POR Number: 029-17
Contract Number: 2R008-170120-001-CY
Contract Award Date: 2017-09-25
Date of Submission: 2018-01-19

FINAL REPORT

2017 Survey with Canadian businesses on privacy-related issues

Prepared for: Office of the Privacy Commissioner of Canada

publications@priv.gc.ca

January 2018

Ce rapport est aussi disponible en français.

Phoenix SPI is a Gold Seal Certified Corporate Member of the MRIA

1678 Bank Street, Suite 2, Ottawa, ON, K1V 7Y6 T 613-260-1700 F 613-260-1300 E info@phoenixspi.ca

Table of contents

Table of figures

Executive summary

The Office of the Privacy Commissioner of Canada (OPC) commissioned Phoenix Strategic Perspectives (Phoenix SPI) to administer a 13-minute telephone survey to 1,014 Canadian businesses. Based on a sample of this size, the results can be considered accurate to within ±3.1%, 19 times out of 20. The fieldwork was conducted from October 27 to November 30, 2017, and the results were weighted to reflect the actual distribution of businesses in Canada.

The purpose of the research was to better understand the extent to which businesses are familiar with privacy issues and requirements, to learn more about the types of privacy policies and practices that they have in place, and to determine their privacy information needs. The findings will be used by the Office: 1) to provide guidance to both individuals and organizations on privacy issues, and; 2) to enhance its outreach efforts with small businesses.

1. Collection, storage and protection of customer information

Canadian businesses continue to collect a wide variety of personal information about their customers. As identified in surveys from previous years, contact information topped the list, with the vast majority of companies (94%) collecting names, telephone numbers, and mailing or email addresses from their customers. Other types of information mentioned with some frequency include opinions, evaluations, and comments (29%), financial information, such as invoices, credit cards, or banking records (25%), and identity documents, such as Social Insurance Numbers (21%).

Nearly three-quarters (73%) of respondents said their company stores the customer information it collects on-site electronically. This marks a shift from previous years, when storing information on paper was the top storage method used by companies. At 56% (down from 62% in 2015), storage on-site on paper was the second most frequently mentioned method. Other methods of storing customer information include the use of portable devices, like laptops, USB stick, or tablets (26%), and off-site with a third-party (18%).

Turning to data protection, 94% of the businesses surveyed use at least one security method to protect the personal information of their customers. The incidence of using security methods has not changed since 2015, when 93% of businesses used a least one measure. Similar to 2015, the most common measures employed are passwords (78%) and physical measures (77%). A smaller proportion of respondents said their company uses organizational controls (60%), technological measures (59%), and system review tests and security updates (55%).

2. Company privacy practices

Consistent with 2015, approximately two-thirds of surveyed business executives (68%) said their company attributes high importance to protecting the personal information of their customers. Underscoring this importance, nearly half or more of surveyed businesses have a designated privacy officer (59%), internal policies for staff that address privacy obligations (50%), and procedures for dealing with customer complaints (51%) or customer requests to access their personal information (47%). These results are virtually

unchanged since 2015. In addition, 37% (up from 32% in 2015) provide staff with regular privacy training and education.

When the focus shifted to privacy policies, fewer than half the respondents (44%) said their company has a privacy policy that explains to customers how the company will collect and use their personal information. Among the companies that do have a privacy policy (n=486), more than nine in 10 have a policy that explains in plain language what personal information is being collected (92%) and for what purpose it is being collected (95%). In addition, three-quarters of these companies have a privacy policy that clearly explains which parties the collected personal information will be shared with. Among the companies with a privacy policy, half (52%) explain the risk of harm in the event of a breach in their policy.

3. Managing privacy risks

Executives were somewhat divided on how concerned they are about a data breach. Nearly one-quarter (23%) provided the highest rating of extremely concerned, whereas 36% said they were not concerned at all. Overall, nearly half (48%) expressed at least a moderate level of concern (scores of three or higher on the seven-point scale) and exactly half (50%) expressed low or no concern at all. The proportion of executives not concerned about a data breach has increased, from 44% in 2015 to 50% in 2017.

Four in 10 (40%) surveyed companies have policies or procedures in place in the event of a breach where customer personal information is compromised. Almost as many respondents (38%) said their company has policies or procedures in place to assess privacy risks related to their business. The proportion of businesses with policies or procedures to address data breaches and to assess privacy risks is virtually unchanged since 2015.

4. Awareness and impact of federal privacy law

Corporate awareness of responsibilities under Canada's privacy laws has not changed since 2015. When asked to rate their company's awareness of its responsibilities under Canada's privacy laws, a strong minority (44%) of business executives said their company is highly aware, while a slightly smaller proportion (38%) said their company has a moderate level of awareness. As was the case in 2015, overall, 82% of companies are at least somewhat familiar with their responsibilities under Canada's privacy laws.

Two-thirds of surveyed businesses (66%) said their company has taken steps to comply with Canada's privacy laws. This marks an increase of seven percentage points since 2015 when 59% of companies had taken such steps. Of those who have taken steps to comply (n=719), roughly nine in 10 (89%) said their company did not find it difficult. Additionally, most of the companies that took steps to comply with Canada's privacy law (66%) did not encounter any challenges. Among companies that have not taken steps to comply (n=237), nearly six in 10 (57%) do not anticipate any challenges or barriers.

5. Communications and outreach

Business executives were asked how useful potential tools or resources would be for their company in terms of helping comply with Canada's privacy laws. Just over half (53%) said that information about PIPEDA and related responsibilities would be a useful resource.

Fewer than half rated the other tools or resources as useful: 44% said online learning tools that explain PIPEDA would be useful, 43% said this about training tools to educate staff, and 35% said interactive tools to assess privacy practices would be useful (almost one-quarter did not know whether or not interactive tools would be useful).

Just over one-quarter (27%) of surveyed business executives said their company has looked for information or contacted someone for advice about their company's responsibilities under Canada's privacy laws. When asked what organizations or resources their company uses (or would use) to help clarify its privacy related responsibilities, 27% of business executives pointed to the Internet (in general), as well as to Google (14%) or to specific websites (5%). Following the Internet, 19% consulted (or would consult) the federal government, 15% a provincial government, and 14% a lawyer. More than four in 10 respondents (44%; up from 41% in 2015) were aware that the OPC has information and tools to help companies comply with privacy obligations.

Subgroup differences

As has been the case in previous years, the size of a company is the strongest predictor of a company's privacy practices. Companies with at least 100 employees tend to collect more types of personal information from customers and they are more likely to store this information on-site electronically. Additionally, large companies are more likely to have taken steps to protect their customers' personal information, to have put in place a series of privacy practices, and to have a privacy policy that explains how they collect and use customers' information. Large businesses also are more likely to have protocols in place for a data breach, as well as policies to assess privacy risks related to their business. Finally, awareness of responsibilities under Canada's privacy laws was higher among large companies, and large companies were more likely to have taken steps to ensure they comply with privacy laws.

Additional Information

Contract value:

The contract value was $58,737.40 (including applicable taxes).

Statement of Political Neutrality:

I hereby certify as a Senior Officer of Phoenix Strategic Perspectives that the deliverables fully comply with the Government of Canada political neutrality requirements outlined in the *Communications Policy* of the Government of Canada and Procedures for Planning and Contracting Public Opinion Research. Specifically, the deliverables do not contain any reference to electoral voting intentions, political party preferences, standings with the electorate, or ratings of the performance of a political party or its leader.

Alethea Woods
President
Phoenix Strategic Perspectives Inc.

Introduction

Phoenix Strategic Perspectives (Phoenix SPI) was commissioned by the Office of the Privacy Commissioner of Canada (OPC) to conduct public opinion research (POR) with Canadian businesses on privacy-related issues.

Background and Objectives

The OPC is an advocate for the privacy rights of Canadians, with the power to investigate complaints and conduct audits under two federal laws, publish information about personal information-handling practices in the public and private sectors, and conduct research into privacy issues. Mandated by Parliament to act as an ombudsman and guardian of privacy in Canada, the Commissioner is responsible for enforcing the *Personal Information Protection and Electronic Documents Act* (PIPEDA), which applies to commercial activities in the Atlantic provinces, Ontario, Manitoba, Saskatchewan and the Territories. Quebec, Alberta, and British Columbia each has its own law covering the private sector. However, even in these provinces PIPEDA continues to apply to the federally-regulated private sector and to personal information in interprovincial and international transactions.

Given its mandate, the OPC needs to understand the extent to which businesses are familiar with privacy issues and what type of privacy policies and practices they have in place. The Office also needs to assess compliance with the law. To do so, it is also important that the Office understands businesses' awareness and approaches to privacy protection. Therefore, the OPC regularly commissions surveys with businesses to inform and guide its outreach efforts with businesses.

In addition, the OPC has identified strategic priorities and approaches to help it achieve the Commissioner's vision of increasing Canadians' control over their personal information. In the summary report on the priorities, *Mapping a Course for Greater Protection*, the OPC notes that small and medium enterprises (SMEs) are in need of outreach to reinforce their understanding of their privacy obligations under PIPEDA. As such, the Office seeks to deepen its understanding of small businesses, so that it can develop appropriate materials and approaches for enhancing its outreach to small businesses.

This year's survey will help the Office to better understand the extent to which businesses are familiar with privacy issues and requirements. It will also help the Office learn more about the types of privacy policies and practices that businesses have in place, as well as their privacy information needs. The findings will be used by the Office: 1) to provide guidance to both individuals and organizations on privacy issues, and; 2) to enhance its outreach efforts with small businesses.

