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

FINAL REPORT
Executive Summary

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

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.