2010

Privacy Professional's Role, Function and Salary Survey

International Association of Privacy Professionals

iapp CANADA

international association of privacy professionals

+1 207.351.1500 | www.privacyassociation.org/canada

2010 Privacy Professional's Role, Function and Salary Survey

International Association of Privacy Professionals

| *A Message from the President*

We are thrilled to offer you our first national study of the privacy profession. "The IAPP Canada Privacy Professional Role, Function and Salary Survey" examines the growth and development of the privacy profession across Canada today. It is the product of collaboration between IAPP Canada, based in Ottawa, and the Privacy and Cyber Crime Institute of Ryerson University, based in Toronto.

Whether you are an established Canadian professional or new to the privacy field this study will give you a richer understanding of where the privacy profession is headed in Canada – across both public and private sector organizations. You will find it useful in gauging your own efforts and professional value. The study is part of a growing portfolio of resources and services that the IAPP is proud to offer to our Canadian members and which we look forward to growing in the coming months and years.

Sincerely,

Nuala O'Connor Kelly, CIPP, CIPP/G
IAPP President
Chief Privacy Leader & Senior Counsel, Information Governance
General Electric Company

| Contents

| Executive Summary

IAPP Canada and the Privacy & Cyber Crime Institute at Ryerson University are pleased to present the findings of the first survey of IAPP Canada's membership. This report provides a portrait of Canada's privacy profession and is based on the results of a survey of IAPP Canada members, conducted during a three-week period in April 2010. The survey covered four major areas:

1. Salary and privacy career information.
2. Structure of current privacy positions.
3. Function and operations of privacy programs.
4. Organizational and industry considerations.

The Privacy & Cyber Crime Institute developed the survey in collaboration with the IAPP and IAPP Canada in order to provide an opportunity for comparison across borders (i.e. IAPP and Ponemon Institute's Benchmarking Privacy Report) as well as to specifically reflect the Canadian privacy reality. Ryerson University analysed the results of the anonymous and confidential survey.

This study sought to provide insight on several key questions:

1. What are the typical responsibilities performed by Canadian privacy professionals? Where does the privacy role fit within the organization?
2. What are the compensation norms within the Canadian profession? How do individual characteristics such as education, certifications, and years of experience determine compensation? What is the influence of industry, organization size, job scope and reporting relationships?
3. How is the privacy office staffed and budgeted? What are its top priorities? How does it operate with other organizational functions?
4. How is privacy program success measured?

The key findings of this research are summarised in this report. We have organised the results into four themes: who are we? (privacy careers); what is our function? (privacy roles and responsibilities); how do we operate? (privacy programs); where do we operate? (our organizations). Due to the inherent limitations of benchmarking methodology, this report focuses on description and patterns rather than statistical reliability.

Who are we? Our privacy careers.
Among respondents, the "typical" Canadian privacy professional is a 35 to 49-year-old female with post-secondary education (at least an associate or bachelor degree). She is somewhat more likely to be employed in the healthcare or government sectors as opposed to her male counterpart, who is more likely working in the consulting or financial services industries. While she has extensive work experience (10-25 years) as well as some privacy

experience (5-10 years), her previous position would not necessarily have been focussed primarily on privacy. She is working full time as a privacy manager or privacy analyst. She has held the position for two to five years. She is paid $75,000–$99,000, which she considers to be equal to her organizational peers' compensation but either equal or below the compensation of her industry peers. She expects to receive a bonus this year based on some combination of her organization's performance and her performance in her privacy role.

KEY FINDINGS:

- There is no discernible pattern across the combined private and public sector sample to explain salaries earned.
- Key findings within the private sector include:
  - There appears to be a modest relationship between years of work experience and salary. The relationship between salary and privacy experience was somewhat stronger.
  - The majority of respondents have some level of formal education gained through post-secondary study. There appears to be a modest relationship between university education and salary.
- The most popular certification is the IAPP's Certified Information Privacy Professional (CIPP) designation series. More than half of respondents have some form of CIPP designation or have recently tested for a CIPP designation.

What is our function? Our privacy roles and positions.

The findings indicate that the archetypical privacy professional is most likely to be located in a corporate functional area such as audit/compliance/risk management, strategy/planning or legal. She reports directly to a senior manager/director who, in turn, reports directly to the CEO or to a position within two layers of the CEO. She spends 60 to 100 percent of her time on privacy. In the case where she has other formal non-privacy duties, they might involve any number of other functions such as legal, IT or project management. Her position is equally as likely not to have been relocated from a different part of the organization. Regardless, she believes strongly that the privacy position she occupies has increased in importance to the organization in the past five years.

KEY FINDINGS:

- The privacy role is significant. Its importance within responding organizations has increased in the past five years as reported by 82 percent of respondents.
- The privacy position is largely full time (97%) and exists relatively close to top management (69% within two reporting levels).
- The position is associated with core functions (audit/compliance/risk management and legal) that protect the enterprise.

How do we operate? Our privacy programs.

On average, an IAPP Canada privacy professional has five major priorities:

1. Complying with laws and regulations—primarily PIPEDA (or the provincial equivalent) and provincial health privacy legislation

2. Managing risk
3. Safeguarding data against external attacks
4. Safeguarding reputation and brand in the marketplace
5. Safeguarding data against internal attacks.

To manage these concerns, she has a small staff complement (typically fewer than five staff) and an equally modest budget (less than $500,000). The budget is allocated against a small range of activities including policies, procedures and governance, audits and incident/breach response. She is most likely to rely on a crisis team to respond to privacy/breach events. It is somewhat less likely that she would use a cross-functional team to manage the organization-wide privacy responsibility. If she did use a cross-functional team, it would have been used to set policy and promote privacy awareness. An important aspect of the privacy role was to collaborate and cooperate with other organizational entities, especially information security and risk management peers as well as regulatory compliance and legal staff. Finally, measuring the success of the privacy function is important. She uses self assessments, audits, informal observation and benchmarking to assess the organization's level of privacy policy compliance, success in responding to or avoiding breaches, resolving customer complaints and conducting annual employee training.

KEY FINDINGS:

- The focus of and priority for privacy programs is compliance (65%) and related issues such as managing risk (56%) and safeguarding assets (54%). Issues such as improving the value of the information asset (32%) or increasing employee trust (30%) are of much less importance.
- Privacy programs function with modest personnel (64% have fewer than five staff) and operating budgets (47 percent have less than $500,000 annual budgets).
- Despite the modest resources available to the privacy programs in general, less than half (37%) of the respondents reported the use of cross-functional teams.
- Most privacy programs (62%) attempt to measure successes using a variety of techniques. The most popular techniques include inwardly focussed, with only one—benchmarking (23%)—used to compare performance against external standards.

Where do we operate? Our organizations.

There is no typical organization for the Canadian privacy professional, who may have been employed in the private or public sector and may have worked for a large or small organization. But most Canadian privacy professionals work in organizations whose focus is most likely domestic in geographic sphere, with a Canada-based head office. Those working in large organizations most likely would have had revenues in excess of $1 billion annually and employed more than 5,000 people in more than 20 locations. On the other hand, those working for smaller organizations would have seen annual revenues under $100 million and fewer than 100 staff in five or fewer locations.

KEY FINDINGS:

- Essentially, there is an even split between private (51%) and public (49%) respondents.