Methodology

A 13-minute telephone survey was administered to 1,014 companies across Canada. Businesses were divided by size for sampling purposes. A random sample frame was generated for each of the three target business size quotas: small (one-19 employees); medium (20-99 employees; and large (100+ employees). The target respondents were senior decision-makers with responsibility and knowledge of their company's privacy and security practices. The results were weighted by size, sector and region using Statistics

Canada data to ensure that they reflect the actual distribution of businesses in Canada. Based on a sample of this size, the results can be considered accurate to within ±3.1%, 19 times out of 20.

The following specifications applied to the survey:

- A telephone pre-test was conducted in English and French, with 10 interviews in each official language. Interviews were digitally recorded for review afterwards.
- Interviews were conducted in the respondent's official language of choice.
- The survey was registered with Marketing Research and Intelligence Association's (MRIA) national survey registration system.
- Respondents were informed that the survey was commissioned by the OPC.
- The response rate was 17%.
- The fieldwork was conducted from October 27 to November 30, 2017.

The following table presents information about the final call dispositions for this survey, as well as the associated response rate (using the MRIA formula)[1]:

Total Numbers Attempted	**7,322**
Out-of-scope - Invalid	**1,084**
Unresolved (U)	**1,780**
No answer/Answering machine	1,780
In-scope - Non-responding (IS)	**3,423**
Language barrier	32
Incapable of completing (ill/deceased)	58
Callback (respondent not available)	2,512
Refusal	694
Termination	127
In-scope - Responding units (R)	**1,035**
Completed interview	1,014
Quota full	1
Cell phone – not safe to talk	20

Notes to readers

- All results in the report are expressed as a percentage, unless otherwise noted.
- Throughout the report, percentages may not always add to 100 due to rounding.
- Only subgroup differences that are statistically significant at the 95% confidence level or are part of a pattern or trend are reported.
- The survey questionnaire is appended to the report.

[1] The response rate [R=R/(U+IS+R)] is calculated as the number of responding units [R] divided by the number of unresolved [U] numbers plus in-scope [IS] non-responding households and individuals plus responding units [R].

Detailed findings

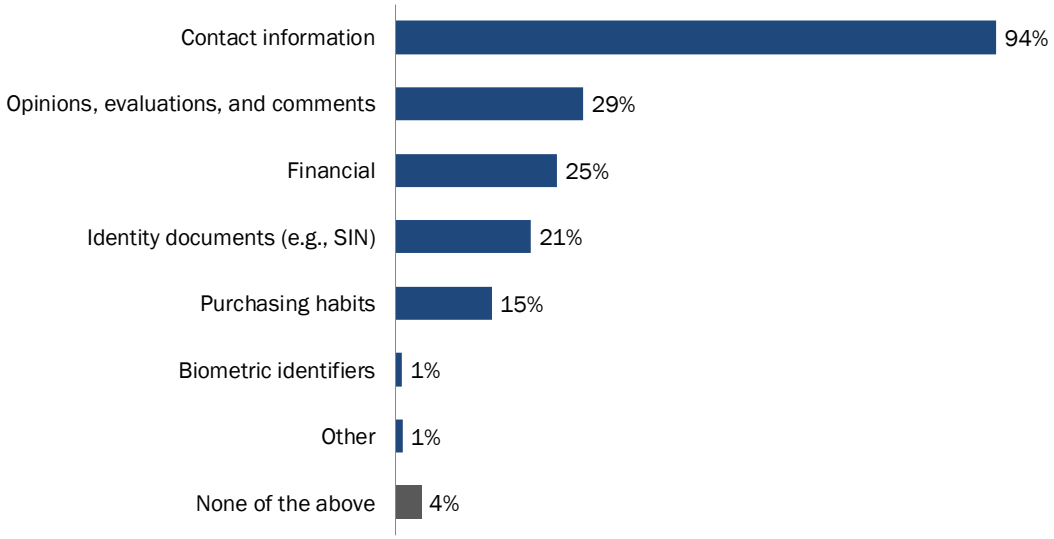
1. Collection, storage and protection of customer information

This section discusses the type of customer personal information collected by businesses, how the data is stored, and the measures taken by companies to protect it from disclosure.

Contact information—most widely collected piece of customer information

With regards to the type of information that is collected about customers, the vast majority of companies surveyed (94%) collect contact information, such as names, telephone numbers, and mailing or email addresses. Other types of information that were mentioned with some frequencey include opinions, evaluations and comments (29%), financial information, such as invoices, credit cards, or banking records (25%), and identity documents, such as Social Insurance Numbers (SIN) (21%).

Figure 1: Type of customer information collected by companies



Q3. Which of the following types of information does your company collect about your customers? [Multiple responses accepted]
Base: n=1,014; all respondents

In total, 4% of respondents said their company does not collect any of these types of customer information.

Since tracking began in 2011, the type of customer information collected by companies has changed little. Contact information, financial information and feedback remain the most frequently collected customer information.

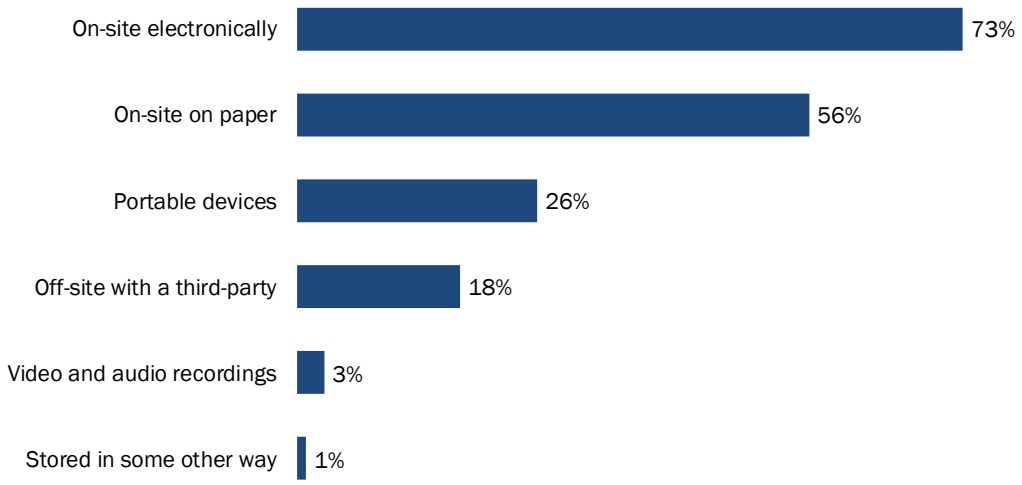
The likelihood of collecting information about their clients generally increases as the size of the business increases. Large companies (those with 100 or more employees) were more likely to collect opinions, evaluations, and comments (45%), financial information (45%), identity documents (32%), and purchasing habits from their customers (28%).

Variety of methods used to store personal information

Businesses reported using a variety of methods to store customers' personal information. Topping the list was on-site electronically, with nearly three-quarters (73%) of respondents saying their business stores customer information this way. Following this, 56% of respondents said their business stores customers' personal information on-site on paper. This represents a noteworthy shift from previous years, when on-site paper storage was the top method used by businesses.

In addition, roughly one-quarter (26%) of businesses store customer information on portable devices, like laptops, USB sticks, or tablets. Eighteen percent said their business stores customer information off-site electronically with a third-party.

Figure 2: Methods used by companies to store personal information



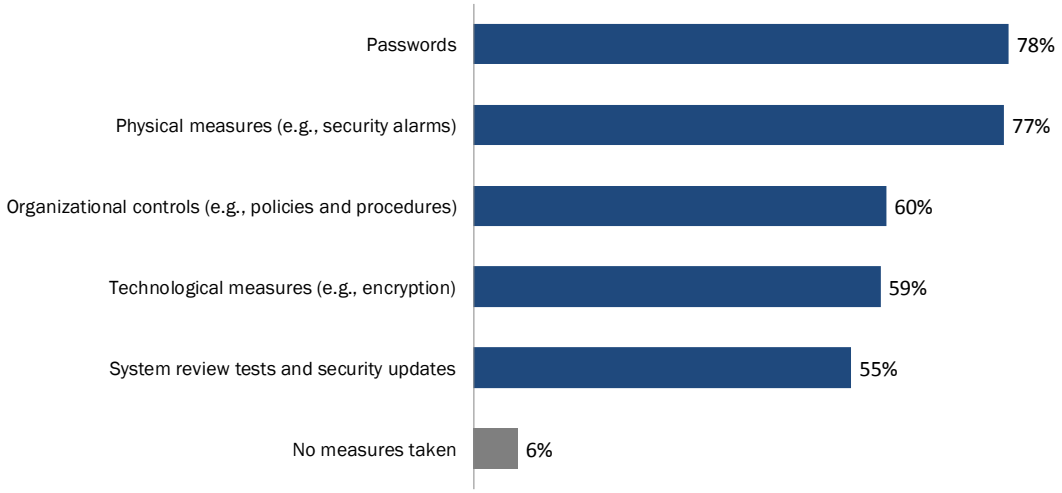
Q4. In which of the following ways does your company store personal information on your customers? [Multiple responses accepted]
Base: n=1,014; all respondents; DK/NR=6%

Sole proprietorship businesses are most likely to store customers' personal information on portable devices (45%). The likelihood of storing this information on-site electronically generally increased with business size, from 53% of sole proprietorships to 84% of companies employing 100 or more employees.

Electronic and physical measures taken to protect personal information

The vast majority of surveyed businesses (94%) use at least one security method to protect the personal information of customers. Passwords continue to be the most commonly used security measure, with almost four in five (78%) businesses using them to protect customers' personal information. Closely following this is the use of physical methods, such as security alarms (77%). Smaller proportions use organizational controls, such as policies and procedures (60%), technological measures, like encryption (59%), and system review tests and security updates (55%).

