes**



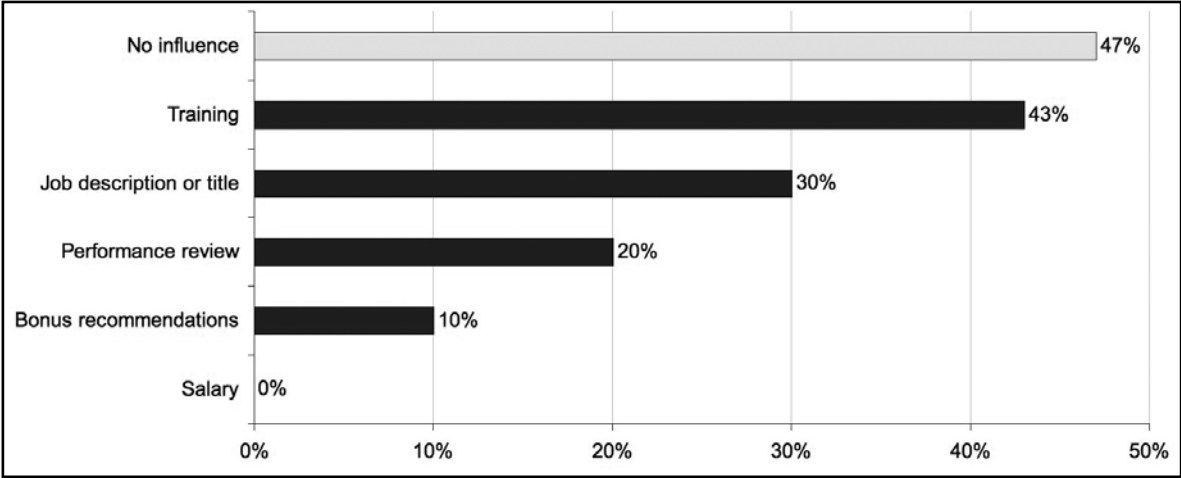
Bar Chart 8 shows 55% of participating organizations use privacy liaisons to supplement their staffing needs. Of those organizations, privacy liaisons are assigned primarily by business functions (73%) such as corporate IT, marketing, human resources, information security, business divisions and so forth. While not shown here, privacy liaisons are used by both smaller and larger-sized companies.

Bar Chart 8: Are privacy liaisons utilized and if so how are they assigned?



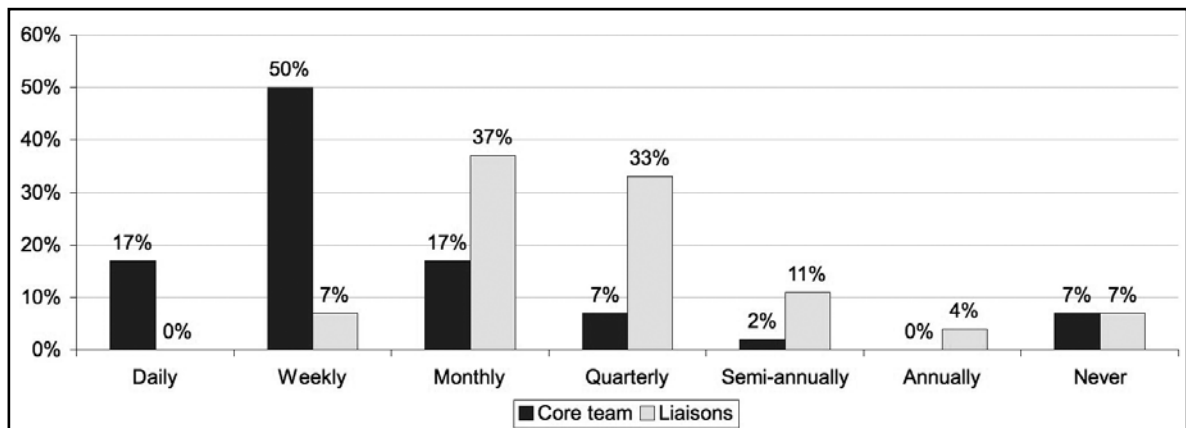
As noted in Bar Chart 9, privacy leaders have relatively little influence over the privacy liaisons in their companies. Almost half (47%) reported they have no organizational influence over the performance of privacy liaisons. Although, 43% of leaders indicated influence in the training of liaisons and 30% indicated influence over job description or title. Only 20% and 10% of leaders influence liaison performance reviews and bonus recommendations, respectively. While not shown, leaders reported that 77% of privacy liaisons receive annual training, but only 45% of these liaisons are required to have specific skill sets as a prerequisite or background to being appointed.

Bar Chart 9: How does the leader influence privacy liaisons?



As shown in Bar Chart 10, 17% of respondents hold daily meetings or conference calls with their core privacy team, 50% talk weekly, 17% talk monthly and the remaining 16% talk quarterly, annually or never. Although not as frequent as core team meetings/conference calls, seven percent of leaders reported weekly contact with privacy liaisons while 37% reported monthly, 33% reported quarterly, 15% of leaders reported semi-annual or annual calls and seven percent reported never talking to privacy liaisons.

**Bar Chart 10: Communications with privacy liaisons**



Finally, as shown in Bar Chart 11, full-time and part-time headcount varies by size of budget with companies with a smaller budget having a lower headcount. Salary is a smaller percentage of budgets that are \$500k or less. Smaller budgets have higher percentages of funds allocated to policies, procedures, and governance (approximately 11%), legal counsel (6%) and monitoring (5%) and organizational training and awareness (5%).

Larger budgets (more than \$500k) have higher percentages allocated to overhead and administration (6%), outside consultants (5%) and staff development and training (4%). These differences could reflect a one-person office (leader only) at smaller organizations with smaller budgets, program maturity level or cross-functional integration or job responsibilities for the privacy office.

**Bar Chart 11: Full-time and part-time headcount for budgets less than \$500k and more than \$500k**

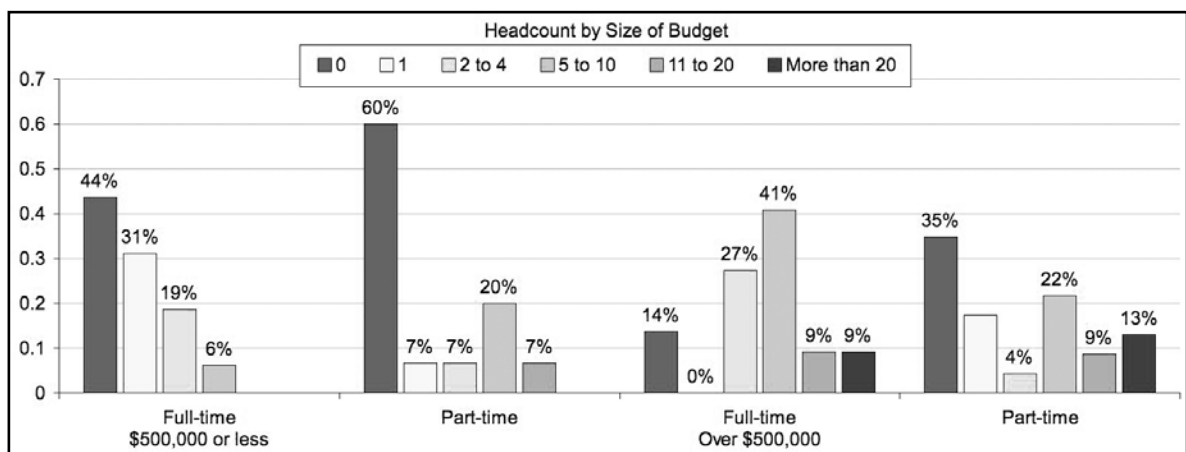




Table 1 shows categories of budget spending for smaller and larger-sized privacy programs.

**Table 1: Category represents more than five percent of the budget on average**

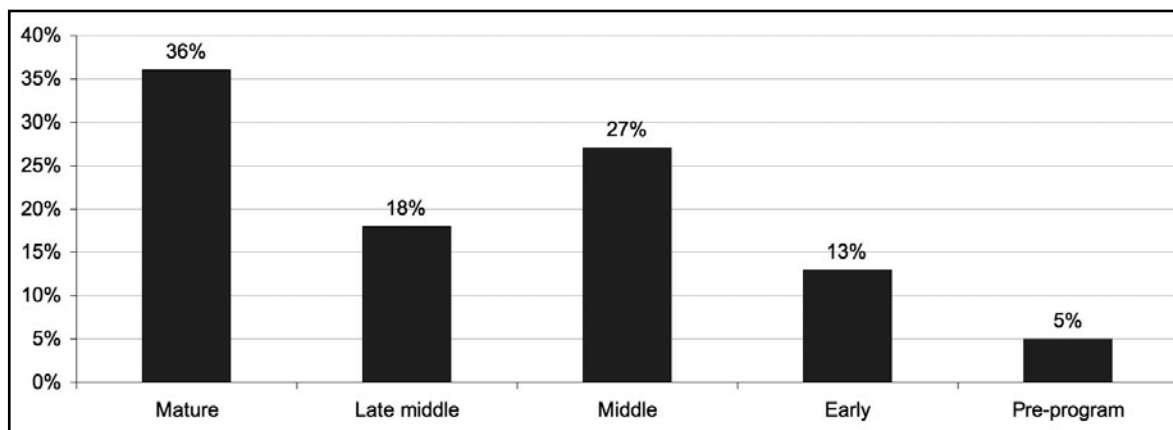
Budget categories	\$500,000 or less	Above \$500,000
Salary and benefits	45.5%	59.3%
Policies, procedures. & governance	10.9%	3.0%
Legal counsel	6.3%	3.3%
Monitoring	5.3%	0.5%
Organizational awareness & training	4.5%	2.8%
Overhead & administration	2.6%	6.0%
Outside consultants	2.9%	5.4%
Development & training for staff	3.2%	3.9%

## 2. Program maturity level and privacy program objectives

We also asked privacy leaders to tell us about the maturity level of their programs, their priorities, the types of information they were expected to safeguard, internal collaboration and measures of success.

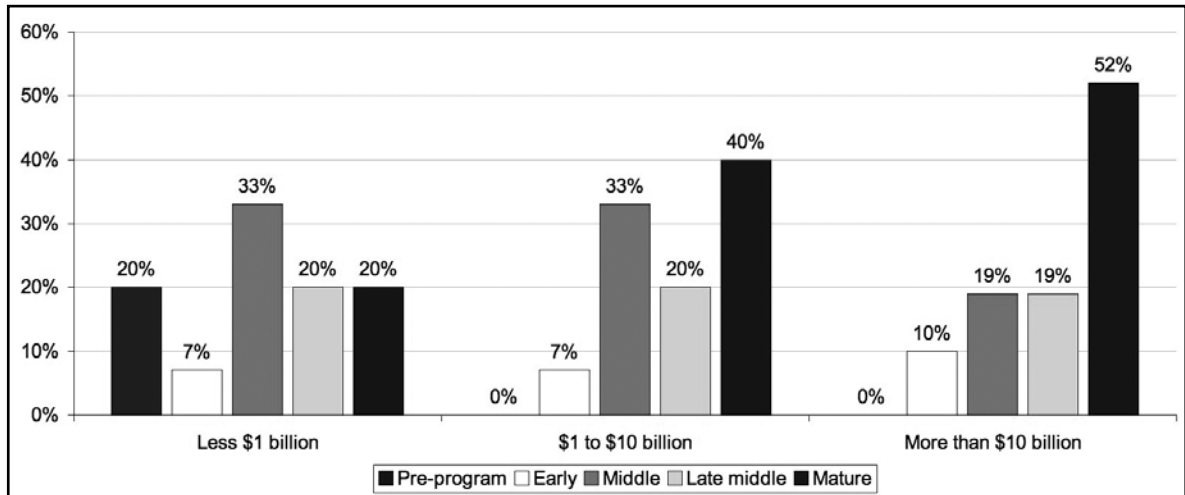
Maturity level is inextricably related to the structure and function of the privacy program. As shown in Bar Chart 12, 36% of respondents indicated their program was at the mature stage, 18% at the late middle stage, 27% at the middle stage, 13% at the early stage and five percent are pre-stage.