- Respondents are overwhelmingly focussed on domestic operations (67%). Operations are carried out in all provinces and territories, with the largest number in Ontario (79), BC (47), Alberta (43), Nova Scotia (39) and Quebec (38).
- There is little discernible relationship among organization size (as measured by annual revenues or overall headcount) and privacy program size (as measured by dedicated number of privacy staff). A simple relationship appears to exist between the number of locations and size of dedicated privacy staff complement. Very large organizations (37% have more than 20 locations) are more likely to have larger dedicated privacy staff complements. Very small organizations (48% have fewer than five locations) are more likely to have numbers of dedicated privacy staff.

| Survey Methods, Analysis and Limitations

The anonymous and confidential survey was prepared by the Privacy & Cybercrime Institute at Ryerson University in collaboration with IAPP Canada and IAPP. The questions were developed to reflect the Canadian privacy reality and to provide an opportunity for comparison across borders (i.e. IAPP and Ponemon Institute's Benchmarking Privacy Report).

This report presents the analysis IAPP Canada members' voluntary responses. IAPP Canada e-mailed members, inviting them to participate and providing them with a link to the online survey. Members who have not consented to receiving e-mail from the IAPP were not included in the invitation. To encourage participation, IAPP Canada offered a complimentary pass to the 2010 IAPP Canada Privacy Symposium to one randomly drawn respondent. In order to be included in the random draw, respondents were invited to provide an e-mail address. This contact information was decoupled from survey responses prior to analysts' accessing the data. The e-mail address was used only for the purpose of entering respondents in the contest for the complimentary conference pass and to contact the winner.

IAPP Canada issued more than 500 invitations to participate. The organization followed up with members twice during the period of April 7 through 23. During this period, 208 recipients viewed the survey and 166 attempted it. The surveyors asked respondents to answer 50 questions of various styles and lengths. All mandatory questions included an "I decline to respond," or similar, response category. Overall, 99 recipients completed the survey. This represents a 60 percent completion rate for those who attempted the survey and a 20 percent rate for those invited to participate. The researchers analysed and wrote up the results in April and May 2010.

It is not possible to assess whether there are significant differences among the members who chose to respond to the survey and those who did not. However, we attempted to assess the degree to which the respondents represent the membership in terms of gender. The survey respondents are 61 percent female and 38 percent male. One percent preferred not to answer. A review of the names associated with IAPP Canada's members, published in the IAPP Member Directory 2010, determined that the gender split appears to be 52 percent female and 48 percent male. This means that the present survey over-represents the female membership and under-represents the male membership. Cross-tabulations using the variables "gender" and "salary" were manipulated to reflect the sample pool of 98. (In both cases, there was a case where the respondent declined to provide identity or salary information.)

Establishing the proportion of members employed in the private versus public sectors proved more difficult given the many different organizational types from which IAPP Canada draws its membership. We believe that the survey sample approximates the sector split across the membership.

The survey results (descriptive statistics and cross tabulations) were first analysed using the online tools provided within the survey software. Additional analysis was conducted using Excel statistical tools once the final results were downloaded and reviewed by Ryerson University analysts. There were no significant differences between the online and Excel results.

It is not possible to determine the reasons for the differences among the viewing rates of the survey versus attempting it, and abandoning the survey versus completing the survey in its entirety. Further, these results reflect a single point in time—a "snapshot" of the portion of the membership that chose to participate. As a result, the findings are useful to the extent that they provide some information about privacy careers, positions, programs and organizational settings within the Canadian context. However, findings should be interpreted with caution as they are not statistically generalisable for the following reasons:

1. Not all IAPP Canada members participated in the survey. The respondents represent approximately 20 percent of the membership.
2. While IAPP Canada's membership covers many sectors, industries and regions, not all of these are represented in the responses. Some sectors, industries, and regions may be over- or under-represented.
3. The survey respondents were fairly equally distributed between private (51%) and public (49%) sectors. This appears to fairly approximate the distribution among the membership.

Readers are reminded that a correlation does not necessarily indicate causation. There may be a statistical relationship between two variables, for example salary and length of tenure in a position (correlation). That is, the two variables appear together. However, the present methodology does not permit us to state categorically that one variable (length of tenure) causes a change in another variable (salary).

| Survey Results

This section reports on the major findings of the first IAPP Canada Privacy Professional Survey. The results are reported in four themes:

Theme 1: Who are we? Our privacy careers – provides an overview of the respondents according to the indicators of gender, age, credentials, years of work experience, years of privacy experience, present level of responsibility, length of tenure in present position, salary and bonus and perceptions of salary equality.

Theme 2: What is our function? Our privacy roles and positions – details the respondents' privacy positions including where they are located in their organization by function, reporting relationship, headcount and budget. We also asked about the extent to which privacy was the primary role of their positions.

Theme 3: How do we operate? Our privacy programs – explores how privacy programs are organised, including the size of the privacy staff and budget and the activities for which respondents were responsible, program priorities, the use of cross-functional teams as well as crisis-response teams, and the use of program effectiveness measures.

Theme 4: Where do we operate? Our organizations – explains the organizational settings in which IAPP Canada privacy professionals operate, including information about the industries/sectors, geographic scope of operations and size of organization by revenue and headcount, with a primary focus on respondents' Canadian operations.

Each section provides detailed findings as well as a discussion about the implications of the findings.

| Who are we? Our privacy careers.

This section provides an overview of the respondents according to the indicators of gender, age, credentials, years of work experience, years of privacy experience, present level of responsibility, length of tenure in present position, salary and perceptions of salary equality. We include the industry of employment to provide necessary context to these career portraits. We report the results in aggregate and, where useful, by gender. Overall, we provide a portrait of the Canadian privacy professional in 2010.

Ninety-nine IAPP Canada members—61 percent female and 38 percent male—completed the survey. One percent declined to indicate gender. Thus, the present survey over-represents IAPP Canada's female members and under-represents the males. This should be kept in mind as the patterns in the data are discussed below.

Detailed Findings[1]

We report the aggregate results for gender, age, credentials (education and privacy), years of work experience, years of privacy experience, present level of responsibility, length of tenure in present position, salary, bonus, and perceptions of salary equality. We begin with an explanation of the industries in which the IAPP Canada survey respondents are employed.

Industry

Respondents were asked to select all sectors in which they operated; therefore, results sum greater than 100 percent. The results indicate that, in general, female respondents are distributed across healthcare (30%), government (all sectors combined, 25%), professional services (combined, 23%) and finance (20%). In contrast, 45 percent of male respondents came from professional services—combined, 40 percent from government – all sectors combined, 29 percent from finance, and 18 percent from healthcare.

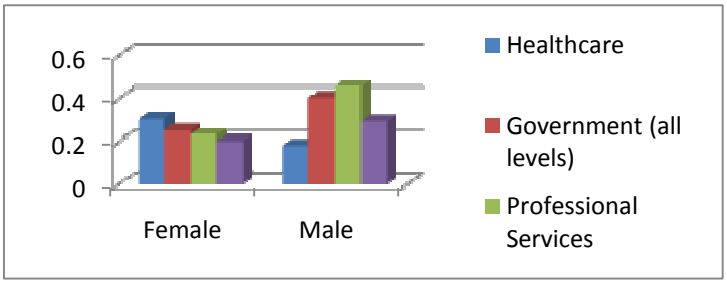

Figure 1: Distribution of sectors by gender

[1] Note that 96 percent of respondents indicated that their position is full time; therefore, we considered the entire sample to be full time and conducted no further analysis using the full time variable.

Gender
The respondents were 60 percent female and 38 percent male (2 percent did not identify their gender).

Age
The respondents are distributed across the age ranges. The largest group, at 23 percent, is the 35 to 39-year-old category followed by the 45-49 age group at 19 percent.