Figure 3: Steps taken by companies to protect customers' information



Q5. What steps do you take to protect the personal information on your customers? [Multiple responses accepted]
Base: n=1,014; all respondents; DK/NR=1%

The likelihood of taking steps to protect customers' personal information increased with business size. Large businesses were more likely to use passwords (94%), organizational controls (89%), system review tests and security updates (85%), and technological measures like encryption (84%) to protect their customers' information.

Businesses located in Quebec tend to use fewer methods of protection for their customers' information than those in other regions. Additionally, businesses located in the Prairies (75%) were significantly more likely to use technological measures than those in Quebec (42%), Atlantic Canada (49%), and Ontario (61%).

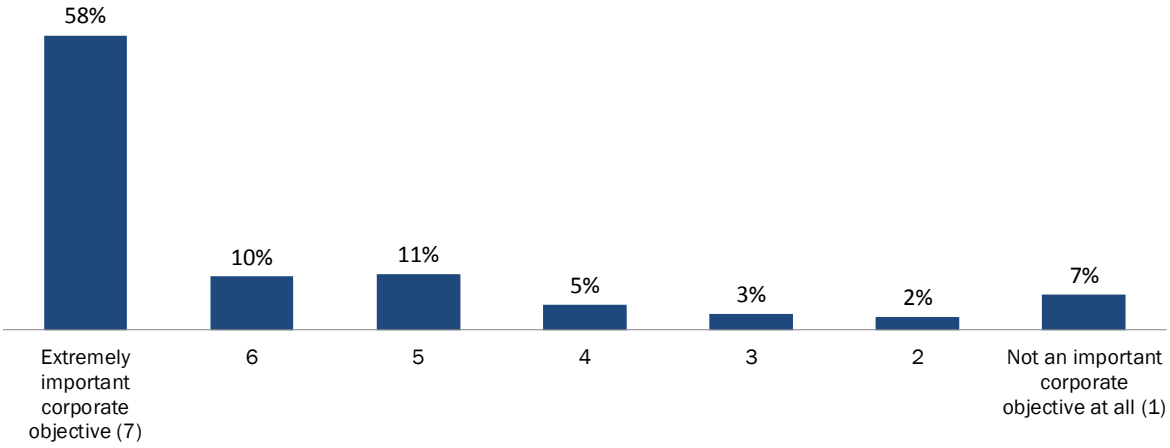
2. Company privacy practices

This section identifies the procedures and policies companies have in place to protect the personal information they collect about their customers.

Most attribute high importance to protecting customers' privacy

Most businesses attribute importance to protecting their customers' personal information. Nearly three in five (58%) chose the highest score available (on a seven-point scale), indicating they believe that protecting customers' personal information is an extremely important objective for their company. Over two-thirds said that protecting customers' privacy is highly important (scores of six to seven). The remaining (19%) were more likely to attribute moderate importance to this (scores of three to five). Only 9% of respondents indicated that protecting customers' personal information is not an important objective for their company.

Figure 4: Importance companies attribute to protecting customers' privacy

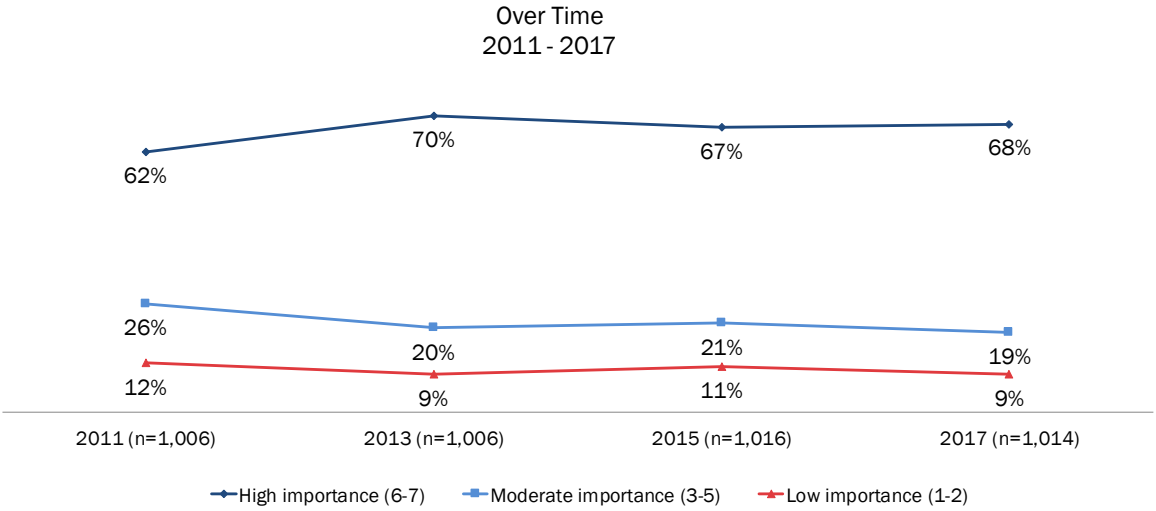


Q13. What importance does your company attribute to protecting your customers' personal information?
Base: n=1,014; all respondents; DK/NR=3%

The likelihood of attributing high importance (scores of six to seven) was higher among businesses located in Ontario (74%), and specifically, in the Greater Toronto Area (76%) compared to Alberta (61%). Businesses with two to four employees (59%) were less likely than sole proprietorships (73%) and larger businesses to attribute high importance to protecting their customers' personal information. Among larger businesses, 68% of those with five to nine employees, 76% of those with 10 to 19 employees, 71% of those with 20-99 employees, and 79% of those with 100+ employees attributed high importance to protecting customers' personal information.

Compared to 2015, the importance attributed to protecting customers' personal information is virtually unchanged. Since 2013, importance has fluctuated by no more than three percentage points, and, at 67%, it remains higher than the baseline of 62% recorded in 2011.

Figure 5: Importance companies attribute to protecting customers' privacy over time



Q13. What importance does your company attribute to protecting your customers' personal information?

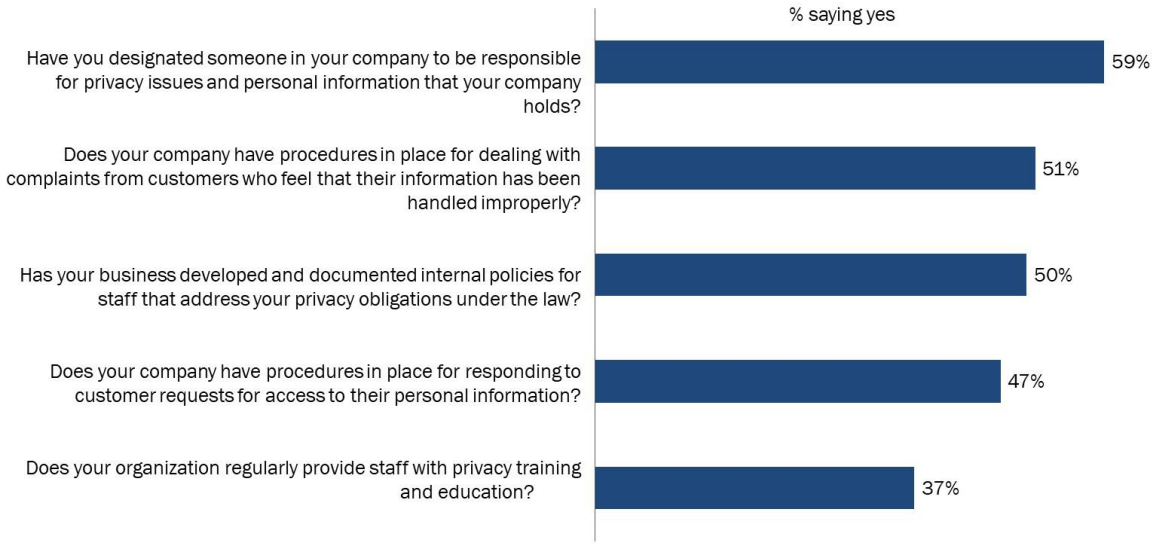
Uneven implementation of privacy compliance practices

Business representatives were asked whether their company had put in place a series of privacy practices. These included:

- Having designated someone in their company to be responsible for privacy issues and personal information that the company holds;
- Having developed and documented internal policies for staff that address their privacy obligations under the law;
- Having staff regularly receive privacy training and education;
- Having procedures in place for responding to customer requests for access to their personal information; and
- Having procedures in place for dealing with complaints from customers who feel that their information has been handled improperly.

Three of these practices have been put in place by half, or more, of surveyed businesses. This includes having a designated privacy officer (59%), procedures for dealing with complaints from customers (51%), and internal policies for staff that address privacy obligations (50%). Almost half (47%) said their company has procedures in place for responding to customer requests for access to their personal information. Respondents were least likely to say that their company regularly provides staff with privacy training and education (37%).

Figure 6: Companies' privacy compliance practices



Q6 to Q10.
Base: n=1,014; all respondents [DK/NR=5% or less]

Businesses with 100 or more employees, and those with revenues over $20 million, were more likely to have put in place each of these privacy practices. The likelihood of not having implemented these privacy practices, generally, was higher among businesses located in Quebec.