**Bar Chart 12: Maturity stages of participating companies**



**Bar Chart 13: Maturity stages by company's revenue size (range)**

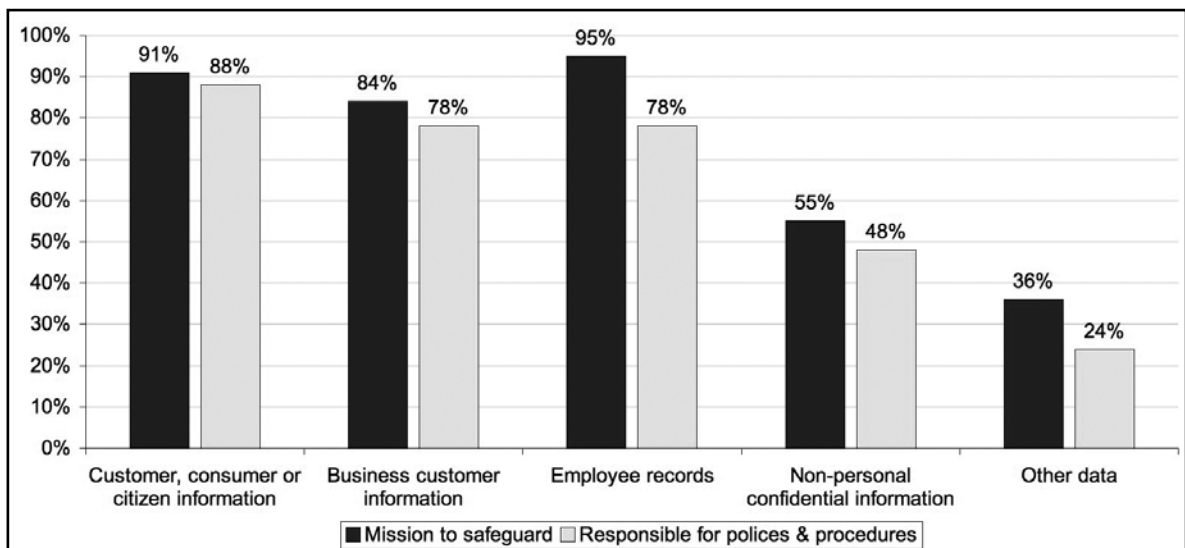
The maturity level of a company's privacy program was analyzed within three organizational size categories based on total revenue.



As shown in Bar Chart 13, large companies reported a large mix of mature (52%) and middle-stage programs (38%) while mid-size companies reported fewer mature programs (40%) but more mid-stage (53%). Small companies reported mature programs at 20% of the distribution but also reported pre-stage programs at 20%. This may not be surprising given that large companies typically have more resources to apply at the onset of a privacy incident and, hence, more likely to advance to maturity.

Leaders were asked about the mission of their programs in terms of information types they sought to safeguard. As shown in Bar Chart 14, most respondents reported the need to safeguard multiple types of information including employee (95%), customer or consumer (91%), business customer (84%), non-personal business confidential (55%) and other data, including intellectual property (36%). Respondents also indicated program responsibility for providing policies, procedures and other forms of guidance to business units but the average response rate was lower level in each category than for safeguarding of information. Most notable is the 17% point difference in safeguarding employee records and providing policies, procedures and guidance.

**Bar Chart 14: Maturity stages by company's revenue size (range)**



Regardless of program maturity level, it appears there are high expectations that privacy programs will safeguard customer/ consumer, business customer and employee information and will provide policies, procedures and other guidance accordingly. However, there are some interesting observations among the privacy levels and expectations as shown in Table 2.

**Table 2: Privacy Program Maturity Level**

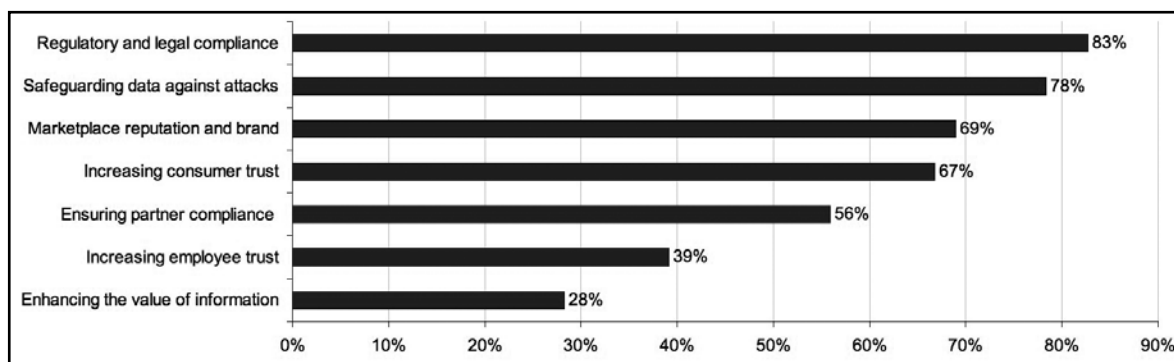
Information Type	Pre- or Early		Middle		Late Middle		Mature	
	Safeguard	Provide Guidance	Safeguard	Provide Guidance	Safeguard	Provide Guidance	Safeguard	Provide Guidance
<b>Customer/ Consumer</b>	70%	70%	100%	93%	70%	70%	100%	80%
<b>Business Customer</b>	70%	50%	87%	73%	70%	80%	95%	75%
<b>Employee</b>	80%	70%	93%	67%	90%	80%	100%	70%
<b>Non-Personal</b>	30%	20%	73%	67%	50%	50%	55%	35%
<b>Other</b>	20%	20%	47%	20%	20%	20%	40%	25%

It appears that programs start narrowly focused; then expand to more data categories as they reach the middle stage; and refocus on top areas in the late middle stage. Mature programs have high expectations to safeguard information across all three of the top categories but guidance is not as high a priority.

Leaders were provided seven typical priorities for a privacy program and were asked to force rank them from most important to least important. Respondents reported multiple categories as tied at most important or important, negating a true forced ranking. It is interesting to note that the “enhancing the value of information assets” and the “increasing employee trust” categories received the lowest scores for importance as a priority.

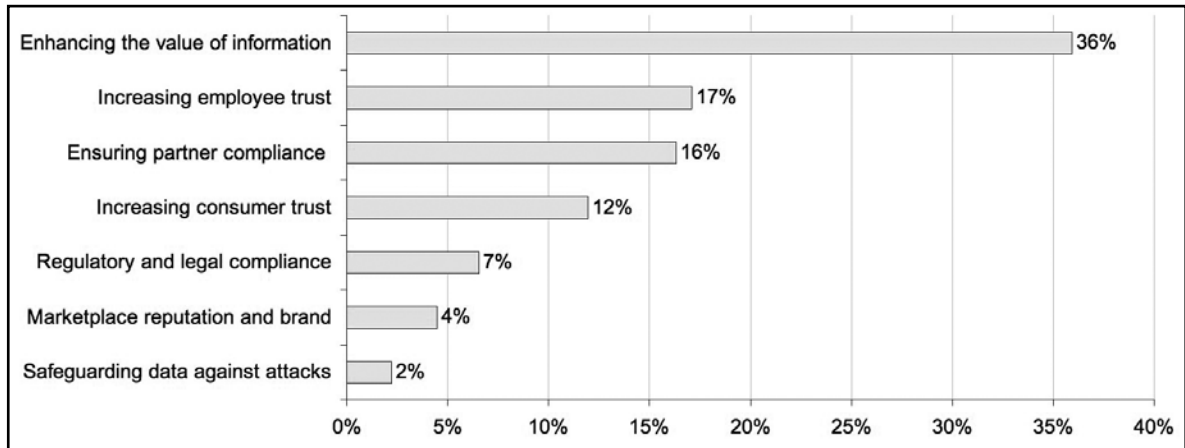
Bar Chart 15 below shows the distribution of the two highest-ranked categories combined (on a seven-point scale). The highest priorities include regulatory and legal compliance (83%), safeguarding data (78%), and marketplace reputation and brand (69%). It is interesting to note that increasing consumer and employee trust, and enhancing the value of information assets are relatively low priorities.

**Bar Chart 15: The two highest privacy program priorities combined**



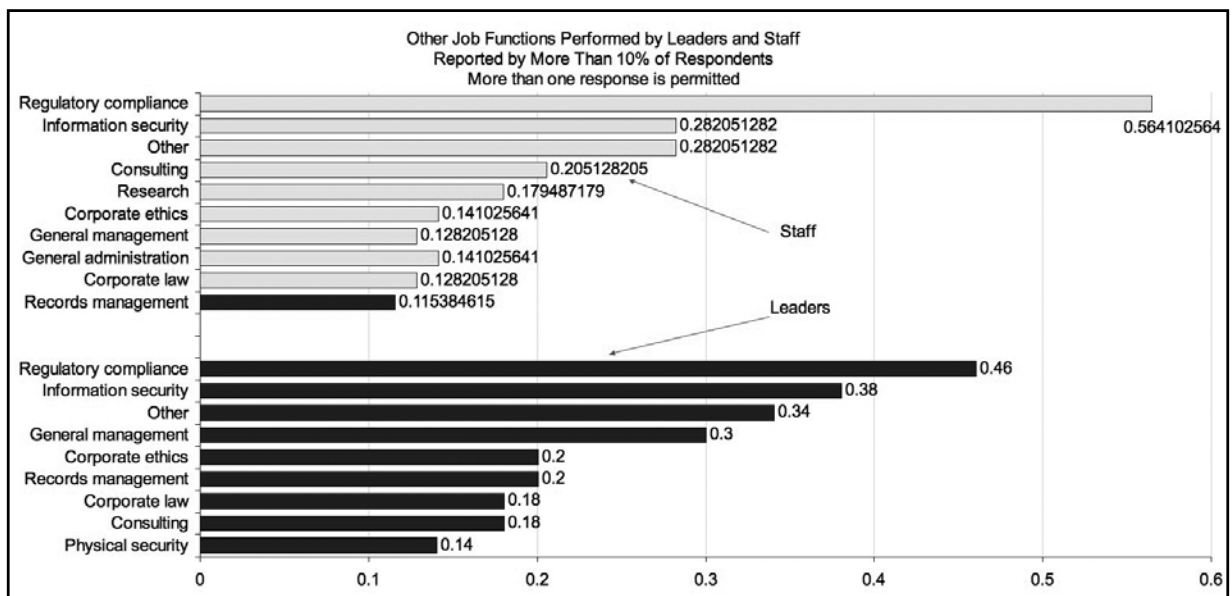
Bar Chart 16 reports the distribution of the three lowest-ranked categories combined. Enhancing the value of information assets and increasing employee trust are the lowest priorities.