Education Credentials
Overall there is little difference between female and male respondents in terms of general academic and professional credentials. Ninety percent of all respondents have some post-secondary education. Twenty-eight percent have advanced degrees and designations (e.g., Masters, LLB, CA). The one significant difference is that more females (20%) have associate/community college degrees than males (8%).

Privacy Credentials
Overall, IAPP members tend to seek IAPP-sanctioned privacy credentials. Male (66%) and female (43%) respondents have earned at least one of the IAPP Privacy credentials such as the CIPP, CIPP/C, or CIPP/G. However, females (43%) were more likely than males (29%) not to have earned any privacy credential.

Work Experience
The majority of respondents have work experience ranging between five and 15 years. There was one significant difference in the female and male work experience responses. A greater proportion of the females (37%) reported having 25 or more years of work experience compared with 26 percent of male respondents.

Figure 2: Private Sector – Salary relative to years of work experience (% of respondents)

Privacy Experience

Overall, 61 percent of respondents have between two and 10 years of privacy experience. However, female respondents were more likely to have five to 20 years experience (38%) than males (21%).

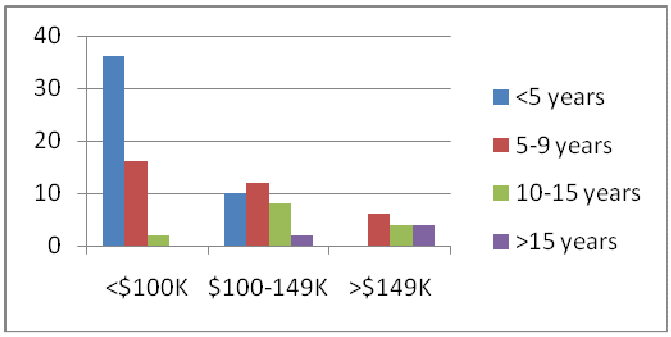

Figure 3: Private Sector – Salary relative to years of privacy experience (% of respondents)

Level of Responsibility

There appear to be some significant differences between the levels of responsibility between genders. While both groups reported essentially similar participation rates in the "Analyst/Staff" category (27% for females and 29% for males) there was a significant disparity in the manager and senior manager categories. Female representation at the "manager" level was 40 percent compared with 26 percent for males, while 26 percent of males were designated "senior managers" in contrast to 17 percent of females. In addition, while there were few respondents in the "executive" category, an executive was more likely to be male than female.

Years in Position
Most respondents have two to five years experience in their present position. Half of the female respondents have occupied their position for two to five years, compared with 37 percent of male respondents. There were proportionately more males (29%) than females (23%) new to their positions (less than two years).

Prior Position
Only 20 percent of previously held positions were primarily focussed on privacy, while 25 percent had nothing to do with privacy. Fifty five percent of previously held positions have had some privacy focus, but to a limited degree.

Salary
The salary data showed a clustering for both female and male respondents across the three categories that defined a salary range of $50,000–$149,000. This range accounted for 90 percent of female respondents and 81 percent of male respondents. However, the $149,000-and-over salary range represented 29 percent of male respondents versus 8 percent of female respondents.

Annual Bonus
Approximately 30 percent of respondents indicated that the annual bonus question was either not applicable to their positions or that they preferred not to answer. Fifty-five percent of respondents indicated that they expected to receive a bonus, while 15 percent indicated that they did not. Those who indicated "no" suggested that budget constraints, salary freezes and union contracts were reasons for not receiving bonuses.

Respondents indicated that the basis for receiving a bonus could be complex. Because the question was posed to provide for multiple answers, the sum is greater than 100. Forty-five percent indicated that overall company performance determined bonus decisions, while only 19 percent responded that business unit performance was part of the bonus decision. However, 38 percent claimed that meeting their position's objectives was part of the bonus equation.

Compensation Comparison with Organizational Peers
Approximately 13 percent of the respondent pool indicated that this question was not applicable to their situation. There were significant differences in perceptions among those who responded as to how well privacy professionals are compensated in comparison with their organizational peers. Proportionately more male respondents (67%) indicated that their compensation was equal to organizational peers, compared with 55% of female respondents. Almost 40 percent of female respondents expressed that their compensation was below their organizational peers while only 24 percent of males reported this perception.

Compensation Comparison with Industry Peers
Approximately 19 percent of the respondent pool indicated that this question was not applicable to their situation. There were significant differences in perceptions among those who responded as to how well they, as privacy professionals, are compensated in comparison with their industry peers. Proportionately more male respondents (58%) indicated that their compensation was equal to industry peers compared with 46 percent of

female respondents. Forty-four percent of female respondents expressed that their compensation was below that of their industry peers, while 32 percent of males reported this perception.

Key Findings:

- There is no discernible pattern across the combined private and public sector sample to explain salaries earned.
- Within the private sector sample, there are some key findings:
    - There appears to be a modest relationship between years of work experience and salary. The relationship between salary and privacy experience was somewhat stronger.
    - The majority of respondents have some level of formal education gained through post-secondary study. There appears to be a modest relationship between university education and salary.
- The most popular certification is the IAPP's CIPP designation series. More than half of the sample has some form of CIPP designation or has recently tested for a CIPP designation.

| What is our function? Our roles and positions.

In this section we detail respondents' privacy positions, including where they are located in their organization by function, their reporting relationship, headcount and budget. We also highlight the extent to which privacy is the primary role of their positions.

Detailed Findings

Functional Location of Position
The majority of respondents indicated that their positions are located in either audit/compliance/risk management (27%), strategy/planning/office of ceo/board secretariat (14%) or their organization's legal department (13%). An overwhelmingly 60 percent of these respondents' positions are not organised in a "dotted line" relationship. Therefore, the majority have a single superior to whom they report.

Reporting Relationships
Thirty-five percent of respondents indicate that their immediate superior is a senior executive, while 31 percent said senior manager/director. They also report that there is variation in the number of layers between their organization's privacy leader and its highest ranking executive. Thirty-six percent indicate that their privacy leader reports directly to the highest executive, while 33 percent are within two levels of the highest executive. There were three layers in 21 percent of organizations and only 5 percent reported four layers.

Significance of Privacy Function
Respondents were asked about the extent to which privacy was the most significant function/responsibility for their position ("how much time do you spend on privacy?"). Forty percent reported that their privacy responsibilities took up 80–100 percent of their time. The rest of the respondents were fairly evenly distributed across the remaining three categories. Seventeen percent spent 60-80 percent, 22 percent spent 40–60 percent and 20 percent spent up to 40 percent of their time on privacy. When respondents who had indicated that they had other "significant" responsibilities (taking more than 10 percent of their time) that were not privacy related, no clear pattern emerged. There were a variety of other functions performed, ranging from audit/compliance/risk management (9%) to IT, legal, marketing, security, project management (1 or 2% each).

