

PWGSC Contract # 2R008-090284/001/CY
POR Registration #POR 105-09
Contract Award Date: 16/02/2010



Canadian Businesses and Privacy-Related Issues

FINAL REPORT

Submitted to:

Office of the Privacy Commissioner of Canada Communications
Place de Ville 112 Kent Street, Suite 300
Ottawa, Ontario
K1A 1H3

EKOS RESEARCH ASSOCIATES INC.

March 2010

EKOS RESEARCH ASSOCIATES

Ottawa Office

359 Kent Street, Suite 300

Ottawa, Ontario

K2P 0R6

Tel: (613) 235 7215

Fax: (613) 235 8498

E-mail: pobox@ekos.com

Toronto Office

480 University Avenue, Suite 1006

Toronto, Ontario

M5G 1V2

Tel: (416) 598 8002

Fax: (416) 598 2543

E-mail: toronto@ekos.com

www.ekos.com

TABLE OF CONTENTS

Executive Summary	iii
1. Background and Methodology	1
1.1 Background.....	1
1.2 Methodology	2
2. Privacy and Personal Information.....	3
2.1 Time Spent On Privacy-Related Issues	3
2.2 Collection of Personal Information	4
2.3 Amount of Information Collected	5
2.4 Amount of Information Stored.....	6
2.5 Implementation of Policies re. Collection, Usage and Disclosure	7
2.6 Implementation of Safeguards re. Protecting Info from Unauthorized Access.....	8
2.7 Implementation of Accessibility of Personal Information Provisions.....	9
2.8 Implementation of Ways for Customers to Contact Company.....	10
2.9 Procedures to Handle Privacy-Related Issues.....	11
3. Privacy Legislation.....	13
3.1 Awareness of Responsibilities of Privacy Laws.....	13
3.2 Training on Responsibilities Under Privacy Laws.....	14
3.3 Frequency of Reviewing Training.....	15
3.4 Proportion of Companies Which Collect Personal Information and Send to Another Company	16
3.5 Awareness of Measures to Protect Personal Information	17
3.6 Impact of PIPEDA.....	18
3.7 Seeking Clarification on Privacy Laws	19
3.8 Source of Clarification	20
3.9 Difficulties in Adapting to Privacy Laws	21
3.10 How Businesses Would Find Out More Information on Privacy Laws	22
3.11 Awareness of OPC Information and Tools	23
3.12 Use of OPC Information and Tools.....	24
3.13 Usefulness of Training.....	25
3.14 Type of Training	26
3.15 Delivery of Training.....	27

4.	Security Breaches	29
4.1	Concern About Security Breaches.....	29
4.2	Experience with Security Breaches.....	30
4.3	Actions Taken in Event of Security Breach.....	31
4.4	Guidelines in Event of Security Breach.....	32
4.5	Support for Mandatory Breach Reporting.....	33
4.6	Source of Threat of Security Breach.....	34
4.7	Reduction in Spending on Security Measures	35
4.8	Cloud Computing Tools.....	36
4.9	Privacy Consideration in Development of New Technology	37

EXECUTIVE SUMMARY

EKOS Research Associates was commissioned by the Office of the Privacy Commissioner of Canada (OPC) to undertake a survey examining the views of Canadian businesses on a number of issues relating to privacy and the implementation of PIPEDA. The survey tracked a number of questions first asked in 2007, and also included a number of new questions about PIPEDA and privacy-related issues.

The methodology for this study involved a telephone survey of 1,005 businesses in Canada. Given that the main focus of the study was on the adoption and impact of privacy laws, the survey was designed to contact senior decision makers with responsibility or knowledge of their company's privacy and security practices.