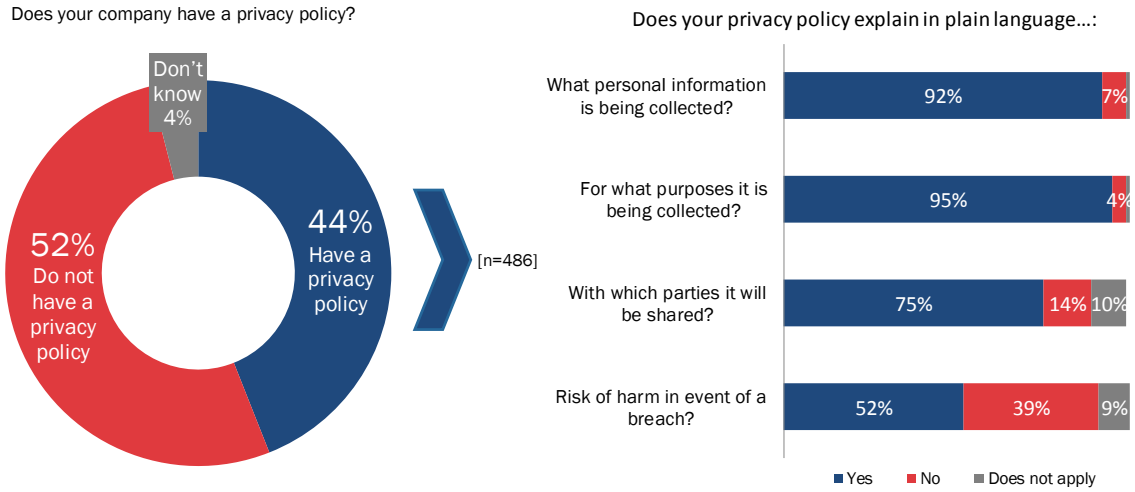
Among the practices that have been tracked, the proportion of companies implementing them has changed very little since 2015. The only notable increase since 2015 was in the proportion of businesses that provide staff with regular privacy training and education (37% in 2017 versus 32% in 2015).

Fewer than half of companies have a privacy policy

When asked if their company has a privacy policy that explains to customers how they collect and use customers' personal information, fewer than half (44%) the respondents said their company did. Conversely, 52% said their company does not have such a privacy policy.

Among the companies that do have a privacy policy (n=486), more than nine in 10 have a policy that explains in plain language what personal information is being collected (92%) and for what purpose it is being collected (95%). In addition, three-quarters of these companies have a privacy policy that explains plainly which parties the collected personal information will be shared with. Among the companies with a privacy policy, only 52% explain the risk of harm in the event of a breach in their policy.

Figure 7: Privacy policies



Q11. [left] Does your company have a privacy policy that explains to customers how you will collect and use their personal information?
Base: n=1,014; all respondents
Q12. [right] Does your privacy policy explain in plain language…?
Base: n=486; companies with privacy policies

Businesses with 100 or more employees, and those with revenues over $20 million, were more likely to have a privacy policy that explains how they collect and use customers' personal information (66% and 74% respectively). Regionally, businesses located in Ontario (50%), and specifically, in the GTA (58%), as well as in the Prairies (52%) were more likely than businesses in Quebec (38%) to have a privacy policy.

3. Managing privacy risks

This section examines respondents' level of concern about, and plans for dealing with, data breaches.

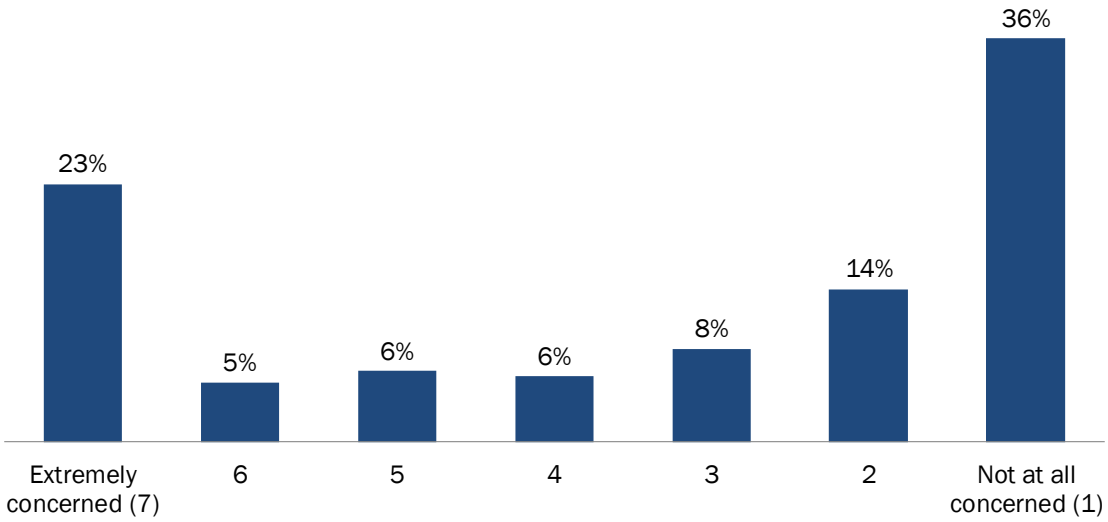
Businesses split on concern over data breach

There was a divide among surveyed executives with regards to how concerned they are about a data breach. Nearly one-quarter (23%) provided the highest rating of extremely concerned, whereas 36% said they were not concerned at all. Overall, nearly half (48%) expressed at least a moderate level of concern (scores of three or higher on the seven-point scale) and half (50%) expressed low or no concern at all.

Before being asked this question, respondents were provided with the following information:

> *Data breaches can be caused by criminal activity, theft, hacking, or employee error such as misplacing a laptop or portable device.*

***Figure 8*: Concern about a data breach affecting customers' personal information**

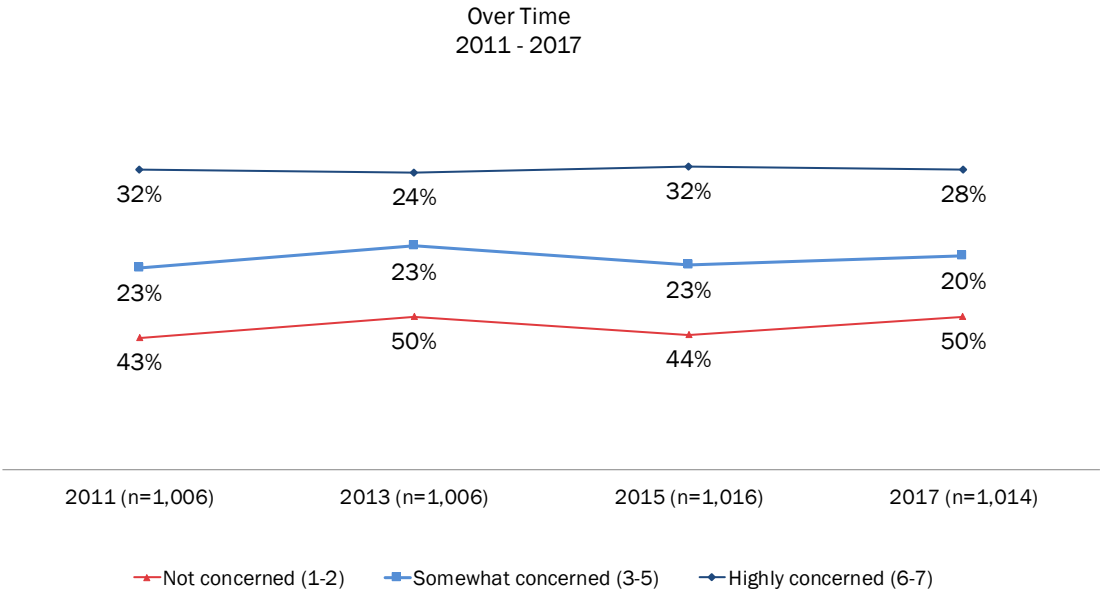


Q18. How concerned are you about a data breach, where the personal information of your customers is compromised?
Base: n=1,014; all respondents [DK/NR=2%]

Businesses located in Quebec were far more likely to say they are highly concerned (scores of six to seven) about a data breach (48% compared to a low of 15% of businesses in Alberta to a high of 29% of businesses in British Columbia and in the GTA).

Levels of concern about a data breach have decreased from 2015, with the proportion of executives highly concerned (six to seven out of seven) about a data breach having declined down four percentage points. Additionally, the proportion of executives not concerned about a data breach has increased six percentage points, from 44% in 2015 to 50% in 2017.

Figure 9: Concern about a data breach affecting customers' personal information over time

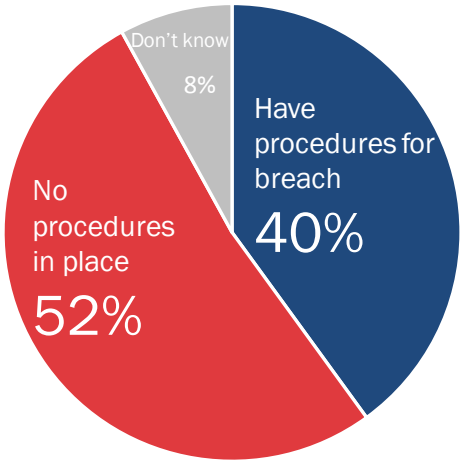


Q18. How concerned are you about a data breach, where the personal information of your customers is compromised?

Strong minority have protocols for data breach

A strong minority (40%) said their company has protocols or procedures in place that are to be followed in the event of a breach in which their customers' personal information is compromised. Conversely, 52%, said their company does not have any protocols or procedures in place (8% were uncertain whether or not their business has protocols).