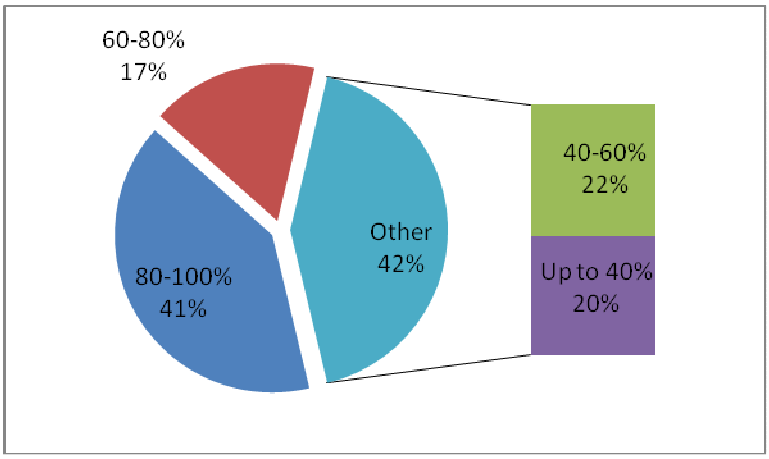

Figure 4: Proportion of time devoted to privacy duties

Changes to Privacy Function

To learn the extent to which there had been changes to the privacy function in the past five years. The respondents were also most evenly split between those that who indicated that the location of the privacy function had not changed in the past five years (48%) and those who said that the location had changed (42%). Examples of the changes included:

1. From corporate affairs to audit/compliance/risk management
2. From government relations to security
3. From corporate services/secretariat to finance
4. From corporate affairs to legal.

At the same time, there was overwhelming agreement (82%) with the statement that the "importance of the privacy position I currently occupy has increased in importance to my organization in the past five years."

Key Findings

- The privacy role is significant. Its importance within responding organizations has increased in the past five years as reported by 82 percent of respondents.
- The privacy position is largely full time (97%) and exists relatively close to top management (69% within two reporting levels).
- The position is associated with core functions (audit/compliance/risk management and legal) that protect the enterprise.

| How do we operate? Our privacy programs.

In this section we provide information about how privacy programs are organised, including the size of the privacy staff and budget and the activities for which respondents are responsible, program priorities, the use of cross-functional teams as well as crisis response teams, and the use of program effectiveness measures.

Detailed Findings

Program Priorities

Respondents chose from a list of 10 typical priorities for a privacy program and ranked them in order of importance to their organizations.[2] The single highest program priority was "complying with laws and regulations." This was selected by 51 percent of respondents as a number one priority. The strength of this grew when the selection for priorities one, two and three were considered together. In this case, compliance was the most popular selection for 64 respondents. The table below shows how the priorities were ranked when the first, second and third priority choices were aggregated.

Priority		Top 3 Cumulative Respondents	% Response	Private Sector Count	Public Sector Count	Private Sector %	Public Sector %
1.	Complying with laws and regulations	64	65	36	28	56	44
2.	Managing risk	56	57	32	24	57	43
3.	Safeguarding data against external attacks and threats	54	55	29	25	54	46
4.	Safeguarding reputation and brand in marketplace	48	48	29	19	60	40
5.	Safeguarding data against internal attacks and threats	46	46	25	21	54	46
6.	Increasing consumer trust	40	40	27	13	68	32

[2] We had expected to use a "force rank" approach in which respondents would be forced to indicate a single first priority, second priority, etc. However, respondents selected several first priorities. As a result, our analysis is limited to reporting on the variety of first priorities selected by the majority of respondents.

7.	Ensuring business partner compliance	35	35	27	8	77	23
8.	Enhancing the value of information assets	32	32	18	14	56	44
9.	Increasing employee trust	30	30	19	11	63	37
10.	Influencing regulatory and legal frameworks	22	22	14	8	64	36

Table 1: Summary of Privacy Program Priorities

The second largest category of 'first' priority was "safeguarding reputation and brand in the marketplace" (29 respondents). Safeguarding the organizations' data from external (28 respondents) or internal (23 respondents) attacks and threats, and managing risk (26 respondents) rounded out the top five priorities.

There was an interesting split between the public sector and private sector respondents, which suggests that the priorities provided for evaluation have more salience with the private sector respondents than their public sector counterparts.

Privacy Employee Complement

Privacy employee complements were overwhelmingly modest. Sixty-four percent of respondents indicated that their complement was less than five employees while 19 percent said that they had five to 10 privacy staff.

As well, respondents were asked to comment on whether they anticipated a change to the directly-related privacy headcount in the next fiscal year. The majority (60%) indicated that there would be no change. More than 20 percent indicated an increase was anticipated while 18 percent were not able to comment at the time of the survey.

Privacy Budget Overall

Consistent with the proportion of respondents that are employed in professional consulting services, 39 percent of respondents indicated that the question of the size of the dedicated privacy budget was not applicable. The remainder of responses show that privacy program budgets are also modest. Twenty-seven percent of respondents indicated having a budget of less than $100,000 while 20 percent have budgets in the range of $100,000-$499,000. At the same time, a handful (9%) indicated having privacy program budgets in excess of $1 million.

At the time of the survey, there was a high degree of uncertainty about the direction of next year's privacy budget. Forty percent were unable to say if there would be a budget change. Forty one percent thought that there would be no change, while 11 percent said they were expecting a budget increase.

Privacy Budget by Activity
Respondents were asked to indicate the approximate allocation of their privacy budgets to a list of privacy-related activities. Twenty-nine percent indicated that this was not applicable to their circumstances. The activities for which there was the greatest average allocation of budget included for policies, procedures and governance (9 percent of budget), audits (8.5%), and incident/breach responses (7.5%). Organization awareness and training as well as salaries and benefits each averaged six percent of budget. Interestingly, only one organization reported allocating any budget for Web seals and certification, accounting for less than one percent of their privacy budget.

The matter of potentially greatest interest but lowest information is the percentage of budgets devoted to salaries and benefits. Because only 11 responses were provided, we cannot comment on the statistical validity of the data. However, the pattern is provided in the table below.

Proportion of Privacy Budget Allocated to Salaries and Benefits (%)	Private Sector Occurrence	Public Sector Occurrence	Not for Profit Occurrence
10	1		
30		1	
35	1		
40	2		
50		1	1
75	1	1	
80	1		1

Table 2: Proportion of Privacy Budgets devoted to Salaries & Benefits

Privacy Laws
Several respondents provide consulting services and as a result are not necessarily required to comply with any particular privacy statute. As a result, we report counts of statutes rather than percentages. Consistent with the scope of Canadian and foreign operations indicated by respondents, there was a large number of different privacy statutes to which members' organizations must comply. Not surprisingly, PIPEDA topped the count (61 respondents). At the same time, a significant proportion (up to 45 organizations) reported having to comply with health privacy legislation such as Ontario's PHIPA. Respondents from organizations that operate outside of the Canadian jurisdiction reported that they are engaged with several privacy and privacy-related statutes including Unfair and Deceptive Trade Practices (15 responses), Sarbanes-Oxley Act (14 responses), Health Insurance Portability and Accountability Act (12 responses) and the European Union's Data Directive (12 responses).

Use of Teams
The survey asked respondents to indicate whether their organization used a cross-functional team to oversee the privacy function and/or activities. Interestingly, more than half (53%) said they did not, while 37 percent affirmed the role of the team in their privacy program. Ten percent reported that the concept was not applicable to their situation.

Those who responded affirmatively to the use of cross-functional teams indicated that policy setting (13 respondents) and awareness and promotion (11 respondents) were the two top primary roles for the committees. Compliance monitoring and operational co-ordination were also important to six organizations.

In contrast to the limited interest in cross-functional teams, the survey found that 62 percent of respondents employed a privacy/security breach crisis response team that operated only in response to a significant threat (no ongoing operational role). There was no significant difference between the use of these teams between the private and public sector respondents.