**Bar Chart 16: The three lowest privacy program priorities combined**



The survey asked respondents to select the job functions that applied to their position. As shown in Bar Chart 17, both leaders and staff have responsibilities beyond the privacy role. Leaders indicated regulatory compliance (46%) and information security (38%), other (34%) and general management (30%) as the top four categories. Privacy staff participants reported regulatory compliance (56%), information security (28%), other (28%) and consulting (21%) as the top four categories.

**Bar Chart 17: Job functions of privacy leaders and staff**

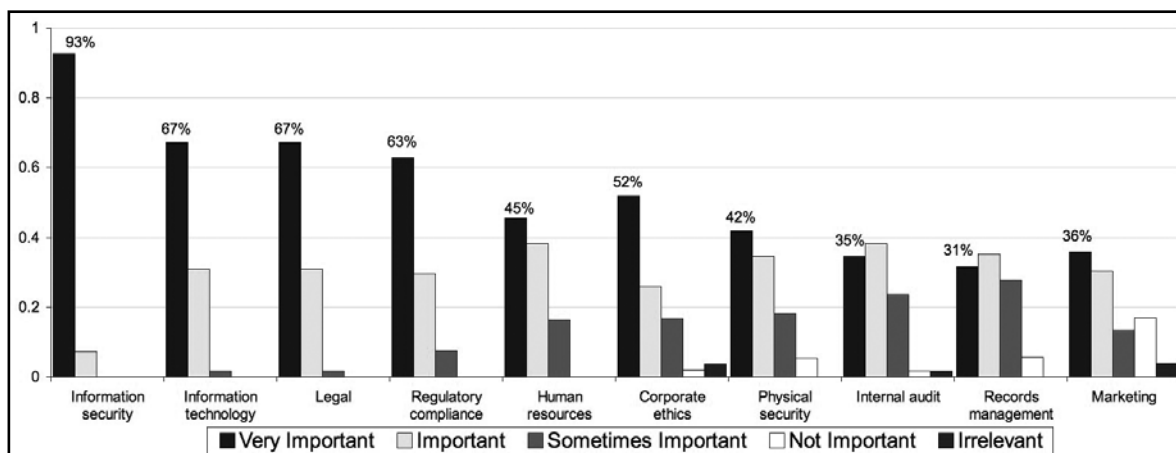


### 3. Collaboration with other functional areas

Leaders were asked to rank the importance of collaboration between privacy and 17 specified functions (plus other) on a scale of one (very important) to five (irrelevant). The top ten categories based on percent of very important and important responses are shown in Bar Chart 18. Respondents reported collaboration with Information Security at very important or important at 100% followed closely by information technology (98%), legal (98%) and regulatory compliance (93%).

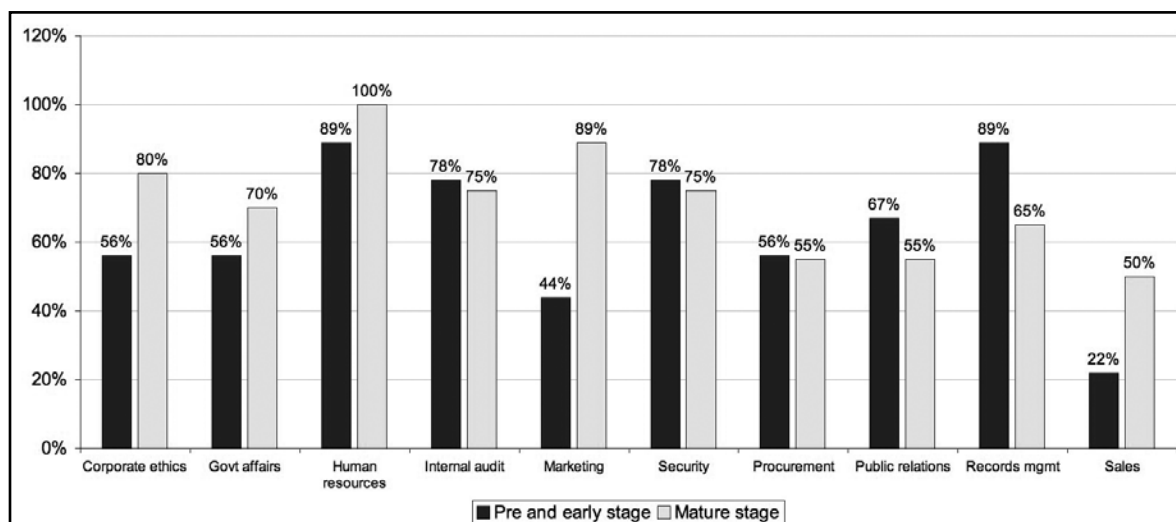
The importance (defined as very important or important) of collaboration is high across all maturity levels for Information Technology (100%) Information Security (95%-100%), Legal (95%-100%) and Regulatory Compliance (86%-100%).

**Bar Chart 18: Importance of collaboration between privacy and other functions**



Bar Chart 19 shows the importance of collaboration across 10 functional areas for pre- and early-stage versus mature-stage companies. Accordingly, pre- and early-stage programs are most interested in collaboration with functions you might expect to see – human resources, internal audit, physical security, and records management. In contrast, mature programs place higher importance on those categories and have the most interest of all levels in government affairs, marketing and sales, likely indicating a more strategic governance orientation across the enterprise.

**Bar Chart 19: Collaboration at different stages of maturity**

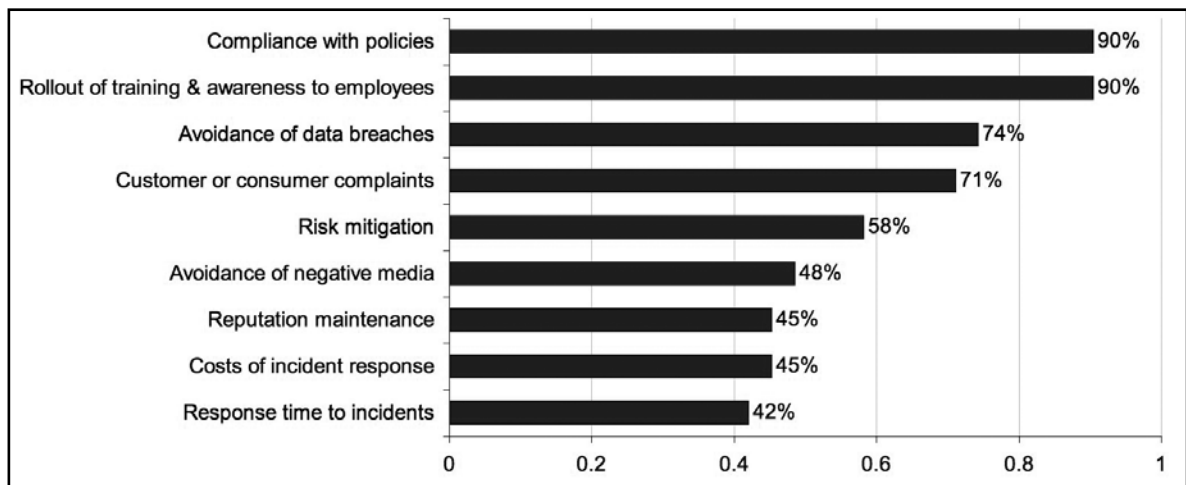


#### 4. Measurements of success in meeting objectives

Fifty-five percent of leaders reported their organization takes steps to measure the privacy program's performance (i.e., success or failure) in meeting its objectives. From a list of 20 items these respondents were asked what measures were used to evaluate performance.

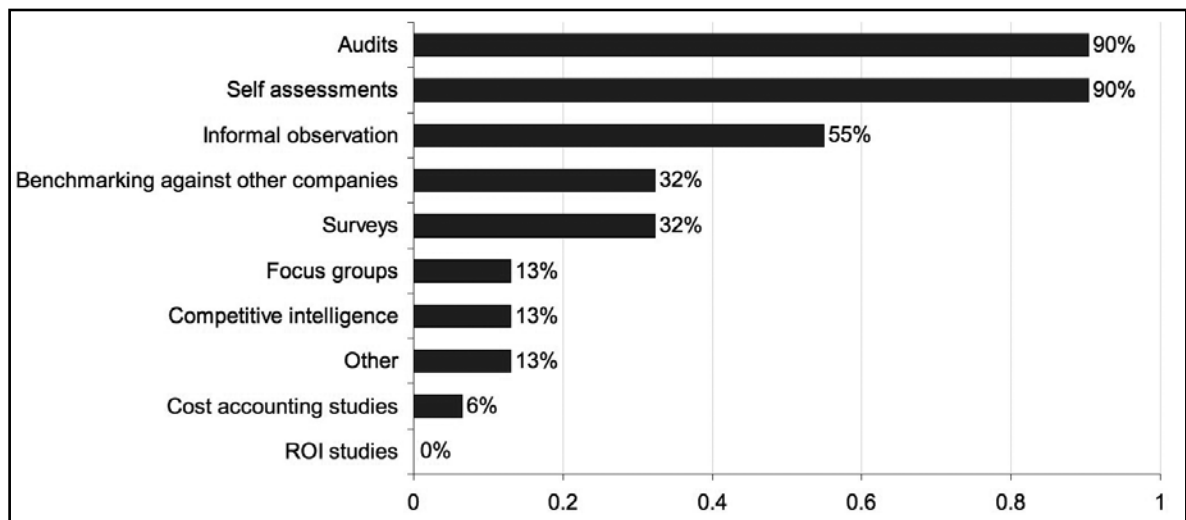
As shown in Bar Chart 20, compliance with policies (90%), rollout of training/awareness with employees (90%), avoidance of data breaches (74%), customer or consumer complaints (71%) and risk mitigation (58%) are the most common measurement domains. Less than 50% of respondents selected reputation maintenance and incident response.