Figure 10: Protocols in place for data breach



Q19. Does your company have any protocols or procedures in place that would be followed in the event of a breach where the personal information of customers is compromised?
Base: n=1,014; all respondents

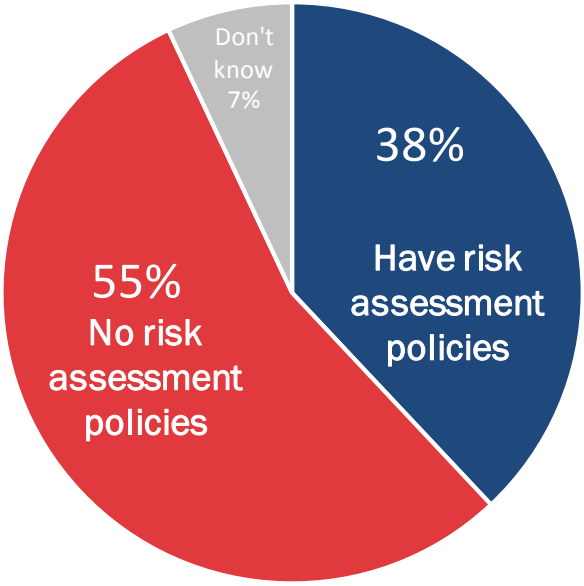
Business that have 100 or more employees (61%) and that have revenues of over $20 million (79%) were more likely to have procedures in place in case of a data breach. In fact, the likelihood of respondents saying their company has procedures in place increased with business size and business revenues. Regionally, businesses in Ontario (46%), and specifically in the GTA (54%), were more likely than those located in Quebec and Atlantic Canada (31% each) to have these types of procedures.

The proportion of businesses with policies or procedures to address data breaches is virtually unchanged since 2015.

Few companies have policies to assess privacy risks

Almost four in 10 respondents (38%) said their company has policies or procedures in place to assess privacy risks related to their business. On the contrary, just over half (55%) said they do not have any assessment policies in place (7% were not sure if they have risk assessment policies or not).

Figure 11: **Corporate policies in place to assess privacy risks**



Q20. Does your company have any policies or procedures in place to assess privacy risks related to your business? This includes assessing privacy risks associated with the development or use of new products, services, or technologies.
Base: n=1,014 all respondents

At 66%, businesses with over 100 employees are most likely to have policies or procedures in place to assess privacy risks related to their business. Additionally, companies with revenues under $10 million were more likely to *not* have put in place risk assessment policies (62% under $1 million and 58% $1 million to under $10 million).

The proportion of Canadian businesses that have policies or procedures in place to assess privacy risks has not changed since 2015, when 37% of respondents said their company had these measures in place.

4. Awareness and impact of federal privacy law

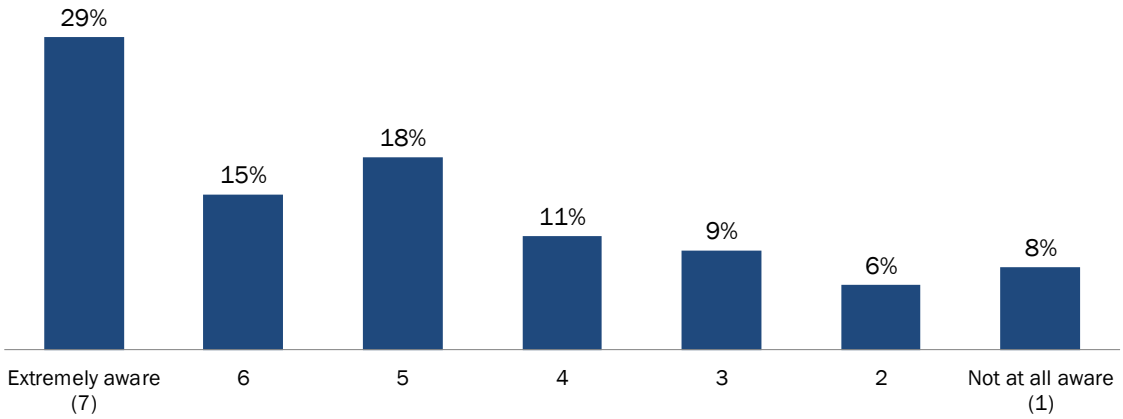
This section examines findings regarding companies' awareness of their responsibilities under privacy laws. Questions in this section were prefaced with the following description of Canada's privacy laws:

> *The federal government's privacy law, the* Personal Information Protection and Electronic Documents Act *or PIPEDA, sets out rules that govern how businesses engaged in commercial activities should protect personal information. In Alberta, BC and Quebec, the private sector is governed by provincial laws, which are considered to be similar to the federal law.*

Moderate level of awareness of responsibilities under privacy laws

When respondents were asked to rate their company's awareness of its responsibilities under Canada's privacy laws, a strong minority (44%) indicated that they think their company is highly aware of its responsibilities (scores six or seven on the scale). Of these respondents, 29% said their company is extremely aware. A somewhat smaller proportion (38%) rated their company as moderately aware with regards to its privacy responsibilities (scores of three to five). Fourteen percent rated their company's awareness as low (scores of one to two).

Figure 12: Companies' awareness of responsibilities under privacy laws



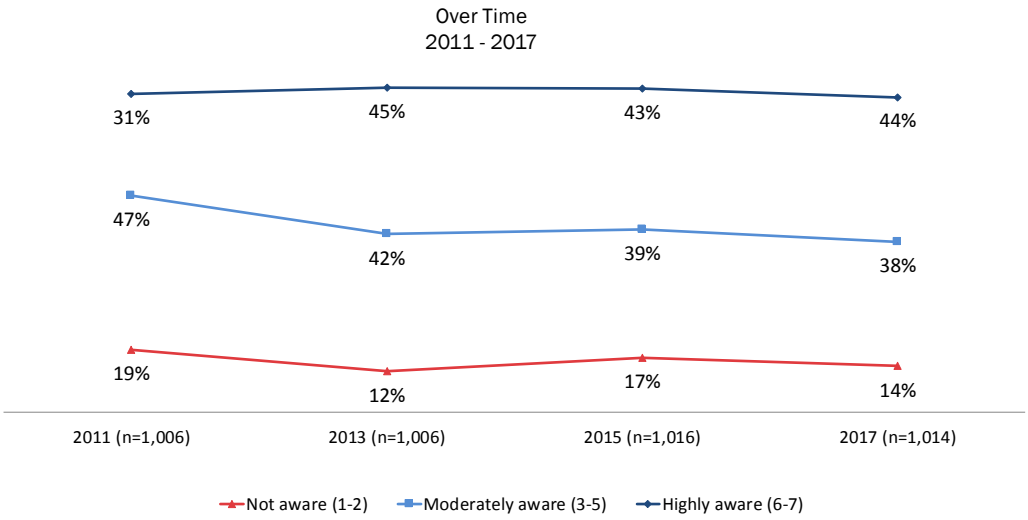
Q14. How would you rate your company's awareness of its responsibilities under Canada's privacy laws?
Base: n=1,014; all respondents [DK/NR=4%]

The likelihood of saying their company is aware of its responsibilities under Canada's privacy laws was higher among respondents from businesses in the GTA (51%) compared to those located in Atlantic Canada (26%) and in British Columbia (36%). Businesses that have 100 or more employees (64%), and those that have revenues of over $20 million (54%) were more likely to rate their company's awareness of its responsibilities under Canada's privacy laws as high (scores of six to seven).

Compared to 2015, there has been a slight decrease in the proportion of executives that rated their company's awareness as low (from 17% in 2015 to 14% in 2017). However,

the proportion of respondents who said their company has a high level of awareness of their responsibilities is virtually unchanged from 2015.

Figure 13: Companies' awareness of responsibilities under privacy laws over time

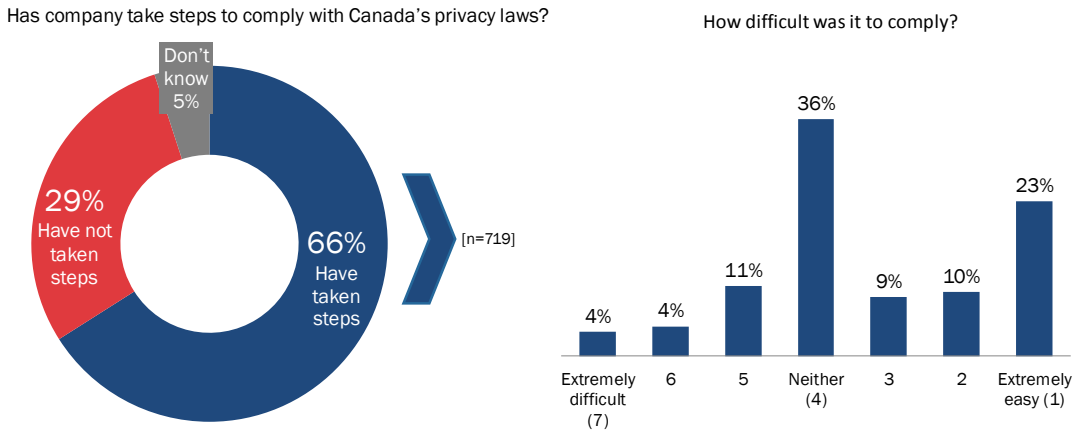


Q14. How would you rate your company's awareness of its responsibilities under Canada's privacy laws?

Two-thirds have taken steps to comply with privacy laws

Two-thirds of executives surveyed (66%) said their company has taken steps to ensure it complies with Canada's privacy laws. Roughly nine in 10 (89%) of those who have taken steps to comply (n=719) did not find compliance difficult.

Figure 14: **Compliance with Canada's privacy laws**



Q15. [left] Has your company taken steps to ensure that it complies with Canada's privacy laws?
Base: n=1,014; all respondents
Q16. [right] How difficult has it been for your company to bring your personal information handling practices into compliance with Canada's privacy laws? Base: n=719; companies that have taken steps [DK/NR=3%]

The likelihood of having taken steps, generally, increased with business size, from 58% of businesses with fewer than five employees to 91% of businesses with 100 or more employees. The same pattern was evident when the focus was on corporate revenues, with the likelihood of having taken steps increasing with a company's annual revenues.

Businesses located in Atlantic Canada were less likely to have taken steps to comply with Canada's privacy laws (49% compared to 54% of businesses in Quebec, 67% of businesses in Alberta, 68% of businesses in British Columbia, 71% of businesses in Ontario, and 72% of businesses in the Prairies).