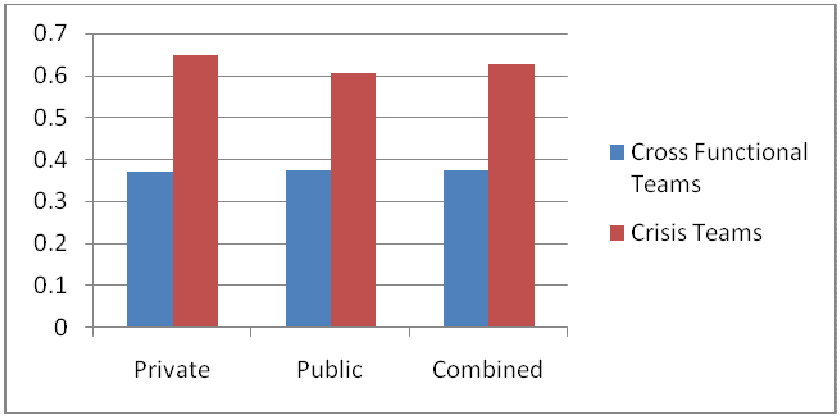

Figure 5 : Use of Cross-functional and Crisis Response Teams

Program Collaboration

Respondents were asked to comment on how important to their organizations is privacy coordination and collaboration across functional areas. There was a high proportion of "Not Applicable" responses as well as "No response" (respondents had not answered the question). As a result, we report the top five areas of collaboration importance according to the rankings of five (very important) and four (important).

Respondents indicated that collaboration and cooperation with Security-information (61 respondents) was of highest importance followed closely by Risk Management (60 respondents). Fifty-eight respondents said that collaborating with Information technology was important or very important while 57 said that working with the regulatory compliance function was key. Cooperating with legal was also important or very important to 54 respondents.

Program Measurement

Overall, 62 percent of IAPP Canada privacy professionals agreed that they attempted to measure their privacy programs' success. They employed a variety of approaches to gauge several different objectives. The five most important objectives include complying with policies, and addressing/resolving data breaches (45 responses each); conducting annual employee privacy awareness and training (43 responses); addressing/resolving customer complaints (41 responses); and avoiding data breaches (40 responses).

The degree of achievement of these various objectives was measured in a variety of ways. Respondents indicated that the top five approaches to measuring program success included self-assessments (46 responses); audits (44 responses); informal observation (32 responses); and benchmarking against others and internal case studies/after action reports (23 respondents each).

Key Findings

- The focus of and priority for privacy programs is on compliance (65%) and related issues such as managing risk (56%) and safeguarding assets (54%). Issues such as improving the value of the information assets (32%) or increasing employee trust (30%) are of much less importance.
- Privacy programs function with modest personnel (64 percent have less than 5 staff) and operating budgets (47 percent have less than $500,000 annual budgets.)
- Despite the resources available in general to the privacy programs, less than half (37%) of the respondents reported using cross-functional teams.
- Most privacy programs (62%) attempted to measure their successes using a variety of techniques. The most popular techniques were very inwardly focussed with only one (benchmarking, 23%), used to compare performance against external standards.

| Where do we operate? Our organizational settings.

In this section we describe the organizational settings that employ the IAPP Canada privacy professional. We include information about the industries/sectors, geographic scope of operations, and size of organization by revenue and headcount. We focus primarily on respondents' Canadian operations.

Detailed Findings

Industry Type
Respondents were asked to select all sectors in which they operated; therefore results sum greater than 100 percent. IAPP Canada members come from a variety of industries and sectors. The largest clusters were government across all levels (31 responses), healthcare (26), financial services (23), professional services (13), IT consulting and telecommunications (20), education (5), and other (11). Note that respondents were able to report more than a single industry, therefore the count and not a percentage is reported in the table below.

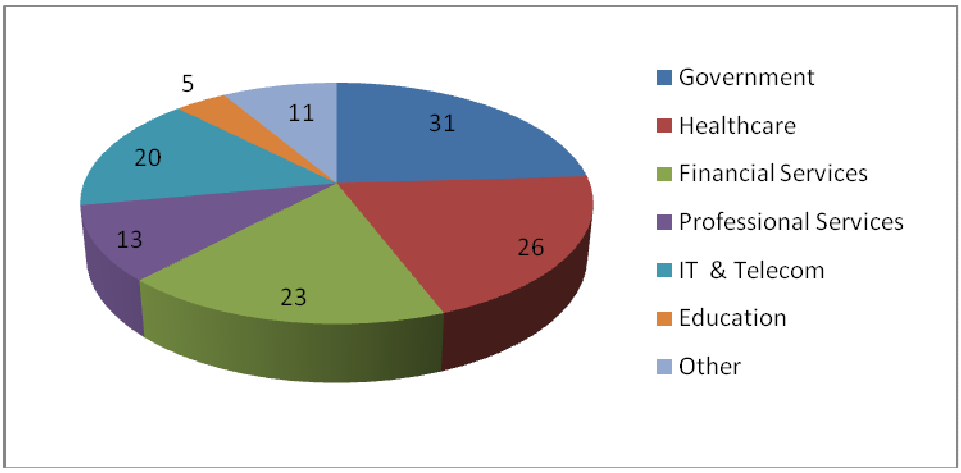

Figure 6: Relative proportion of industries and sectors

Public versus Private Sector
Not surprisingly given the structure of the Canadian economy, respondents were fairly evenly split between the private (51%) and public (49%) sectors. Of the private sector respondents, half indicated that their organizations are publicly traded.

Geographic Scope of Operations
While the majority of respondents (67%) reported that their organizations had domestic operations only, 27 percent indicated that their organizations had a global geographic scope (operated on more than two continents). As a result, IAPP Canada members have

employees across the globe including the USA (28 organizations), Latin and South America including Mexico and the Caribbean (33 organizations), Europe (22 organizations), Asia-Pacific including Australia and New Zealand (17) and the Middle East including Turkey (6).

Head office Location
While the vast majority of respondents indicated that their organization's head office was located in Canada (83%), 15 percent indicated a U.S.-based head office while two percent listed Europe.

Dimensions of Canadian Operations
Within the domestic sphere, respondents' organizations had operations/activities in all provinces and territories. Ontario (79), British Columbia (47), Alberta (43), Nova Scotia (39) and Quebec (38) represent the five provinces with the most respondents. Interestingly, the count of offices/permanent locations indicated that IAPP Canada's members' organizations are either quite large (37 percent have more than 20 locations) or quite small (48 percent said less than 5 locations).

Dimensions	Revenues	Public	Private	Employees	Public	Private	Locations	Public	Private
V. Large	>$1 B	6	19	>25,000	8	4	>20	10	24
Large	$ 100 M-9999	10	9	10,000-25,000	2	6	16-20	4	4
Medium	$1 M - 99	19	14	1,000-9,999	15	20	11-15	3	3
Small	$500,000-$1M	0	1	100-1,000	18	10	6-10	1	3
V. Small	<%500,000	2	2	<100	4	7	<5	28	16
No response		12	6		2	4		2	2
		100%			100%			100%	

Table 3: Dimensions of Canadian operations

Employees
At the same time, the headcount of employees from domestic operations has wide dispersion. Thirty-two percent of respondents indicated organizational sizes of 100–999 employees, 30 percent employed 5,000–49,999 people, and 20 percent had a headcount ranging from 1,000–4,999. There were a few very large organizations with in excess of 50,000 Canadian employees (7 %) and slightly more (11%) small organizations with fewer than 100 employees.