**Bar Chart 20: Privacy program areas that organizations attempt to measure**



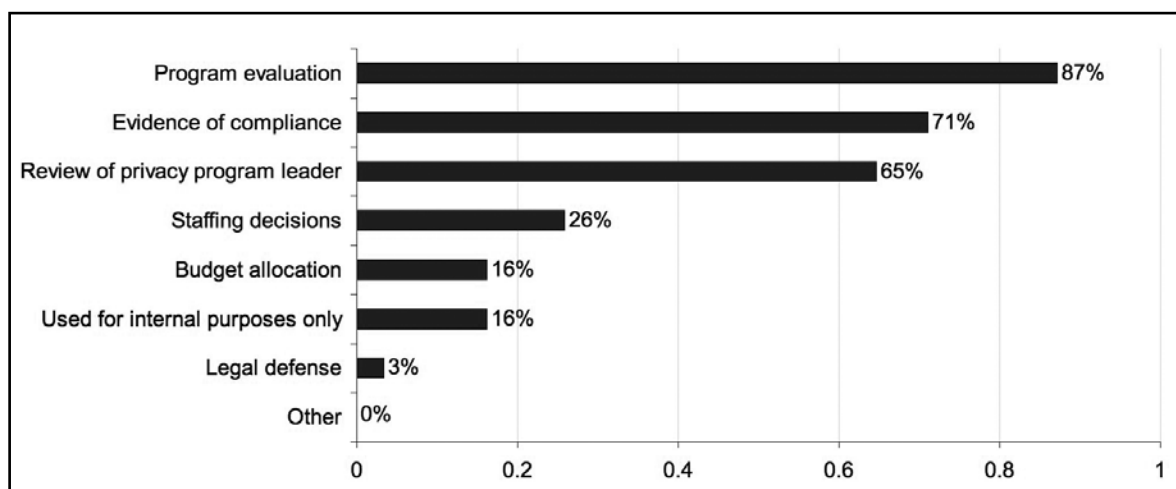
Respondents also were provided a list of 10 items and then asked to check any that described how they go about measuring program effectiveness. As shown in Bar Chart 21, self assessments and audits were the two top measurement approaches at 90%, followed by informal observation at 55%. Only 32% of companies stated they utilize benchmarks against other companies or take surveys to determine the program's performance.

**Bar Chart 21: Privacy program measurements**



Respondents were provided a list of eight items and then asked to check any that applied to how the measurement information is used in their organization. As shown in Bar Chart 22, program evaluation is the top measurement at 87% followed by evidence of compliance at 71% and the top-down review of the privacy program's leader at 65%. Surprisingly, only 26% of respondents state program measures are used to evaluate staffing and 16% state measures are used to justify budget allocation.

**Bar Chart 22: Uses for privacy program measurements**

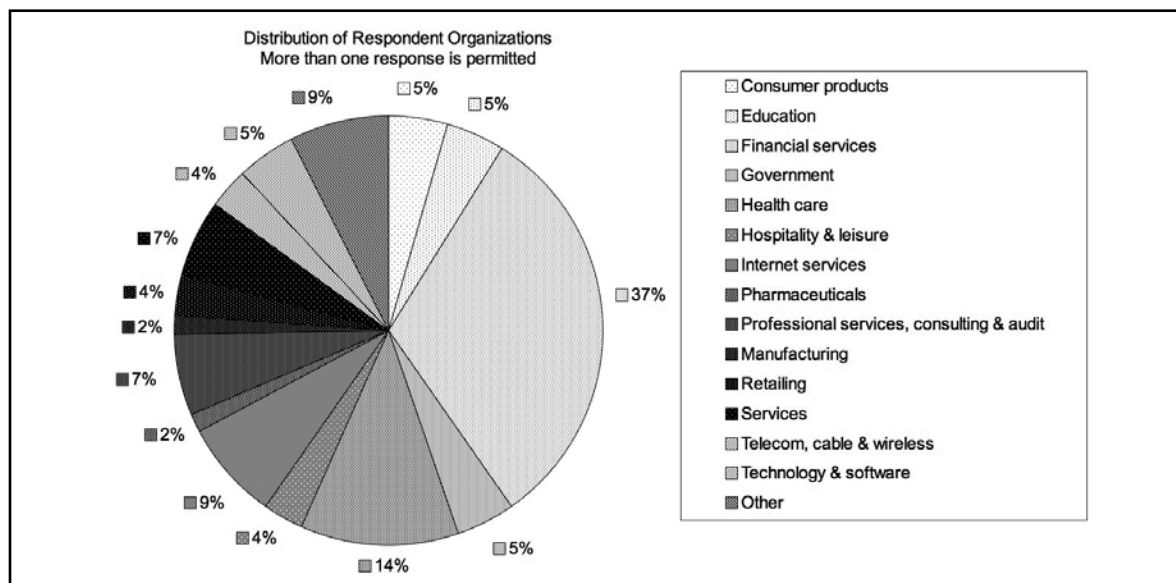


An organizational size analysis indicated that larger companies (over \$10 billion in revenue) are more likely to measure their privacy program's performance, followed by mid-size (over \$1 billion to \$10 billion) and smaller companies (less than \$1 billion). The yes responses were 73%, 57% and 27% respectively.

## 5. Organizational demographics

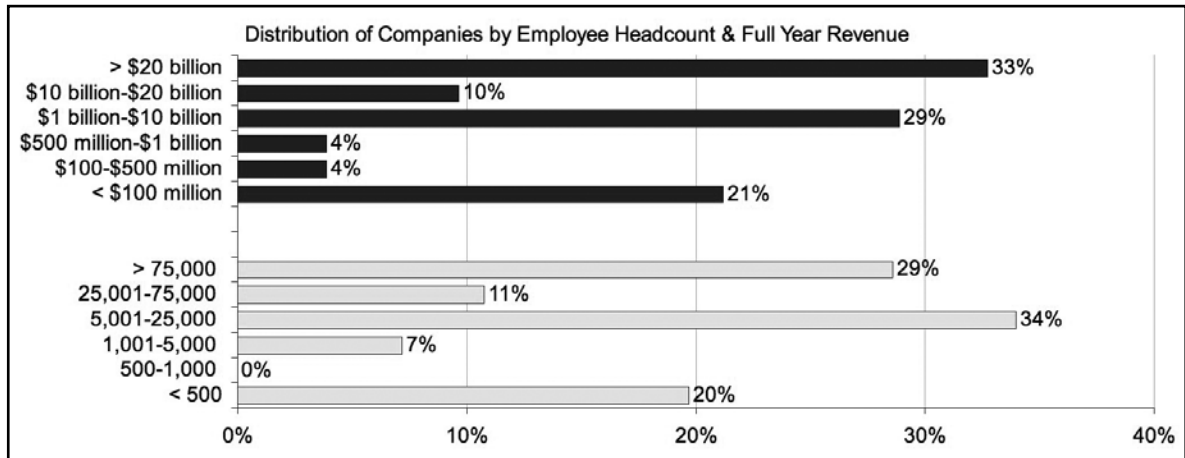
This section provides a description of the companies where the leaders are employed. Sixty-two percent of respondents work for publicly traded companies and 38% work for private companies (not shown). The pie chart below shows the respondents by their primary industry sector. The largest percentage of respondents (37%) is employed in the financial services industry. Fourteen percent work in health care and 9% are in Internet Services. The remaining 40% work in a variety of industries.

**Pie Chart 1: Industry distribution**



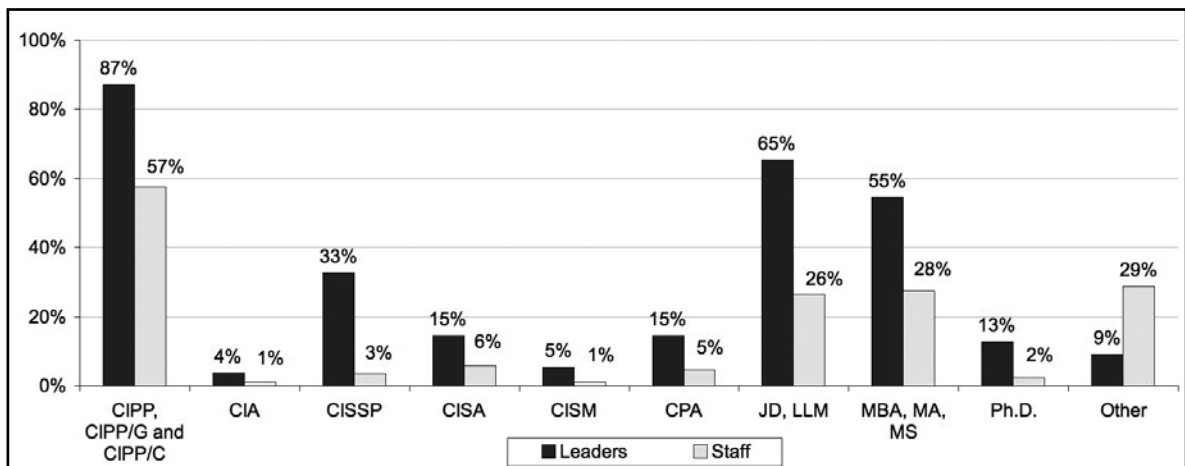
The size of the respondents' companies varies by headcount and revenue. As shown in Bar Chart 23, 21% of respondents indicated their company revenue was below \$100 million and 20% reported they had fewer than 500 employees. Similarly, 33% of respondents indicated revenue of more than \$20 billion and 29% reported headcount of more than 75,000 employees.

**Bar Chart 23: Distribution by company size**



Privacy leaders reported on total credentials and certifications held within their organization while staff reported their personal credentials and certifications. As shown in Bar Chart 24, the privacy organizations in total and staff personally hold substantial credentials.

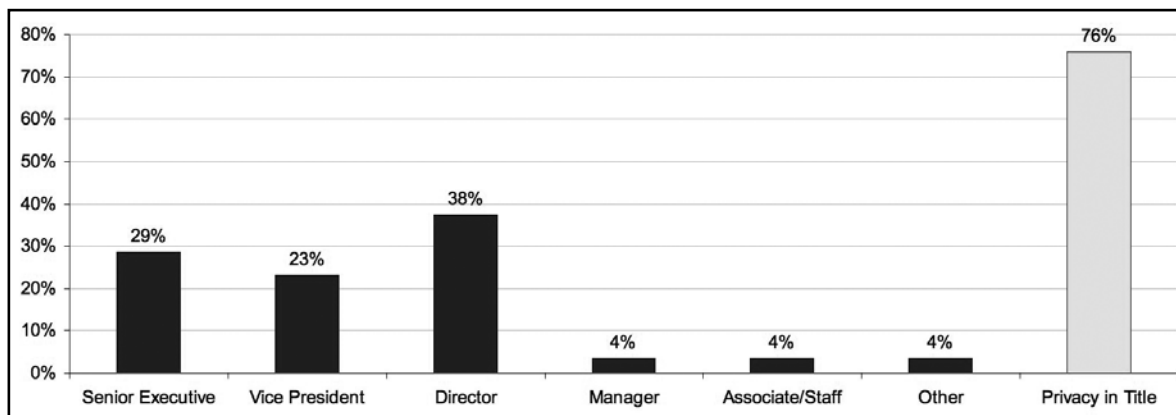
**Bar Chart 24: Credentials and certifications**





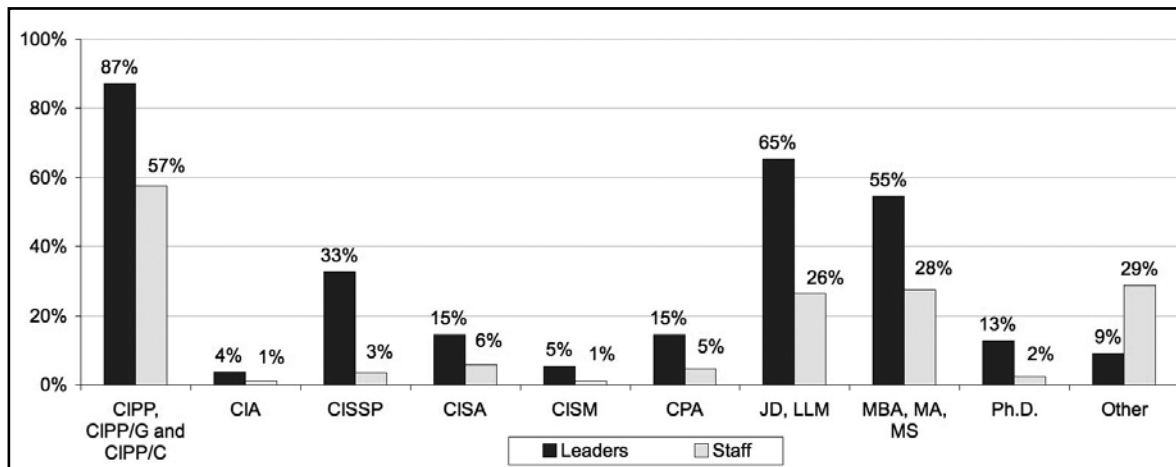
Bar Chart 25 shows the distribution of the leaders by organizational level. Eighty-nine percent of leaders reported that they were director level or higher and 76% had privacy in their title.