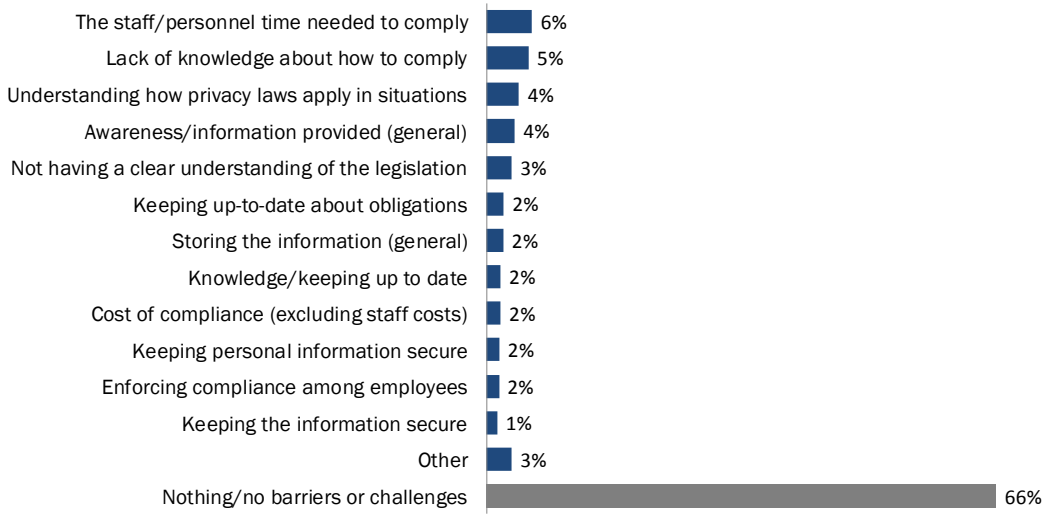
Compared to 2015[2], there has been an increase in the proportion of business executives that indicated their company has taken steps to comply with Canada's privacy law (from 59% in 2015 to 66% in 2017).

Sole proprietor companies and companies with five to nine employees were more likely than companies with 100 or more employees to find it easy to comply with Canada's privacy laws (41% and 38%, respectively vs. 21%).

Very few challenges encountered or anticipated

Of those executives who said they have taken steps to comply with privacy laws, fewer than two in five (38%) said they encountered any challenges when complying. The majority (66%) did not encounter any challenges. Figure 15 depicts the proportions that mentioned each of the challenges encountered.

Figure 15: Challenges encountered when complying with Canada's privacy laws



Q17. Thinking about the steps your company has taken to comply with Canada's privacy laws, what challenges, if any, did it encounter? [Multiple responses accepted]
Base: n=777; companies that have taken steps to comply [DK/NR=9%]

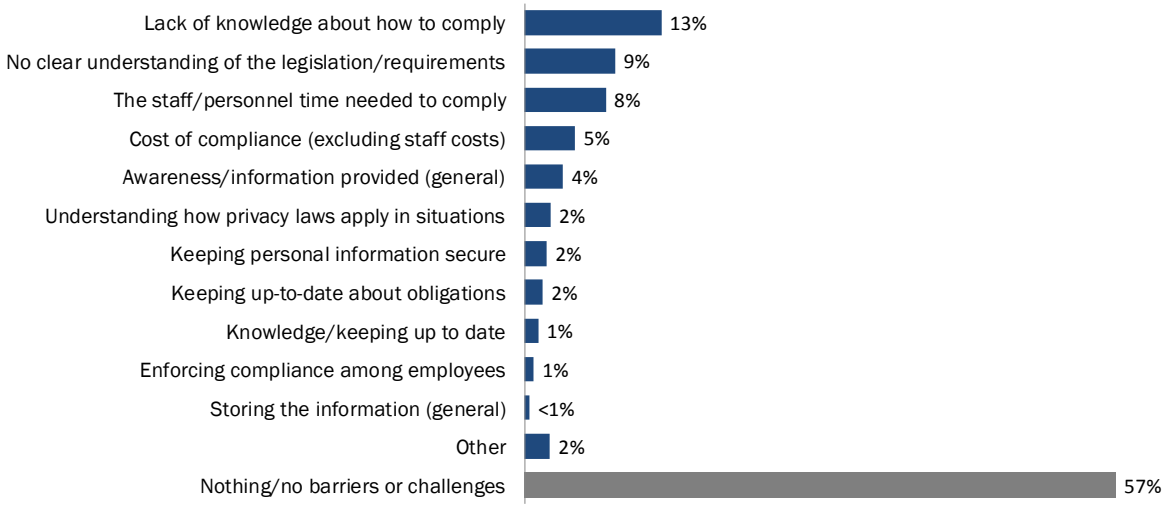
[2] In 2017 the question wording was changed to "Has your company taken steps to ensure that it complies with Canada's privacy law" from "Still thinking specifically about PIPEDA, has your company taken steps to ensure that it complies with the federal government's privacy law". For this reason, comparisons over time should be viewed with caution.

The likelihood of saying their company experienced no challenges or barriers was higher among respondents from businesses located in Alberta (77%) than respondents from businesses located in British Columbia (53%). Respondents from companies with fewer than 20 employees were more likely than those from larger companies to say their company encountered no challenges.

Turning to companies that have not taken steps to comply with Canada's privacy laws (n=237), 57% said they did not anticipate encountering any challenges or barriers to complying with Canada's privacy laws. Among the rest, lack of knowledge (13%) about how to comply was the most commonly cited challenge. This was followed by no clear understanding of the legislation or requirements (9%) and the staff or personal time needed to comply (8%).

As Figure 16 depicts, other challenges were cited by no more than 5% of business executives.

Figure 16: Challenges anticipated when complying with Canada's privacy laws



Q17A. What challenges, if any, do you think your company might encounter when it comes to ensuring that it complies with Canada's privacy laws? [Multiple responses accepted]
Base: n=237; companies that have not taken steps to comply [DK/NR=14%]

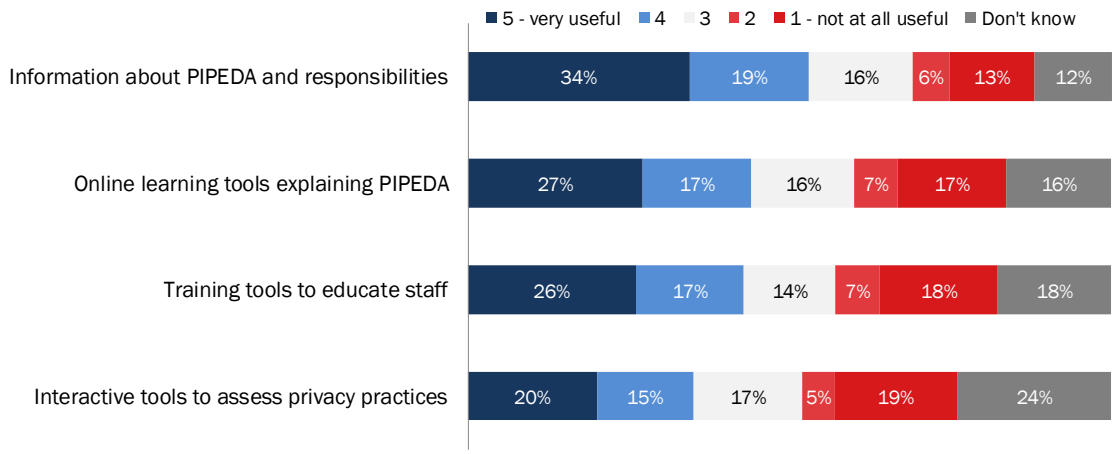
5. Communications and outreach

This section describes executives' feedback on issues related to communications and outreach.

Among a list of potential tools and resources that could help businesses comply with privacy laws, respondents were most likely to view information about PIPEDA and responsibilities as useful

When business executives were asked how useful potential tools or resources would be in terms of helping their company comply with Canada's privacy laws, information about PIPEDA and responsibilities was ranked as the most useful. Just over half (53%) said that information about PIPEDA and related responsibilities would be a useful resource. Fewer than half rated the other tools or resources as useful: 44% said online learning tools that explain PIPEDA would be useful, 43% said this about training tools to educate staff, and 35% said interactive tools to assess privacy practices would be useful (almost one-quarter did not know whether or not interactive tools would be useful).

Figure 17: Perceived usefulness of various potential tools/resources



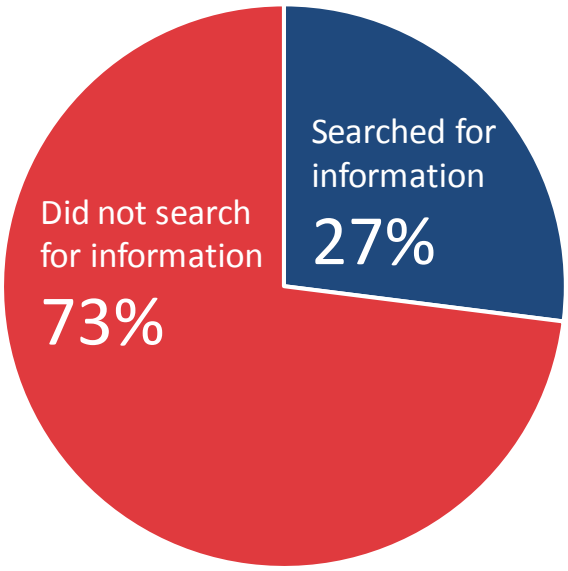
17B. How useful would the following tools or resources be in helping your company comply with Canada's privacy laws?
Base: n=1,014; all respondents

The likelihood of rating the tools and resources as useful (scores of four to five on a five-point scale) increased with business size. Conversely, representatives of sole proprietorship businesses were more likely to rate the tools and resources as not useful (scores of one or two) compared to respondents from businesses with more than one employee. Regionally, respondents from companies located in Quebec and Alberta were generally less likely to attribute value to these tools and resources in terms of helping their company comply with Canada's privacy laws.