Revenues
The ranges among organizational size carried over to the respondents' reported revenues. Private sector organizations were dispersed across the ranges. Significant clusters included very large organizations that booked more than $1 billion in revenue (19%), $1 – 100 million (14%) and less than $1 million (3%). Public quasi-public sector organizations were likewise dispersed. Six percent of respondents reported revenues in excess of $1 billion, 10

percent were in the $100 – 999 million range, and 20 percent fell in the range of $1 – 99 million.

Key Findings

- There was essentially an even split between private (51%) and public (49%) respondents.
- Respondents were overwhelmingly focussed on domestic operations (67%). Operations were carried out in all provinces and territories with the largest number in Ontario (79), BC (47), Alberta (43), Nova Scotia (39) and Quebec (38).
- There was little discernible relationship among organization size (as measured by annual revenues or overall headcount) and privacy program size (as measured by dedicated number of privacy staff). A simple relationship appeared to exist between the number of locations and size of dedicated privacy staff complement. Very large organizations (37 percent had more than 20 locations) were more likely to have larger dedicated privacy staff complements. Very small organizations (48 percent had less than 5 locations) were more likely to have numbers of dedicated privacy staff.

| Conclusion

The IAPP, IAPP Canada and Ryerson University's Privacy & Cyber Crime Institute collaborated on the first survey of Canadian Privacy Professionals. The goal of the survey was to create a portrait of the state of the privacy profession by developing understanding of four areas:

1. Salary and privacy career information.
2. Structure of current privacy positions.
3. Function and operations of privacy programs.
4. Organizational and industry considerations.

This report documents the findings and establishes a baseline for comparisons from future surveys.

The Canadian privacy profession is dynamic and of increasing importance to the organizations it serves. The survey results show the extent to which privacy is becoming integral to the management of the contemporary organization regardless of sector or size.

We thank the members of IAPP Canada who took the time to complete the survey.

| Appendix A: Survey Instrument

The following is the survey instrument. A * indicates a mandatory question.

1. ***What is your gender?****

   Female = 60
   Male = 38
   Prefer not to answer = 1

2. ***What is your age?****

Range	Pct%
25-29	4
30-34	12
35-39	23
40-44	17
45-49	19
50-54	10
55-59	10
60-65	2
Over 65	2

3. ***How many years have you worked in total?***

Range	Pct%
2-5 years	2
5-10 years	11
10-15 years	17
15-20 years	15
20-25 years	21
More than 25 years	33

4. How many years of privacy experience do you have?

Range	Pct%
Less than 2 years	14
2-5 years	29
5-10 years	32
10-15 years	16
15-20 years	5
20-25 years	1
More than 25 years	2

5. Prior to assuming your present position, how would you describe your work (whether in your current organization or another one)?

Responses	**Pct%**
Primarily focussed on privacy issues	**20**
Somewhat focussed on privacy issues	**27**
Only a little bit focussed on privacy issues	**28**
Previous position had nothing to do with privacy	**23**
This is my first position	**1**

6. What is your current annual salary (base pay & benefits) in Canadian dollars to the nearest $1000 using the following ranges?*

Range	**Pct%**
Less than $50,000	1
$ 50,000 to $74,000	27
$ 75,000 to $99,000	33
$100,000 to $149,000	26
$150,000 to $199,000	4
$200,000 to $249,000	2
$250,000 to $499,000	2
Over $500,000	3
I prefer not to answer this question	1

7. Do you expect to receive a bonus/merit increase this year?*

Response	Pct%
Yes, I expect to receive a bonus or other special compensation	55
No, I do not expect to receive a bonus or other special compensation	15
Not applicable to my position/organization	28
I prefer not to answer this question	2

8. If you responded yes or no to the previous question (you expect/do not expect to receive a bonus or other special compensation), please indicate the basis for which you might receive a bonus or other special compensation (check all that apply):

Response	Count
Overall company performance	45
Business unit performance	19
Achieving your position's specific objectives	38
Earning a specific credential (i.e., CIPP(C))	3
Completing a course of education (i.e., MBA)	1
Other	8

9. I believe that the compensation I receive in relation to others in my organization is:

Response	Pct%
Above others with similar experience, education and training, and level of responsibility	6
About equal to others with similar experience, education and training, and level of responsibility	29
Below others with similar experience, education and training, and level of responsibility	51
No opinion/ Not applicable	14

10. I believe that the compensation I receive in relation to other privacy professionals in my industry (or other peer group) is:

Response	Pct%
Above others with similar experience, education and training, and level of responsibility	8
About equal to others with similar experience, education and training, and level of responsibility	32
Below others with similar experience, education and training, and level of responsibility	40
No opinion/ Not applicable	20

11. Please indicate what post-secondary degrees and/or professional designations you have earned (check all that apply)

Response	Count
Doctorate (i.e., DBA, PhD)	3
Master (i.e., JD, LLM, MA, MBA, MSc)	26
Bachelor (i.e., BA, BComm, BEd, BSc)	55
CA/CGA/CMA/CPA	2
LLB	11
Certificate/Associate Degree (Community/Junior College)	28
None	11
Other	

12. Please indicate what privacy and related designations you have earned (check all that apply):

Response	Count
CIPP etc,	52
CIA	2
CISSP	6
CISA	5
CISM	4
None	37
Other	

SECTION TWO: STRUCTURE OF YOUR PRIVACY POSITION

13. What is your current position title?

Text response

14. How many years have you occupied your current position?

Response	Pct%
More than 25 years	2
20 – 25 years	
15 – 20 years	
10 – 15 years	4
5 – 10 years	23
2 – 5 years	45
Less than 2 years	26
Total	100

15. Are you a full time employee as defined by your organization?

Response	Pct%
Yes	**97**
No	**3**
Total	**100**

16. What organizational level best describes your current position?

Response	Pct%
Senior Executive ("C level" equivalent)	5
Executive (Not "C level")	6
Senior Manager / Director	20
Manager	34
Analyst / Staff	27
I am an independent Consultant	4
Other	2
Total	100

17. ***Please indicate the functional area where the primary person you report to works:***

Response	Pct%
Accounting/Comptroller	3
Audit/Compliance/Risk Management	21
Ethics/Corporate Social Responsibility/Public Affairs	4
Finance	2
Human Resources/Compensation/Training	2
Information Technology	8
Legal	13
Marketing	2
Research	4
Security	19
Not applicable	3
Other	19
Total	100

18. **Please indicate the organizational level of your superior's position (as indicated in the previous question):**

Response	Pct%
Senior Executive ("C level" equivalent)	35
Executive (Not "C level")	14
Senior Manager / Director	31
Manager	12
Not applicable/not answered	6
Other	2
Total	100

19. ***Does your position also report to another area of the organization ("Dotted Line" relationship?)***

Response	Pct%
Yes, I report in a dotted line relationship	25
No, my organization is not organised in this manner	60
Not applicable	15
Total	100

20. If you answered yes to the question above (your position is in a dotted line relationship), please indicate the functional area where the "dotted line" person you report to works:

Response	Pct%
Accounting/Comptroller	8
Audit/Compliance/Risk Management	25
Finance	4
Legal	17
Strategy/Planning/Office of CEO/Board Secretariat	21
Other	25
Total	100

21. In your organization, how many reporting levels exist between the privacy leader and the highest ranking executive?

Response	Pct%
One level (direct report)	36
Two levels	33
Three levels	21
Four levels	5
No answer	5
Total	100

22. Please indicate the organizational area of the company area where your current position is located.

Response	Pct%
Accounting/Comptroller	2
Audit/Compliance/Risk Management	27
Ethics/Corporate Social Responsibility/Public Affairs	3
Finance	2
Human Resources/Compensation/Training	3
Information Technology	10
Legal	13
Marketing	1
Operations	6
Security	4
Strategy/Planning/Office of CEO/Board Secretariat	14
Other	14
Total	100

23. To what extent is privacy the most significant aspect/responsibility of your current position? Please check the range that best reflects how much time you spend on privacy in your current position.