**Bar Chart 25: Privacy leader's organizational level**



Staff respondents were asked to provide their titles. As reported in Bar Chart 26, 59% of staff respondents had the word privacy in their title while 41% did not. By position, 23% reported they were managers, 17% were directors, 13% had a legal reference and 12% reported consultant; 21% of respondents had a mix of other titles.

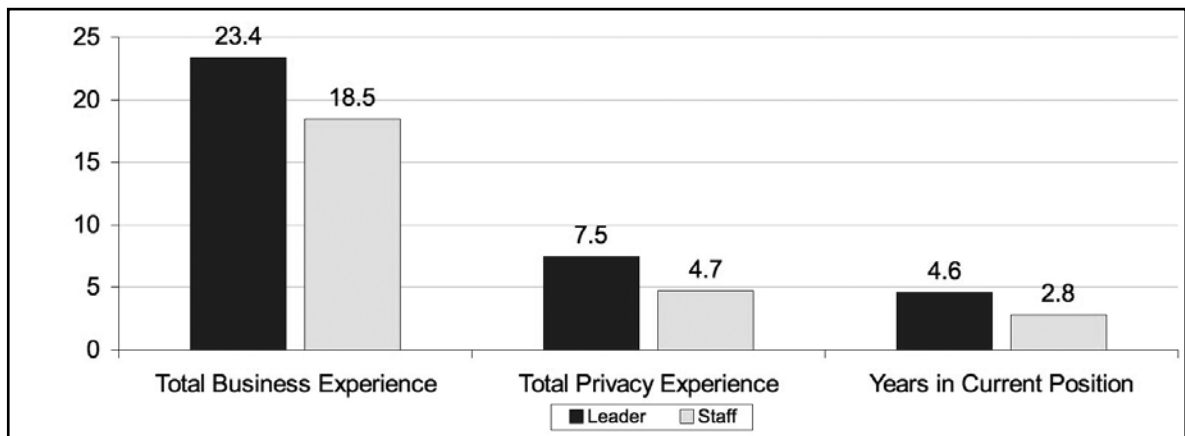
**Bar Chart 26: Privacy staff's organizational level and title**



Among respondents, leaders are evenly split between male and female at 50% each while staff reported gender at 63% female and 37% male. In addition, 93% of the leaders and 99% of respondents indicated the job was full-time (Not shown.)

Bar Chart 27 shows the level of experience of the respondents. The leaders average 23.4 years of business experience, 7.5 years of privacy experience and have been in their present job 4.6 years. On average, staff respondents reported 18.5 years of business, 4.7 years of privacy and 2.8 years in their current position. As shown, this experience is less than the leaders in each category. Of interest, 30% of staff report having two or less years of privacy experience and 28% report having been in their position one year or less (not shown).

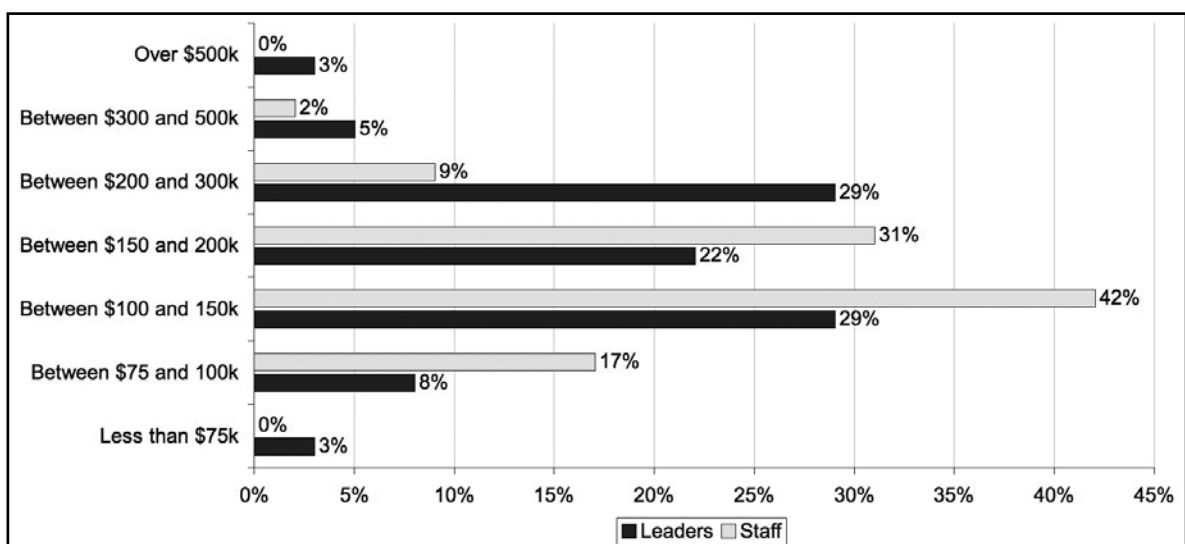
**Bar Chart 27: Experience**



An analysis of leader and staff experience level by organization size and by maturity level of privacy program showed little difference except leaders at large companies (over \$10 billion in revenue) and leaders with mature programs had approximately three-to-four years more total business experience than those of smaller companies or less mature programs.

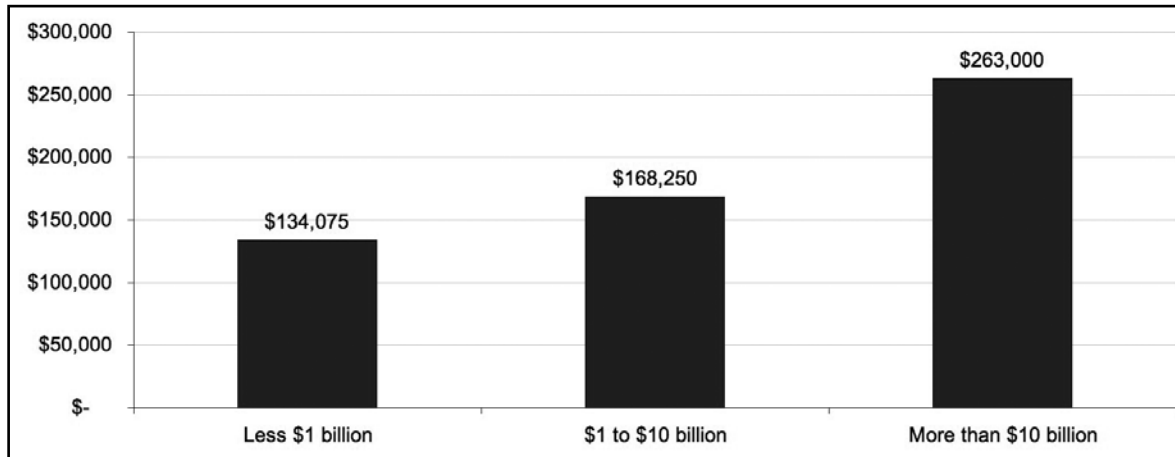
Both the leader and staff surveys asked about salary and what affects salary. Bar Chart 28 shows the salary ranges reported by leaders and by staff. At 80% of respondents, leader salary was concentrated between \$100,001 and \$300,000 while 59% of staff reported salary between \$75,000 and \$150,000.

**Bar Chart 28: Salary range for privacy leaders and staff members**



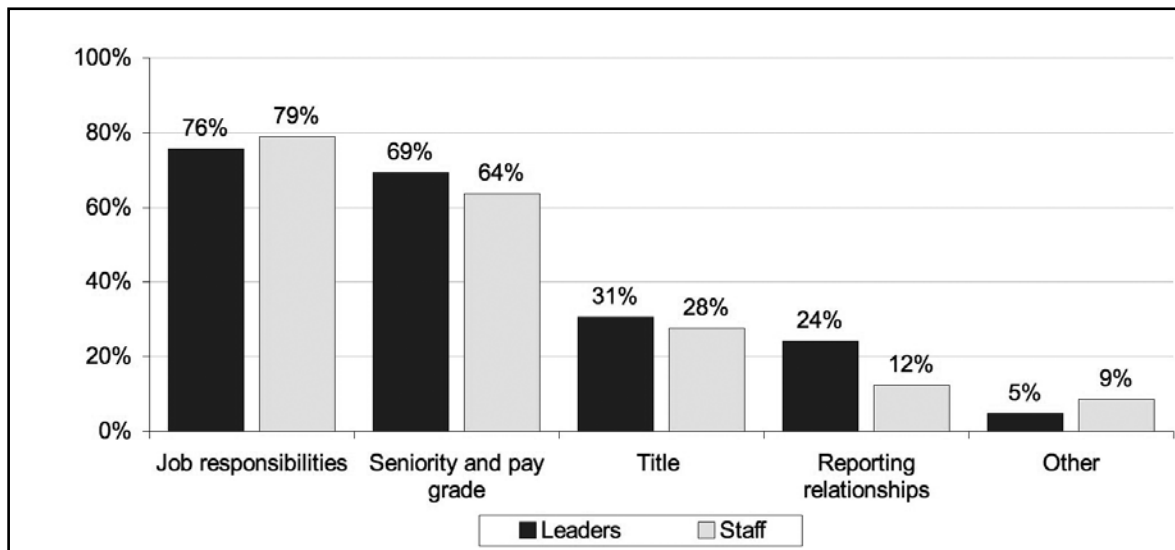
As shown in Bar Chart 29, organizational size affects the distribution of median salary ranges of leaders with larger companies generally at higher salary levels than midsize or smaller companies. The median value was computed from the value of seven income ranges provided in survey question 26.