Just over one-quarter looked for information on privacy law compliance

When business executives were asked if their company has ever looked for information, or contacted anyone for advice about its responsibilities under Canada's privacy law, just over one-quarter (27%) had. Conversely, nearly three-quarters (73%) said their company had not looked for such information.

Figure 18: Searched for information on privacy law compliance



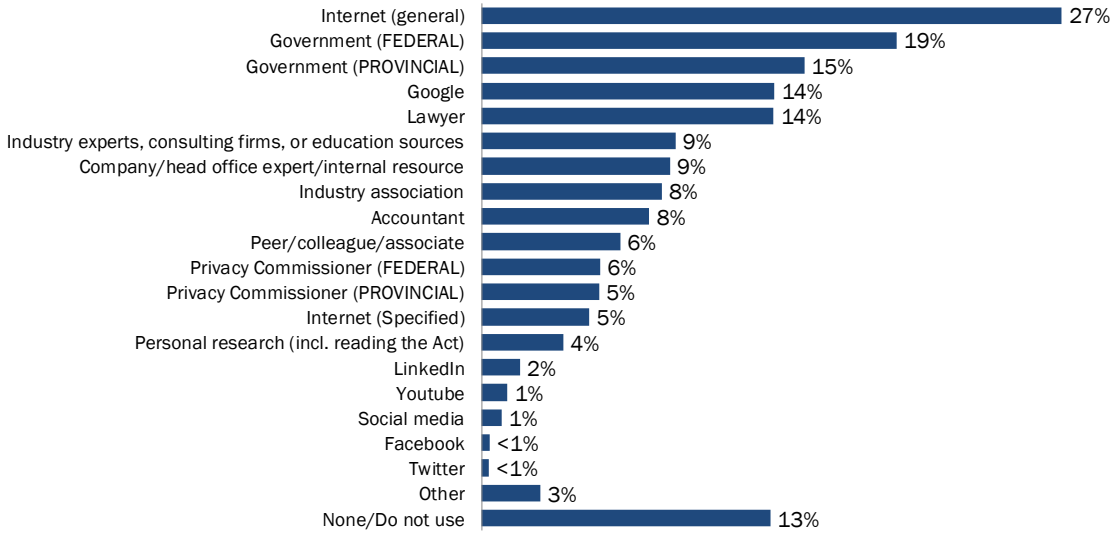
Q21A. Has your company ever looked for information, or contacted anyone for advice, about its responsibilities under Canada's privacy laws?
Base: n=1,014 all respondents

The likelihood of looking for information or contacting someone for advice about their company's responsibilities under Canada's privacy laws increased with business size, from 14% of sole proprietorship businesses to 58% of businesses with 100 or more employees.

Internet—top source for privacy law compliance information

With regards to which organizations or resources companies use to help clarify their responsibilities under Canada's privacy laws, 27% of business executives pointed to the Internet (in general), as well as to Google (14%) or to specific websites (5%). Following the Internet, 19% consulted (or would consult) the federal government, 15% a provincial government, and 14% a lawyer. Other sources were cited by smaller proportions as illustrated by Figure 19.

Figure 19: **Sources used to help comply with Canada's privacy laws**



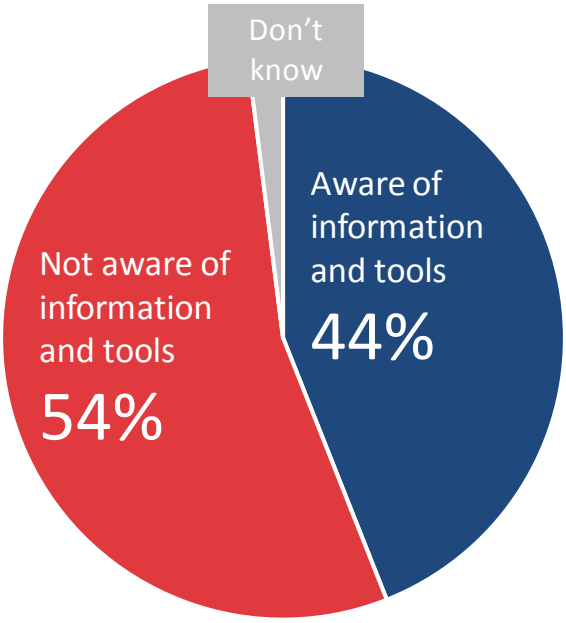
Q21. What organizations or resources [did / would] your company use to help clarify its responsibilities under Canada's privacy laws? [Multiple responses accepted]
Base: n=1,014 all respondents [DK/NR=12%]

Representatives of businesses with 100 or more employees were more likely to say their company uses lawyers as a resource to help clarify their responsibilities under Canada's privacy laws (25% versus 9% of sole proprietorship businesses to 21% of companies with 20 to 99 employees). The likelihood of not consulting any resources generally increased as business size decreased, from 8% of businesses with 100 or more employees to 28% of sole proprietorship businesses.

Almost half aware of resources provided by the OPC

Close to half (44%; up from 41% in 2105) of business executives surveyed were aware that the OPC has information and tools to help companies comply with their privacy obligations. Conversely, 54% said they were not aware of the OPC's resources.

Figure 20: **Awareness of OPC resources**



Q22. Are you aware that the Office of the Privacy Commissioner of Canada has information and tools available to companies to help them comply with their privacy obligations?
Base: n=1,014 all respondents

At 24%, awareness that the OPC has information and tools available to help businesses comply with their privacy obligations was lowest in Quebec.

6. Corporate profile

The following tables present the characteristics of survey respondents (using weighted data).

Customer type	Percent
Sells directly to consumers	37%
Sells directly to other businesses/organizations	25%
Sells directly to consumers and other businesses/organizations	37%
Is a government organization	<1%
Other	1%

Region	Percent
Atlantic Canada	6%
Quebec	20%
Manitoba and Saskatchewan	7%
Alberta	15%
British Columbia	15%
Ontario (excluding the Greater Toronto Area)	20%
Greater Toronto Area	18%

Business size	Percent*
Self-employed (1 employee)	13%
Small (2-19 employees)	73%
Medium (20-99 employees)	10%
Large (100+ employees)	2%
Don't know / no response	2%

Language of interview	Percent
English	82%
French	18%

Revenues in 2016	Percent*
Less than $100,000	16%
$100,000 to just under $250,000	15%
$250,000 to just under $500,000	11%
$500,000 to just under $1,000,000	11%
$1,000,000 to just under $5,000,000	17%
$5,000,000 to just under $10,000,000	3%
$10,000,000 to just under $20,000,000	1%
More than $20 million	2%
Don't know / no response	23%

*Percentages do not sum to 100% due to rounding error.

Appendix

Annex 1: Survey Questionnaire

SCRIPT

Hello, my name is [Interviewer's name]. I'm calling on behalf of Phoenix, a public opinion research company. We're conducting a survey for the Privacy Commissioner of Canada to better understand the needs and practices of businesses across the country in relation to Canada's privacy laws.

Would you prefer to continue in English or French? / Préférez-vous continuer en anglais ou en français?

May I speak to the person in your company who is the most familiar with the types of personal information collected about your customers, and how this information is stored and used. This may be your company's Privacy Officer if you have one.

- IF PERSON IS AVAILABLE, CONTINUE. REPEAT INTRODUCTION IF NEEDED.
- IF NOT AVAILABLE, SCHEDULE CALL-BACK.

The survey takes about 10 minutes. Please note that your responses will be kept entirely confidential and anonymous, and that this survey is registered with the Marketing Research and Intelligence Association (MRIA).

May I continue?

- Yes, now [CONTINUE]
- No, call later. Specify date/time: Date: Time:
- Refused [THANK/DISCONTINUE]

INTERVIEWER NOTES:

IF RESPONDENT ASKS ABOUT THE LENGTH OF THE SURVEY, INFORM HIM/HER IT IS SHOULD TAKE APPROXIMATELY 10 MINUTES.

IF RESPONDENT QUESTIONS THE VALIDITY OF THE SURVEY, OFFER TO FAX/EMAIL HIM/HER THE VALIDATION LETTER FROM THE OPC. IF THIS DOES NOT SATISFY THE POTENTIAL RESPONDENT, ASK HIM/HER TO CALL HEATHER ORMEROD OF THE OFFICE OF THE PRIVACY COMMISSIONER AT 819-994-5682 (OR HAVE HEATHER CALL THE RESPONDENT).

IF RESPONDENT ASKS, THE SURVEY IS REGISTERD WITH THE NATIONAL SURVEY REGISTRATION SYSTEM:

The registration system has been created by the survey research industry to allow the public to verify that a survey is legitimate, get information about the survey industry or register a complaint. The registration system's toll-free phone number is 1-888-602-6742 ext. 8728.

SOME QUESTIONS ARE TRACKING QUESTIONS THAT WERE USED IN EARLIER SURVEYS. TRACKING QUESTIONS ARE IDENTIFIED AS FOLLOWS: T2015 = TRACKING (T) FROM THE 2015 BUSINESS SURVEY.

SECTION HEADINGS SHOULD NOT BE READ TO RESPONDENTS

FOR ALL QUESTIONS, INCLUDE 'DON'T KNOW/NO RESPONSE' OPTION

1. Which of the following best describes your company? [READ LIST, ACCEPT ONE RESPONSE] T2015

It sells directly to consumers
It sells directly to other businesses/organizations
It sells directly both to consumers and other businesses/organizations
Other, please specify:

[DO NOT READ: IF NOT FOR PROFIT OR DON'T KNOW/NO RESPONSE, THANK AND TERMINATE]

*INTERVIEWER NOTE: IF ASKED ABOUT RESPONSE OPTION (1) "CONSUMERS", SAY: This refers to an individual not a business or organization.