Response	Pct%
80 – 100 %	41
60 – 80 %	17
40 – 60%	22
1 – 40 %	20
Total	100

24. In addition to your privacy related responsibilities, what additional significant job functions (more than 10% of your time) do you perform for your organization? Please check all that apply.

Response	Pct%
Privacy is my sole responsibility	14
Accounting/Comptroller	2
Audit/Compliance/Risk Management	27
Ethics/Corporate Social Responsibility/Public Affairs	2
Human Resources	3
Information Technology	6
Legal	10
Marketing	5
Security	9
Other	22
Total	100

25. Has the location (organizational area) of the privacy function changed in the last five years ?

Response	Pct%
No, the organizational area has not changed	48
No opinion	10
Yes,	42
Total	100

26. Thinking back over the past five years … I believe that the privacy position I currently occupy:

Response	Pct%
Has increased in importance to my organization	82
Has decreased in importance to my organization	1
Has neither increased nor decreased in importance	11
No opinion/Not applicable	6
Total	100

SECTION THREE: YOUR CURRENT ORGANIZATION

27. What industry(ies) or sector(s) best define your organization? If your organization competes/operates in more than one sector, please check all that apply. You may also write in the space "OTHER" if necessary.

Response	Count
Advertising/Communications/ Public Affairs	3
Agriculture/Food processing	1
Arts	0
Biological/Chemical/Pharmaceutical	0
Consumer Products/Packaged goods	0
Education – primary/secondary	1
Education – post-secondary	4
Energy	0
Financial Services (retail & investment banking, insurance, etc.)	23
Government/Regulatory – municipal	4
Government/Regulatory – provincial/territorial	18
Government/Regulatory – federal	9
Healthcare	26
Hospitality, Leisure, Tourism	0
Information Technology/Software/Services	12
Manufacturing	0
Professional services – Audit & Accounting	6
Professional services - Consulting	12
Professional services - Legal	1
Research/polling	3
Retailing	3
Services	4
Telecommunications, cable, wireless, internet services	8
Transportation	2
Other	6
TOTAL	182

28. What is the geographic scope of your organization?

Response	Pct%
Global (operations/activities on more than two continents)	27
Transnational (operations/activities on two continents)	2
International (operations/activities in two countries on the same continent)	4
Domestic (operations in Canada only)	67
Total	100

29. Is your company publicly traded ?

Response	Pct%
Yes	26
No, my organization is privately held for profit	25
No, my organization is located within the public (e.g., government department/agency/commission) or "broader" public sector (e.g., college/university, hospital)	37
No, my organization is not-for-profit	10
No, my organization is a co-operative	2
Total	100

30. Your company has employees in (check all that apply):

Response	Count
Canada	99
United States	28
Latin America (including Mexico & Caribbean)	13
South America	20
Europe	22
Asia-Pacific (including Australia & New Zealand)	17
Middle East (including Turkey)	6

31. Please indicate where your organization's head office is located.

Response	Pct%
Canada	83
United States	15
Latin America (including Mexico & Caribbean)	
South America	
Europe	2
Asia-Pacific (including Australia & New Zealand)	
Middle East (including Turkey)	
TOTAL	100

32. For your Canadian organization, please check all provinces and territories where you have operations/activities.

Response	Count
Alberta	43
British Columbia	47
Manitoba	34
New Brunswick	31
Newfoundland and Labrador	31
Northwest Territories	19
Nova Scotia	39
Nunavut	15
Ontario	79
Prince Edward Island	29
Quebec	38
Saskatchewan	32
Yukon	17

33. For your Canadian organization, please indicate the number of offices/permanent work locations you operate .

Response	Pct%
Less than 5	48
Less than 10 but more than 5	7
Less than 15 but more than 10	6
Less than 20 but more than 15	2
More than 20	37
Total	100

34. What is the total headcount of your Canadian organization?

Response	Pct%
More than 50,000 employees	7
25,000 – 49,999 employees	5
10,000 – 25,000 employees	8
5,000 – 10,000 employees	17
1,000 – 4,999 employees	20
500 – 999 employees	6
250 – 499 employees	9
100 – 249 employees	17
Less than 100 employees	11
Total	100

35. If you work in the private sector, please indicate the range that most closely reflects the total revenues earned by your Canadian organization in 2008.

Response	Pct%
I DO NOT work in the private sector	49
More than $10 Billion	5
$ 1 – 9 Billion	14
$500 to $999 million	3
$100 to $499 million	6
$ 50 – $ 99 million	1
$25 - $ 49 million	2
$1 – 24 million	11
Less than $1 million but more than $500,000	1
Less than $500,000	2
Total	6

36. If you work for a government department, charity or other not-for-profit entity, please indicate the total value of revenues from all sources including grants, contributions, donations, etc. for your immediate organization only. For example, include the revenues of only your line ministry or agency, NOT the total revenues for the government of X. For a not-for-profit, include revenues from funding raising, research grants, sales of merchandise, and other monetary contributions. Please indicate the range that most closely reflects the total revenues earned by your Canadian organization in 2008.

Response	Pct%
I DO NOT work in the public sector, public sector, or not-for-profit sector	51
More than $10 Billion	2
$ 1 – 9 Billion	4
$500 to $999 million	4
$100 to $499 million	6
$ 50 – $ 99 million	5
$25 - $ 49 million	3
$1 – 24 million	11
Less than $1 million but more than $500,000	
Less than $500,000	2
Unable to say	12
Total	100

SECTION FOUR: YOUR ORGANIZATION'S PRIVACY PROGRAM

37. How many people work full time (or full time equivalent) in support of your organization's privacy function (whether directly employed by your organization or not)? Think of those people with direct, specific and significant privacy related responsibilities. Remember to include yourself in this count!

Response	Pct%
More than 20 employees	5
11 – 20 employees	6
5 – 10 employees	19
2 – 4 employees	40
1 employee	24
There are no dedicated full time privacy employees	6
Total	100

38. Do you anticipate a change to the directly-related privacy headcount in the next fiscal year ?

Response	Pct%
Headcount will increase	21
Headcount will decrease	1
Headcount will remain the same	60
Not able to determine at this juncture	18
Total	100

39. Does your organization have a cross-functional team steering/overseeing the privacy function/activities?

Response	Pct%
Yes	37
No	53
Not applicable	10
Total	100

40. If you answered yes (your organization does use a privacy steering committee), indicate the primary roles of the steering/overseeing committee (please check all that apply):

Response	Count
Awareness & Promotion	11
Compliance monitoring	6
Crisis management	2
Operational co-ordination	6
Policy setting	13
Training	4
Other	6

41. Do you have a privacy crisis, privacy/security breach response team or similar group that operates only in response to a significant threat?

Response	Pct%
Yes	62
No	26
Not applicable	12
Total	100

42. What are the privacy related activities for which you have responsibility (and budget)? Please allocate the approximate percentage of the budget to the following activities (so that the total equals 100%).