**Bar Chart 29: Median salary levels of privacy leaders by organizational size (revenues)**



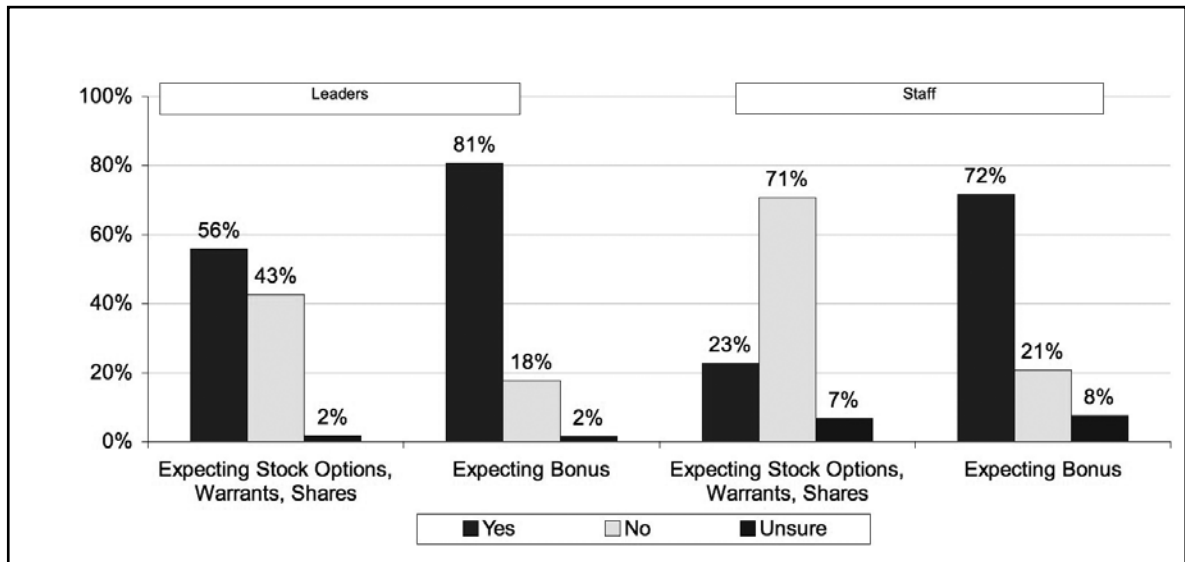
Leaders and staff were asked what they believed helped to determine their salaries. As shown in Bar Chart 30, leaders and staff responded that job responsibilities were the top determinant followed by seniority and pay grade.

**Bar Chart 30: Salary determinants**



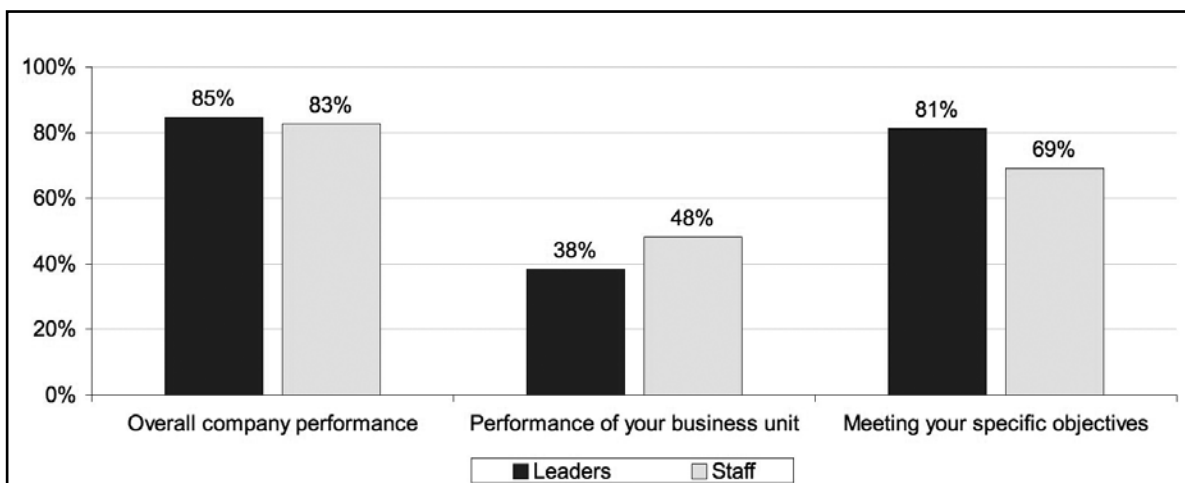
At the time of the survey, 81% of leaders and 72% of staff were expecting a bonus while only 56% of leaders and 23% of staff were expecting stock options, warrants or shares (Bar Chart 31).

**Bar Chart 31: Expectation of performance-based compensation**



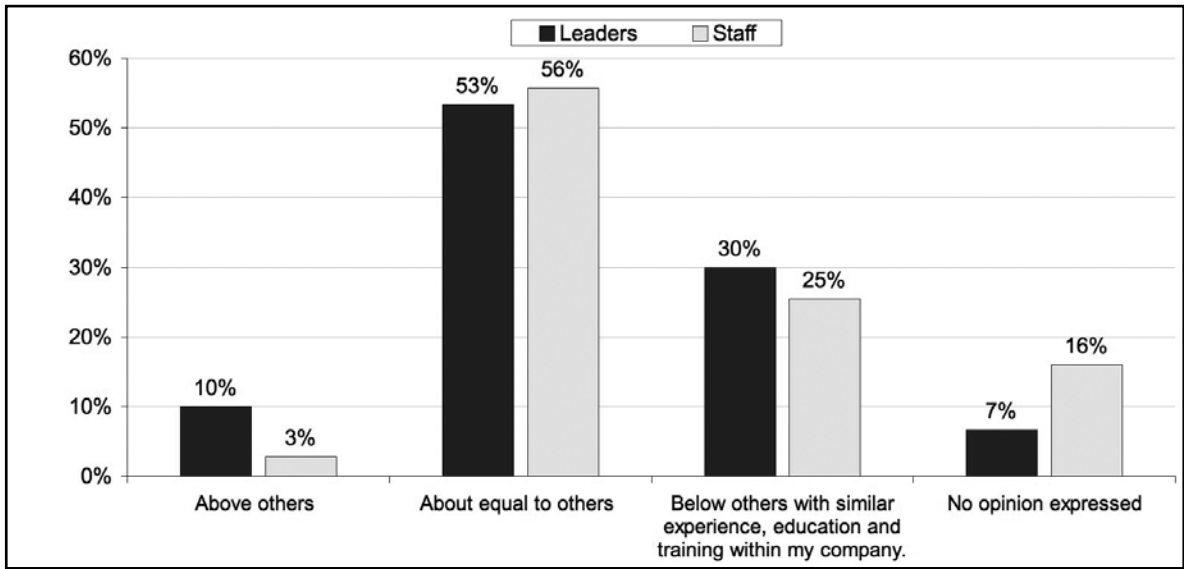
Leaders and staff also were asked what was most likely to determine their bonuses. Both leaders and staff selected overall company performance as the prime determinant at 85% and 83%, respectively, followed by meeting their specific objectives at 75% and 69%, respectively (Bar Chart 32).

**Bar Chart 32: Most likely determinants of a bonus**



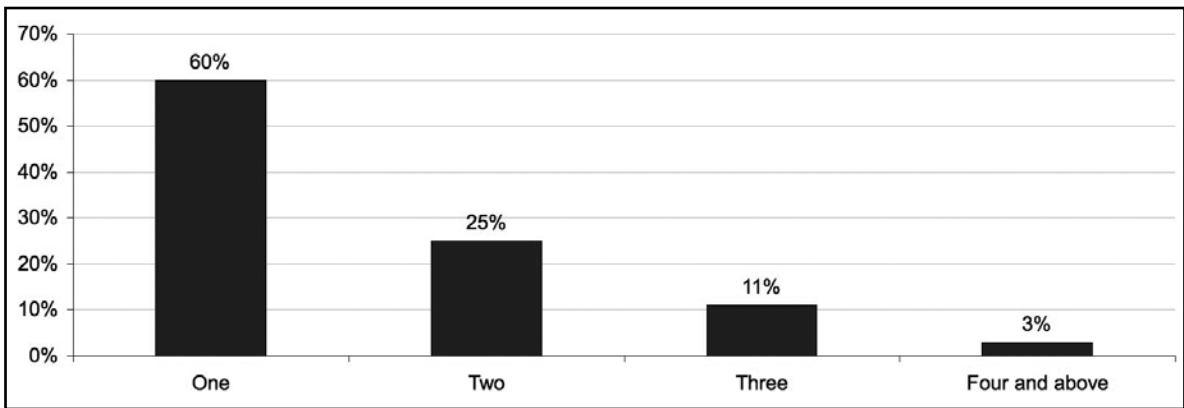
As shown in Bar Chart 33, 63% of leaders and 59% of staff believe their compensation is above or about equal to others while 30% of leaders and 25% of staff reported their compensation is below others with similar experience, education and training.

Bar Chart 33: Perceived fairness of compensation



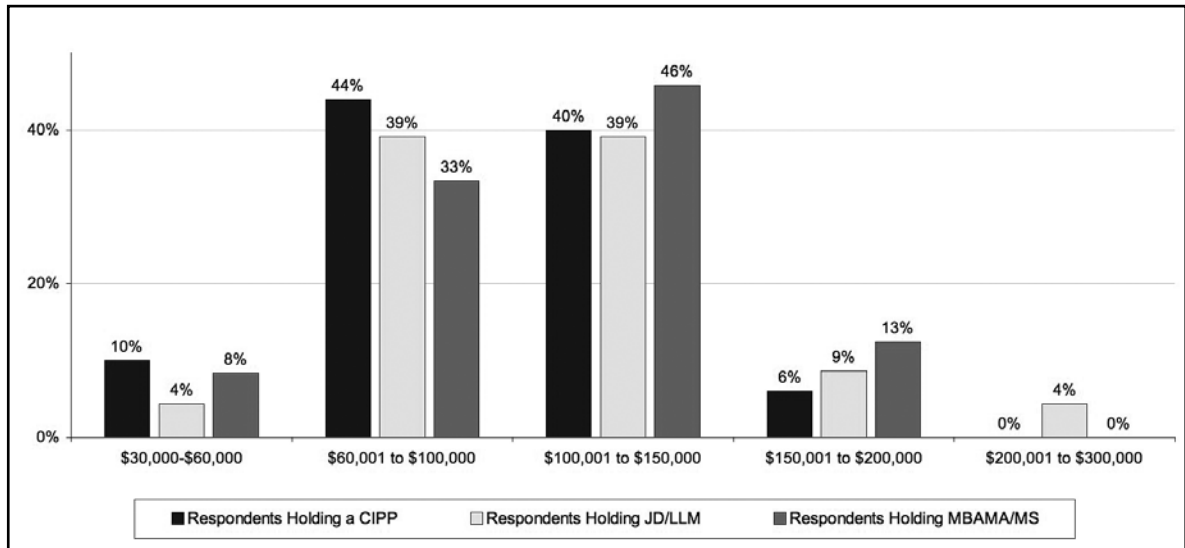
Female leaders seem to be more likely than male leaders to believe their compensation is about equal to others in their company with comparable education and experience – 58% compared with 48%. In contrast, female staff members are less likely than male staff members to believe their compensation is about equal to others in their company with comparable education and experience -- 52% compared with 62%. Staff also reported any credentials or certifications that they held. As shown, 60% of staff had one credential/certification, 25% had two, and 11% had three while 3% had four (Bar Chart 34).

Bar Chart 34: Credentials and certifications



Additionally, staff salary was correlated with credentials/certifications as shown below. As shown in Bar Chart 35, staff in the two most common salaries ranges (\$60,001 to \$150,000 represents 73% of staff respondents) hold multiple credentials or certifications including a CIPP designation.