2. Approximately how many employees work for your company in Canada? Please include part-time employees as full-time equivalents. [DO NOT READ LIST]

One (i.e. self-employed)
2-4
5-9
10-19
20-49
50-99
100-149
150-199
200-249
250-299
300-499
500-999
1,000-4,999
More than 5,000

Section 1: Privacy Practices

I'd like to begin by asking you about the types of personal information held by your company about your customers. T2015

3. Which of the following types of personal information does your company collect about your customers? [READ LIST. ACCEPT ALL THAT APPLY] T2015: MODIFIED

Contact information, such as names, phone numbers, and addresses
Opinions, evaluations, and comments

Preferences or purchasing habits for marketing purposes
Biometric identifiers, such as fingerprints, DNA, facial or voice recognition
Financial
Identity documents, such as a driver's license or Social Insurance Number
Other information
[DO NOT READ] If so, please specify: _____
[DO NOT READ] None of the above

4. In which of the following ways does your company **store** personal information on your customers? Is the information…? [READ LIST. ACCEPT ALL THAT APPLY] T2015

Stored on-site on paper
Stored on-site electronically
Stored on portable devices, such as laptops, USB sticks, or tablets
Stored off-site with a third-party
Stored by video and audio recordings
Stored in some other way: If so, please specify

5. What steps do you take to protect the personal information on your customers? Do you use…. [READ LIST. ACCEPT ALL THAT APPLY] T2015: MODIFIED

Physical measures, such as locked filing cabinets, restricting access, or security alarms
Passwords
Technological measures, such as encryption or firewalls
System review tests and security updates
Organizational controls, such as policies and procedures
Some other measure [DO NOT READ] If so, please specify:
No measures taken

6. Have you designated someone in your company to be responsible for privacy issues and personal information that your company holds? T2015

Yes
No

7. Has your business developed and documented internal policies for staff that address your privacy obligations under the law? T2015

Yes
No

8. Does your organization regularly provide staff with privacy training and education? T2015

Yes
No

9. Does your company have procedures in place for responding to customer requests for access to their personal information? T2015

Yes
No

10. Does your company have procedures in place for dealing with complaints from customers who feel that their information has been handled improperly? T2015

Yes
No

11. Does your company have a privacy policy that explains to customers how you will collect and use their personal information? T2015

Yes
No

IF YES:

12. Does your privacy policy explain in plain language...? [READ LIST]

a) What personal information your company is collecting from customers
b) For what purposes customers' personal information is being collected, used or disclosed
c) With which parties customers' personal information will be shared
d) The risk of harm to the individual, if any, in the event of data breach

RESPONSE OPTIONS:

Yes
No
Does not apply

INTERVIEWER NOTE: If a respondent answers "yes" at Q11, but then volunteers that they don't have a formal privacy when asked Q12, please edit the response to Q11 so it is "no".

Section 2: Privacy as Corporate Objective

13. What importance does your company attribute to protecting your customers' personal information? Please use a scale from 1 to 7, where 1 means that this is **not** an important corporate objective at all, and 7 means it is an extremely important objective. T2015

Section 3: Awareness of Privacy Laws

The federal government's privacy law, the *Personal Information Protection and Electronic Documents Act* or PIPEDA (PRONOUNCED PIP-EE-DAH) sets out rules that govern how businesses engaged in commercial activities should protect personal information. In Alberta, BC and Quebec, the private sector is governed by provincial laws, which are considered to be similar to the federal law. T2015

14. How would you rate your company's awareness of its responsibilities under Canada's privacy laws? Please use a scale from 1 to 7, where 1 is not at all aware, and 7 is extremely aware. T2015

Section 4: Compliance

15. Has your company taken steps to ensure that it complies with Canada's privacy law? T2015: MODIFIED

Yes CONTINUE
No GO TO Q17A

16. How difficult has it been for your company to bring your personal information handling practices into compliance with Canada's privacy laws? Please use a scale from 1 to 7, where 1 is extremely easy, 7 extremely difficult and 4 is neither easy nor difficult. T2013

17. Thinking about the steps your company has taken to comply with Canada's privacy laws, what challenges, if any, did it encounter? Anything else? [DO NOT READ LIST. PROBE FULLY FOR SPECIFICS. ACCEPT MULTIPLE RESPONSES]

No clear understanding of the legislation/requirements
Lack of knowledge about how to comply
The staff/personnel time needed to comply
The cost of compliance (excluding staff costs)
Enforcing compliance among employees
Understanding how privacy laws apply in situations
Keeping up-to-date about obligations
Keeping personal information secure
Other: [DO NOT READ] Specify
Nothing/no barriers or challenges

ASK THOSE WHO SAID 'NO' AT Q15:

17A. What challenges, if any, do you think your company might encounter when it comes to ensuring that it complies with Canada's privacy laws? Anything else? [DO NOT READ LIST. PROBE FULLY FOR SPECIFICS. ACCEPT MULTIPLE RESPONSES]

No clear understanding of the legislation/requirements
Lack of knowledge about how to comply
The staff/personnel time needed to comply
The cost of compliance (excluding staff costs)
Enforcing compliance among employees
Understanding how privacy laws apply in situations
Keeping up-to-date about obligations
Keeping personal information secure
Other: [DO NOT READ] Specify
Nothing/no difficulties

ASK EVERYONE:

17B. How useful would the following tools or resources be in helping your company comply with Canada's privacy laws? When answering, please use a 5-point scale, where 1 means not at all useful and 5 means very useful. If something does not apply to your company, just say so.

a) Interactive tools your company can use to assess your privacy practices.
b) Online learning tools explaining PIPEDA*.
c) Training tools your company could use to educate staff.
d) Information about PIPEDA and your responsibilities.

*INTERVIEWER NOTE: IF ASKED ABOUT PIPEDA, SAY: PIPEDA is the federal privacy law, which applies in most provinces, and which sets out rules that govern how businesses engaged in commercial activities should protect personal information.

Section 5: Breaches

Data breaches can be caused by criminal activity, theft, hacking, or employee error such as misplacing a laptop or other portable device. T2015: MODIFIED

18. How concerned are you about a data breach, where the personal information of your customers is compromised? Please use a scale of 1 to 7, where 1 is not at all concerned, and 7 is extremely concerned. T2015

19. Does your company have any protocols or procedures in place that would be followed in the event of a breach where the personal information of customers is compromised? T2015

Yes
No

Section 6: Corporate Innovation

20. Does your company have any policies or procedures in place to assess privacy risks related to your business? This includes assessing privacy risks associated with the development or use of new products, services, or technologies. T2015

Yes
No

Section 7: Communications

21A. Has your company ever looked for information, or contacted anyone for advice, about its responsibilities under Canada's privacy laws?

Yes
No

21. IF YES AT Q21A: What organizations or resources [IF YES AT Q21A: did / IF NO AT Q21A: would] your company use to help clarify its responsibilities under Canada's privacy laws? [DO NOT READ LIST. ACCEPT MULTIPLE RESPONSES]

Internet [PROBE FOR SPECIFICS]
    Internet (Specified: RECORD IF NOT GOOGLE OR SOCIAL MEDIA CODES)
    Internet (Not specified)
Google
Social media [SPECIFIY: Which social media do you use for business?]
    LinkedIn
    YouTube
    Facebook
    Twitter
Government [PROBE WHETHER FEDERAL OR PROVINCIAL]
Privacy Commissioner [PROBE WHETHER FEDERAL OR PROVINCIAL]
Lawyer
Accountant
Peer/colleague/associate
Company/head office expert/internal resource for company
Industry experts, consulting firms, or education sources
Industry association
None/Do not use
Other. Specify:

Section 8: Office of the Privacy Commissioner of Canada

22. Are you aware that the Office of the Privacy Commissioner of Canada has information and tools available to companies to help them comply with their privacy obligations? T2015

Yes
No

INTERVIEWER NOTE: If asked about the OPC/how to reach the OPC, please share the website: priv.gc.ca.

Section 9: Corporate Profile

These last questions are for statistical purposes only, and all answers are confidential.

23. In what industry or sector do you operate? If your company is active in more than one sector, please identify the main sector. [DO NOT READ LIST. ACCEPT ONE RESPONSE]

Accommodation and Food Services
Administrative and Support, Waste Management and Remediation Services
Agriculture, Forestry, Fishing and Hunting
Arts, Entertainment and Recreation
Construction
Educational Services

Finance and Insurance
Health Care and Social Assistance
Information and Cultural Industries
Management of Companies and Enterprises
Manufacturing
Mining and Oil and Gas Extraction
Other Services (except Public Administration)
Professional, Scientific and Technical Services
Public Administration
Real Estate and Rental and Leasing
Retail Trade
Transportation and Warehousing
Utilities
Wholesale Trade
Other. Please specify:

24. What is your own position within the organization? [DO NOT READ LIST. ACCEPT ONE RESPONSE]

Owner, President or CEO
General Manager/Other Manager
IT Manager
Administration
Vice President
Privacy analyst/officer/coordinator
Legal counsel/lawyer
HR/Operations
Other: Specify

25. In which of the following categories would your company's 2016 revenues fall? [READ LIST. ACCEPT ONE RESPONSE]

Less than $100,000
$100,000 to just under $250,000
$250,000 to just under $500,000
$500,000 to just under $1,000,000
$1,000,000 to just under $5,000,000
$5,000,000 to just under $10,000,000
$10,000,000 to just under $20,000,000
More than $20 million

This concludes the survey.
Thank you for your time and feedback, it is much appreciated.

Annex 2: Tabulated Data

A full set of tabulated data (under separate cover)