Category	Average Allocation Pct%
Audits	8.5
Communications	4.5
Compliance monitoring	5.5
Data inventory & mapping	<1
Development and training for privacy staff (direct reports)	3
General overhead and administration	3
Incident/breach response	7.5
Legal counsel	3
Meetings with regulators	1
Organization awareness and training	6
Outside consultants (non-legal)	1.5
Policies, procedures & governance	9
Professional association memberships	1
Redress and consumer outreach	<1
Salaries and benefits	6
Software and information technology (general office related)	<1
Software and information technology (privacy/security specific)	1
Subscriptions and publications	<1
Vendor management	1.5
Web certification and seals	<1
Other	5
Not applicable given my occupation (indicate 100)	29
TOTAL	100

43. What is the budget dedicated to the privacy function in your organization? Please include all the activities you checked in the previous question and select the closest range.

Response	Pct%
$5 million and over	2
Between $2.5 and $ 4.9 million	2
Between $1.0 and $2.4 million	5
Between $750,000 and $ 999,000	0
Between $ 500,000 and $ 749,000	5
Between $ 250,000 and $499,000	9
Between $100,000 and $ 249,999	11
Less than $ 100,000	27
Not applicable given my occupation	39
Total	100

44. Do you expect your organization's privacy budget to change this year?

Response	Pct%
It will increase	11
It will decrease	8
It will stay the same	41
No opinion/Not able to tell at this juncture	40
Total	100

45. Which privacy law(s) is(are) your organization required to observe? (Please check all that apply)

Response	Count
PIPEDA	61
Privacy Act (federal)	34
PIPA (Alberta)	37
PIPA (BC)	36
PPIPS (Quebec)	29
HIA (Alberta)	14
HIPA (Saskatchewan)	12
PHIA (Manitoba)	13
PHIPA (Ontario)	45
FCRA (Fair Credit Reporting Act)(USA)	9
HIPPA (Health Insurance Portability and Accountability Act) (USA)	12
GLBA (Gramm-Leach-Bliley Act) (USA)	11
COPA (Child Online Protection Act) (USA)	7
TSR (USA)	8
CAN-SPAM (USA)	8
UDTP (Unfair and Deceptive Trade Practices Act) (USA)	15
SOX (Sarbanes-Oxley Act) (USA)	14
EU Data Protection Directive	12
APEC (Asia-Pacific)	6
Other	1

46. The following is a list of typical priorities for organizational privacy programs. Please rank these according to order of importance to your firm where 1= highest priority and 10=lowest. Mark as N/A any priority that is not applicable to your organization.

Priority Activity	Ranking											Pct%
	1	2	3	4	5	6	7	8	9	10	N/A	100
Complying with laws and regulations	51	6	3	4	1	1	2	1	4	13	14	100
Enhancing the value of information assets	11	6	15	6	16	1	9	9	5	3	19	100
Ensuring business partner compliance	15	9	11	6	13	5	5	5	5	4	14	100
Increasing consumer trust	19	11	10	8	8	4	5	3	3	6	15	100
Increasing employee trust	12	5	13	8	10	2	10	8	8	7	9	100
Influencing regulatory and legal frameworks	6	8	8	7	9	8	5	9	9	7	6	100
Managing risk	26	18	12	5	1	5	1	5	6	7	6	100
Safeguarding data against external attacks and threats	28	14	12	2	5	4	5	3	2	9	7	100
Safeguarding data against internal attacks and threats	23	13	10	5	7	1	2	3	7	10	7	100
Safeguarding reputation and brand in marketplace	29	9	10	5	7	1	2	3	7	10	8	100

47. How important to your organization is privacy coordination and collaboration across-functional areas? Please indicate the importance of working together to achieve privacy goals where 1=not applicable, 2=not important, 3=somewhat important, 4=important and 5=very important. Mark as N/A any aspect that is not applicable to your organization. (N.R. indicates that "no response" was provided).

Source for Collaboration	Ranking							
	1	2	3	4	5	N/A	N.R.	Pct%
Corporate ethics/Social Audit/Corporate social responsibility	8	4	8	15	28	23	14	100
Finance & accounting	7	10	18	21	12	20	12	100
Government/public affairs	6	7	13	16	21	24	13	100
Human resources	3	14	12	23	24	10	14	100
Information technology	8	6	7	22	36	8	12	100
Internal audit	8	7	16	18	23	15	13	100
Legal	5	5	7	17	37	15	14	100
Marketing	4	11	22	16	11	23	13	100
Mergers & acquisitions	9	4	8	7	6	52	14	100
Operations	10	3	11	20	29	13	14	100
Procurement	6	15	10	16	16	24	13	100
Project management	7	11	12	26	17	13	14	100
Public relations/ communications	6	9	16	21	20	12	16	100
Records management	5	8	8	19	38	8	14	100
Regulatory compliance	9	4	7	15	42	10	13	100
Risk management	8	7	4	18	42	8	12	100
Sales	5	9	14	10	8	40	14	100
Security - Information	9	5	5	19	42	7	13	100
Security - Physical	6	10	11	20	32	7	14	100
Supply chain & logistics	6	9	14	8	8	41	14	100
Other	5	2	2	2	3	51	35	100

48. Does your organization attempt to measure the privacy program's success in meeting its objectives?

Response	Pct%
Yes	62
No	21
Not applicable	17
Total	100

49. If you answered yes (your organization measures privacy program success), please indicate which objectives you try to measure (check all that apply):

Response	Count
Addressing/resolving customer/consumer complaints	41
Addressing/resolving data breaches	45
Addressing/resolving employee complaints	30
Avoiding data breaches	40
Avoiding external threats	26
Avoiding inside threats	26
Avoiding negative media	27
Complying with policies	45
Conducting annual employee privacy awareness and knowledge reviews	33
Conducting employee privacy awareness and training	43
Enforcing vendor contracts	25
Gaining positive media	6
Implementing enabling technologies	24
Increasing numbers of staff with privacy certification	11
Maintaining reputation and brand image	30
Managing budget	10
Minimizing costs associated with incident responses	9
Minimizing customer churn or turnover	4
Minimizing response times to incidents	18
Mitigating risks	34
Other: completing PIAs; volume & range of activity	2

50. If you answered yes (your organization measures privacy program success), please indicate which measurement methods you use to assess the effectiveness of your privacy programs (check all that apply):

Response	Count
Audits	44
Benchmarking against other companies / industries	23
Competitive intelligence	5
Cost accounting studies	2
Focus groups	5
Informal observation	32
Internal case studies / after action reports	23
"Mystery" shoppers (on and offline)	6
ROI studies	1
Self assessments	46
Surveys	16
Other: numbers; reports & counts	2

| About IAPP Canada

IAPP Canada was created in 2009 to serve the growing needs of the IAPP's Canadian membership. IAPP Canada is a community for Canadian members to exchange ideas and enrich their knowledge. It serves as a resource for the Canadian privacy community by providing services, education, networking opportunities and conferences tailored to the unique challenges and needs of Canadian privacy professionals.

| About the IAPP

The International Association of Privacy Professionals (IAPP) is the world's largest association of privacy professionals, representing more than 7,000 members from business, governments and academic institutions across 52 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 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 annual conferences that are recognized internationally as the leading forums for the discussion and debate of issues related to privacy policy and practice.

| About Ryerson University, Ted Rogers Faculty of Business, Privacy and CyberCrime Institute

The Privacy and Cyber Crime Institute's mandate is to foster partnerships between Ryerson, the private sector, and the public sector to research privacy and disseminate knowledge. The Institute generates knowledge through workshops, public lectures and reports; creates an internal forum for faculty members with related interests to meet, discuss and develop their research; and serves as an external contact point for media and others interested in issues related to the institute.