**Bar Chart 35: Income range based on credentials**



# Appendix: Privacy Leaders and Staff Audited Survey Results

Following are the audited results of a survey involving 62 Privacy Leaders and 106 Staff from organizations located primarily in the United States. These results are presented in a percentage frequency format. Pct% = only one choice permitted. Total% = two or more choices permitted.

## Privacy Leader Responses

<b>Q1.</b>	<b>Your current title (contextual response)</b>	
<b>Q2.</b>	<b>What organizational level best describes your current position?</b>	<b>Pct%</b>
	Senior Executive	29%
	Vice President	23%
	Director	38%
	Manager	4%
	Associate/Staff	4%
	Other	4%
	Total	100%
<b>Q3.</b>	<b>Is this a full-time position?</b>	<b>Pct%</b>
	Yes	93%
	No	7%
	Total	100%
<b>Q4.</b>	<b>Check the primary person you report to:</b>	<b>Pct%</b>
	CEO/Executive Committee	18%
	Chief Financial Officer	2%
	General Counsel	19%
	Chief Information Officer	11%
	Compliance/Ethics Officer	19%
	Chief Marketing Officer/VP	0%
	Human Resources VP	0%
	Chief Security Officer	2%
	Chief Risk Officer	11%
	Other	19%
	Total	100%
<b>Q5.</b>	<b>In your organization, how many reporting layers or levels are there between the privacy leader and the CEO (or highest ranking executive)?</b>	<b>Pct%</b>
	One level (direct report)	16%
	Two levels	45%
	Three levels	27%
	Four levels	11%
	Five levels	0%
	Six levels	2%
	Seven or more levels	0%
	Total	100%

<b>Q6a.</b>	<b>What is your total business experience in years? (Average/Median)</b>	23.4/23.5
<b>Q6b.</b>	<b>What is your total privacy experience in years? (Average/Median)</b>	7.5/8.0
<b>Q6c.</b>	<b>How many years have you held your present position? (Average/Median)</b>	4.6/3.0
<b>Q7.</b>	<b>Gender</b>	<b>Pct%</b>
	Female	50%
	Male	50%
	Total	100%
<b>Q8.</b>	<b>In addition to privacy-related responsibilities, what other job functions do you perform in your organization? Please check all that apply.</b>	<b>Total%</b>
	Corporate ethics	20%
	Corporate law	18%
	Corporate marketing and CRM	8%
	Consulting	18%
	General administration	10%
	General management	30%
	Governmental relations	10%
	Human resources	4%
	Information security	38%
	IT operations	8%
	Internal audit	2%
	Physical security	14%
	Public relations	8%
	Research	4%
	Regulatory compliance	46%
	Records management	20%
	Software development	2%
	Database administration	4%
	Other	28%
	Total	292%



<b>Q9.</b>	<b>What is the industry or business group that best defines your organization? If your organization contains multiple industry sectors or sub-checks, please check all that apply (or write in the space for other).</b>	<b>Total%</b>
	Consumer products	5%
	Education	5%
	Energy	0%
	Financial services	37%
	Government	5%
	Health care	14%
	Hospitality & Leisure	4%
	Internet Services	9%
	Pharmaceuticals	2%
	Professional services, consulting & audit	7%
	Professional services, legal	0%
	Manufacturing	2%
	Retailing	4%
	Services	7%
	Telecom, cable & wireless	4%
	Technology & software	5%
	Transportation	0%
	Other	9%
	Total	118%

<b>Q10.</b>	<b>Where within your organization is the privacy function located? Please select only one response.</b>	<b>Pct%</b>
	Corporate ethics	7%
	Finance & accounting	2%
	Government affairs	2%
	Human resources	0%
	Information security	9%
	Information technology	11%
	Internal audit	2%
	Marketing	2%
	Physical security	0%
	Procurement	0%
	Public relations	0%
	Records management	0%
	Regulatory compliance	23%
	Legal	29%
	Other	14%
	Total	100%

<b>Q11a. Your company has employees located in (check all that apply):</b>	<b>Total%</b>
United States	96%
Canada	51%
Europe	58%
Asia-Pacific	51%
Latin America (including Mexico)	42%
Total	298%

<b>Q11b. What is the geographical location of your privacy office?</b>	<b>Pct%</b>
United States	89%
Canada	7%
Europe	4%
Asia-Pacific	0%
Latin America (including Mexico)	0%
Total	100

<b>Q11c. What is the jurisdiction of your privacy office (check all that apply)?</b>	<b>Total%</b>
United States	96%
Canada	46%
Europe	42%
Asia-Pacific	37%
Latin America (including Mexico)	35%
Total	256%

<b>Q12. What is the worldwide headcount of your organization? Nearest 1,000 or use the following range:</b>	<b>Pct%</b>
Less than 500 people	20%
500 to 1,000 people	0%
1,001 to 5,000 people	7%
5,001 to 25,000 people	34%
25,001 to 75,000 people	11%
More than 75,000 people	29%
Total	100%

<b>Q13. Is your company publicly traded?</b>	<b>Pct%</b>
Yes, NYSE	51%
Yes, NASDAQ	8%
Yes, overseas exchange	4%
Yes, other minor exchange	0%
No	38%
Total	100%

<b>Q14.</b>	<b>2006 total revenues: Nearest \$100 million or use the following range:</b>	<b>Pct%</b>
	Less than \$100 million	21%
	\$100 to \$500 million	4%
	\$500 million to \$1 billion	4%
	\$1 billion to \$10 billion	29%
	\$10 billion to \$20 billion	10%
	More than \$20 billion	33%
	Total	100%
<b>Q15.</b>	<b>Please check the maturity stage of your company's privacy program. Select the one that in your opinion best describes the activities associated with your company's current privacy office or initiatives.</b>	<b>Pct%</b>
	Pre stage – Privacy program has not been established as a unit within the company.	5%
	Early stage – Privacy program is just starting to become staffed and organized.	13%
	Middle stage – Privacy program is in existence and is starting to launch key initiatives.	27%
	Late Middle Stage – Privacy program is starting to evaluate the effectiveness of key initiatives.	18%
	Mature Stage – Privacy program is in maintenance mode focusing on program evaluation and refinement.	36%
	Total	100%
<b>Q16a.</b>	<b>How many employees are dedicated full time to your organization's privacy program? Nearest whole number or use the following range:</b>	<b>Pct%</b>
	0	22%
	1	19%
	2 to 4	30%
	5 to 10	22%
	11 to 20	4%
	More than 20	4%
	Total	100%
<b>Q16b.</b>	<b>Are any of the above full-time employees hired on a contract or temporary basis?</b>	<b>Pct%</b>
	Yes	13%
	No	87%
	Total	100%
<b>Q16c.</b>	<b>Do you anticipate full-time headcount changes in fiscal 2008?</b>	<b>Pct%</b>
	Yes, it will increase	29%
	Yes, it will decrease	4%
	No, it will stay the same	68%
	Total	100%

<b>Q16d. How often does the core privacy team meet (conference call or in-person)?</b>	<b>Pct%</b>
Daily	17%
Weekly	50%
Monthly	17%
Quarterly	7%
Semi-annually	2%
Annually	0%
Never	7%
Total	100%

<b>Q17a. How many employees are dedicated part-time to your organization's privacy program? Nearest whole number or use the following range:</b>	<b>Pct%</b>
0	42%
1	15%
2 to 4	11%
5 to 10	16%
11 to 20	7%
More than 20	9%
Total	100%

<b>Q17b. Are any of the above part-time employees hired on a contract or temporary basis?</b>	<b>Pct%</b>
Yes	12%
No	88%
Total	100%

<b>Q17c. Do you anticipate part-time headcount changes in fiscal 2008?</b>	<b>Pct%</b>
Yes, it will increase	15%
Yes, it will decrease	6%
No, it will stay the same	80%
Total	100%

<b>Q18a. Do you use a privacy liaison function (a.k.a. privacy coordinator) to manage privacy in your organization (note that the privacy liaison has responsibility for privacy but is not part of the core privacy function)?</b>	<b>Pct%</b>
Yes	55%
No	45%
Total	100%

<b>Q18b. If yes, how are they assigned (please check all that apply)?</b>	<b>Total%</b>
By region	17%
By country	17%
By subsidiary	23%
By business function (i.e., marketing, IT)	73%
Other	17%
Total	147%
<b>Q18c. Do you have authority concerning the role, status or compensation of privacy liaisons? If so, please check all that apply.</b>	<b>Total%</b>
Salary	0%
Bonus recommendations	10%
Performance review	20%
Job description or title	30%
Training	43%
No influence	47%
Total	160%
<b>Q18d. Do privacy liaisons receive annual privacy training?</b>	<b>Pct%</b>
Yes	77%
No	23%
Total	100%
<b>Q18e. Do you require privacy liaisons to have specific requirements?</b>	<b>Pct%</b>
Yes	45%
No	55%
Total	100%
<b>Q18f. How often does the core privacy team meet with privacy liaisons (by phone or in-person)?</b>	<b>Pct%</b>
Daily	0%
Weekly	7%
Monthly	37%
Quarterly	33%
Semi-annually	11%
Annually	4%
Never	7%
Total	100%

<b>Q19.</b>	<b>For the following certifications and credentials, please indicate the <i>total number</i> of credentials held by your organization's full- and part-time employees who work in your privacy program.</b>	<b>Total%</b>
	CIPP, CIPP/G and CIPP/C	87%
	CIA	4%
	CISSP	33%
	CISA	15%
	CISM	5%
	CPA	15%
	JD, LLM	65%
	MBA, MA, MS	55%
	Ph.D.	13%
	Other	9%
	Total	300%
<b>Q20.</b>	<b>What is the total budget for the privacy function? Please allocate the approximate <i>percentage</i> of budget to the following activities. The total allocation must equal 100%.</b>	<b>Pct%</b>
	Salary and benefits	56%
	General overhead and administration	5%
	Development and training for staff	3%
	Organization awareness and training	3%
	Communications	2%
	Monitoring	2%
	Audits	2%
	Policies, procedures and governance	5%
	Data inventory and mapping	1%
	Subscriptions and publications	1%
	Software or technology	3%
	Meetings with regulators	1%
	Incident response	2%
	Technologies	2%
	Outside consultants	4%
	Legal counsel	4%
	Vendor management	1%
	Web certification and seals	1%
	Redress and consumer outreach	1%
	Other	1%
	Total (must sum to 100%)	100%

<b>Q21.</b>	<b>Approximately what is the total external budget for your organization's privacy program (dollars paid for the activities listed in Q20)? Please enter to the nearest \$200,000 or use the following range:</b>	<b>Pct%</b>
	Less than \$100,000	18%
	Between \$100,000 to \$250,000	13%
	Above \$250,000 to \$500,000	10%
	Above \$500,000 to \$1 million	26%
	Above \$1 million to \$2.5 million	23%
	Above \$2.5 million to \$5 million	8%
	Above \$5 million to \$10 million	3%
	Over \$10 million	0%
	Total	100%
<b>Q22.</b>	<b>Do you anticipate any charges to the total privacy program budget in fiscal 2008?</b>	<b>Pct%</b>
	Yes, the budget is expected to increase	19%
	Yes, the budget is expected to decrease	13%
	No, budget is expected to stay the same	67%
	Total	100%
<b>Q23a.</b>	<b>What types of information are you required to safeguard in your privacy program (please check all that apply)?</b>	<b>Total%</b>
	Customer or consumer (citizen) information	91%
	Business customer information	84%
	Employee information	95%
	Non-personal, business confidential information	55%
	Other data (including intellectual property)	36%
	Total	361%
<b>Q23b.</b>	<b>What types of information are you required to provide in connection with privacy policies, procedures and other forms of guidance to business units within your organization?</b>	<b>Total%</b>
	Customer or consumer (citizen) information	88%
	Business customer information	78%
	Employee information	78%
	Non-personal, business confidential information	48%
	Other data (including intellectual property)	24%
	Total	316%

- Q24. Following is a list of typical priorities for a privacy program. Please rank these priorities from: 1 = highest to 7 = lowest for your organization. Do not assign any rank for a priority that is not applicable to your organization.**

	Pct%							
	1	2	3	4	5	6	7	Total
Increasing consumer trust	52%	14%	7%	14%	7%	5%	0%	100%
Increasing employee trust	17%	22%	20%	24%	5%	12%	0%	100%
Ensuring business partner compliance (including outsourcers)	26%	30%	14%	14%	12%	2%	2%	100%
Marketplace reputation and brand	51%	18%	16%	11%	2%	0%	2%	100%
Regulatory and legal compliance	65%	17%	7%	4%	4%	2%	0%	100%
Safeguarding data against attacks and threats	54%	24%	11%	9%	0%	2%	0%	100%
Enhancing the value of information assets	10%	18%	18%	18%	8%	15%	13%	100%

- Q25. For the priorities listed above, how important is collaboration between privacy and other functions within your organization? Please use the following scale to indicate the importance of working together to achieve privacy goals: 1 = Very important, 2 = important, 3 = sometimes important, 4 = not important, 5 = irrelevant**

	Pct%					
	1	2	3	4	5	Total
Corporate ethics	52%	26%	17%	2%	4%	100%
Finance & accounting	5%	31%	40%	18%	5%	100%
Government affairs	20%	40%	27%	11%	2%	100%
Human resources	45%	38%	16%	0%	0%	100%
Information security	93%	7%	0%	0%	0%	100%
Information technology	67%	31%	2%	0%	0%	100%
Internal audit	35%	38%	24%	2%	2%	100%
Legal	67%	31%	2%	0%	0%	100%
Marketing	36%	30%	13%	17%	4%	100%
Mergers & acquisitions	6%	28%	38%	6%	23%	100%
Physical security	42%	35%	18%	5%	0%	100%
Procurement	18%	35%	31%	11%	5%	100%
Public relations	22%	36%	31%	9%	2%	100%
Records management	31%	35%	28%	6%	0%	100%
Regulatory compliance	63%	30%	7%	0%	0%	100%
Sales	17%	17%	38%	15%	12%	100%
Supply chain & logistics	6%	16%	35%	22%	22%	100%
Other (please specify)	50%	0%	0%	0%	50%	100%



<b>Q26.</b>	<b>Your current annual salary (base pay) expressed in U.S. dollars is (please enter to the nearest \$1,000 or use the following range):</b>	<b>Pct%</b>
	Less than \$75,000	3%
	Between \$75,001 and \$100,000	8%
	Between \$100,001 and \$150,000	29%
	Between \$150,001 and 200,000	22%
	Between \$200,001 and \$300,000	29%
	Between \$300,001 and \$500,000	5%
	Over \$500,000	3%
	Total	100%
<b>Q27.</b>	<b>Your salary is based upon (please check all that apply):</b>	<b>Total%</b>
	Seniority and pay grade	69%
	Job responsibilities	76%
	Reporting relationships	24%
	Title	31%
	Other	5%
	Total	205%
<b>Q28a.</b>	<b>Do you expect to receive stock options, warrants or shares in 2008?</b>	<b>Pct%</b>
	Yes	56%
	No	43%
	Unsure	2%
	Total	100%
<b>Q28b.</b>	<b>Do you expect to receive a bonus as part of your annual compensation in 2008?</b>	<b>Pct%</b>
	Yes	81%
	No	18%
	Unsure	2%
	Total	100%
<b>Q29.</b>	<b>If you responded yes to Q28 a or b, please check the one or more items that will most likely determine your bonus in 2008:</b>	<b>Total%</b>
	Overall company performance	85%
	Performance in your business unit	38%
	Meeting your specific objectives	75%
	Total	198%

<b>Q30.</b>	<b>Please express your belief about your compensation relative to others within your company. My compensation is:</b>	<b>Pct%</b>
	Above others with similar experience, education and training within my company.	10%
	About equal to others with similar experience, education and training within my company	53%
	Below others with similar experience, education and training within my company	30%
	I do not want to express my opinion.	7%
	Total	100%
<b>Q31.</b>	<b>Does your organization attempt to measure the privacy program's success in meeting its objectives?</b>	<b>Pct%</b>
	Yes	55%
	No	45%
	Total	100%
<b>Q32.</b>	<b>If yes, what areas do you attempt to measure?</b>	<b>Total%</b>
	Compliance with policies	90%
	Risk mitigation	58%
	Avoidance of inside threats	19%
	Avoidance of external threats	16%
	Customer or consumer complaints	71%
	Customer churn or turnover	13%
	Customer or consumer awareness	23%
	Employee complaints	39%
	Avoidance of data breaches	74%
	Rollout of training and awareness to employees	90%
	Professional certification of staff	23%
	Implementation of enabling technologies	35%
	Management of budget costs	29%
	Reputation maintenance	45%
	Enforcement of vendor contracts	35%
	Costs of incident response	45%
	Response time to incidents	42%
	Avoidance of negative media	48%
	Positive media coverage	26%
	Other	3%
	Total	826%

<b>Q33.</b>	<b>If yes, how do you go about measuring the areas listed above?</b>	<b>Total%</b>
	Surveys	32%
	Focus groups	13%
	Audits	90%
	Self assessments	90%
	Cost accounting studies	6%
	Informal observation	55%
	Benchmarking against other companies	32%
	Competitive intelligence	13%
	ROI studies	0%
	Other	13%
	Total	345%

<b>Q34.</b>	<b>If yes, how is this information used?</b>	<b>Total%</b>
	Program evaluation	87%
	Budget allocations	16%
	Staffing decisions	26%
	Legal defense	3%
	Evidence of compliance	71%
	Review of privacy program leader or CPO	65%
	Used for internal purposes only	16%
	Other	0%
	Total	284%

## Privacy Staff Survey Responses

<b>Q1.</b>	<b>Your current title (contextual response)</b>	
<b>Q2.</b>	<b>Is this a full time position?</b>	<b>Pct%</b>
	Yes	99%
	No	1%
		100%
<b>Q3a.</b>	<b>What is your total business experience in years? (Average/Median)</b>	18.5/17.5
<b>Q3b.</b>	<b>What is your total privacy experience in years? (Average/Median)</b>	4.7/4.0
<b>Q3c.</b>	<b>How many years have you held your present position? (Average/Median)</b>	2.8/2.0
<b>Q4.</b>	<b>Gender</b>	<b>Pct%</b>
	Female	63%
	Male	37%
		100%
<b>Q5.</b>	<b>In addition to privacy-related responsibilities, what other job functions do you perform in your organization? Please check all that apply.</b>	<b>Total%</b>
	Corporate ethics	14%
	Corporate law	13%
	Corporate marketing and CRM	6%
	Consulting	21%
	General administration	14%
	General management	13%
	Governmental relations	9%
	Human resources	6%
	Information security	28%
	IT operations	8%
	Internal audit	5%
	Physical security	10%
	Public relations	8%
	Research	18%
	Regulatory compliance	56%
	Records management	12%
	Software development	6%
	Database administration	6%
	Other	28%
	Total	282%

<b>Q6.</b>	<b>For the following certifications and credentials, please indicate the number of credentials you hold.</b>	<b>Total%</b>
	CIPP, CIPP/G and CIPP/C	57%
	CIA	1%
	CISSP	3%
	CISA	6%
	CISM	1%
	CPA	5%
	JD, LLM	26%
	MBA, MA, MS	28%
	Ph.D.	2%
	Other	29%
	Total	159%
<b>Q7.</b>	<b>Your current annual salary (base pay) expressed in U.S. dollars is (please enter to the nearest \$1,000 or use the following range):</b>	<b>Pct%</b>
	Less than \$30,000	0%
	Between \$30,001 to \$60,000	17%
	Between \$60,001 to \$100,000	42%
	Between \$100,001 to 150,000	31%
	Between \$150,001 to \$200,000	9%
	Over \$200,001 to \$300,000	2%
	Over \$300,000	0%
	Total	100%
<b>Q8.</b>	<b>Your salary is based upon (please check all that apply):</b>	<b>Total%</b>
	Seniority and pay grade	64%
	Job responsibilities	79%
	Reporting relationships	12%
	Title	28%
	Other	9%
	Total	191%
<b>Q9a.</b>	<b>Do you expect to receive stock options, warrants or shares in 2008?</b>	<b>Pct%</b>
	Yes	23%
	No	71%
	Unsure	7%
	Total	100%
<b>Q9b.</b>	<b>Do you expect to receive a bonus as part of your annual compensation in 2008?</b>	<b>Pct%</b>
	Yes	72%
	No	21%
	Unsure	8%
	Total	100%

<b>Q9c.</b>	<b>If you responded yes to Q9 a or b, please check the one or more items that will most likely determine your bonus in 2008:</b>	<b>Total%</b>
	Overall company performance	83%
	Performance in your business unit	48%
	Meeting your specific objectives	69%
	Total	200%
<b>Q10.</b>	<b>Please express your belief about your compensation relative to others within your company. My compensation is:</b>	<b>Pct%</b>
	Above others with similar experience, education and training within my company.	3%
	About equal to others with similar experience, education and training within my company	56%
	Below others with similar experience, education and training within my company	25%
	I do not want to express my opinion.	16%
	Total	100%

## About the IAPP

The International Association of Privacy Professionals (IAPP) is the world's largest association of privacy professionals, representing more than 6,000 members from businesses, governments and academic institutions across 49 countries.

The IAPP was founded in 2000 with a mission to define, promote and improve the privacy profession globally. We are committed to providing a forum for privacy professionals to share best practices, track trends, advance privacy management issues, standardize the designations for privacy professionals, and provide education and guidance on opportunities in the field of information privacy.

The IAPP is responsible for developing and launching the first broad-based credentialing program in information privacy, the Certified Information Privacy Professional (CIPP). The CIPP remains the leading privacy certification for many thousands of professionals around the world who serve the data protection, information auditing, information security, legal compliance and/or risk management needs of their organizations.

In addition, the IAPP offers a full suite of educational and professional development services and holds the annual Privacy Summit, Privacy Academy and Practical Privacy Series conferences. These events are recognized internationally as the leading forums for the discussion and debate of issues related to privacy policy and practice.

## Ponemon Institute

### Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the **Council of American Survey Research Organizations (CASRO)**, we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.

Inside Back Cover (blank)

For more information, please contact us at:

---

IAPP

170 Cider Hill Road, York, Maine 03909 USA

+1 207.351.1500

[www.privacyassociation.org](http://www.privacyassociation.org)