Results suggest that Canadian businesses are largely familiar with Canada's privacy laws, are finding them fairly easy to comply with, and have implemented many privacy policies to help protect the personal information of their customers. In addition, privacy legislation is seen as having had a positive impact on how Canadian businesses handle the personal information of their customers. The key findings from this study are outlined below, and described in more detail in the remainder of this report:

- Survey results reveal that the collection of personal information by Canadian businesses is a common occurrence: almost seven in ten of the companies surveyed (68 per cent) report that they collect information on their customers (and this is up five per cent since 2007).
- Results also reveal that the majority of businesses that collect personal information on customers have implemented provisions to protect customer information.
- Almost half of the businesses surveyed report high awareness of their responsibilities under Canada's privacy laws, and only 10 per cent rate their awareness in this area as low.
- The plurality of the businesses surveyed feel it has been fairly easy to comply with privacy laws (47 per cent, up five per cent since 2007), and only five per cent feel it has been difficult to comply with these laws (down three per cent since 2007).
- Survey results also suggest PIPEDA has had a positive impact on Canadian businesses' handling of customers' personal information. About two in three of the companies surveyed indicate they are more concerned about protecting their customers' personal information (68 per cent), and have increased their awareness of privacy obligations (63 per cent) as a result of PIPEDA. And more than half (57 per cent) said the introduction of PIPEDA has resulted in improved security associated with personal information held by the company on its customers.
- More than half of the businesses surveyed report awareness of OPC information and tools to help companies comply with their privacy obligations. About a third of the businesses aware of

OPC information and tools have accessed this information, and most of the companies that did access this information found the information to be useful.

- The plurality of the companies surveyed are not concerned about security breaches in which the personal information of customers is compromised (42 per cent), possibly because the vast majority (94 per cent) have not experienced a data breach.
- Only about one-third of the companies surveyed indicate they have formal guidelines to deal with a breach where the personal information of their customers is compromised; the majority (63 per cent) do not have any such guidelines in place.
- Finally, results reveal that the vast majority of the companies surveyed (89 per cent) indicate that the poor economic situation over the past year and a half did not result in reduced spending on measures to protect customer information.

Supplier Name: EKOS Research Associates

PWGSC Contract Number: # 2R008-090284/001/CY

Contract Award Date: 16/02/2010

To obtain more information on this study, please e-mail publications@privcom.gc.ca.

1. BACKGROUND AND METHODOLOGY

1.1 BACKGROUND

The Privacy Commissioner of Canada is an advocate for the privacy rights of Canadians, with the powers to investigate complaints and conduct audits under two federal laws; publish information about personal information-handling practices in the public and private sector; and conduct research into privacy issues.

The two federal laws are the Privacy Act which governs the public sector and the Personal Information Protection and Electronic Documents Act (PIPEDA) which governs the private sector. More specifically, PIPEDA “sets out ground rules for the management of personal information in the private sector ... (and) balances an individual's right to the privacy of personal information with the need of organizations to collect, use or disclose personal information for legitimate business purposes.”

Under PIPEDA, personal information is defined as “any factual information, recorded or not, about an identifiable individual”, employee or otherwise, including their age, name, income, ethnic origin, social status, credit records, loan records, and medical records. If an organization wishes to use an individual’s personal information for reasons other than the purpose for which it was collected, consent must first be obtained from the individual. As well, individuals have “the right to access personal information held by an organization and to challenge its accuracy.”

PIPEDA came into force in 2001, but at the time only applied to federally-regulated private sector companies. The Act was extended to cover personal health information for these organizations and activities in 2002. Two years later, PIPEDA came into full effect in January 2004. Today, the Act covers all organizations engaged in commercial activities, including those that for other purposes (for example, employment) are regulated by the provinces. PIPEDA includes provisions for a mandatory review by Parliament every five years.

Against this backdrop, there is a need to better understand the extent to which businesses are familiar with and are complying with their responsibilities under PIPEDA, as well as understanding any other related issues to the implementation of the Act. Within this context, there was a need to undertake a survey of Canadian businesses to help develop this understanding.

1.2 METHODOLOGY

The research findings for this study have been drawn from the results of a 16 minute telephone survey with 1,005 businesses in Canada, conducted from March 4 to March 25, 2010. Given that the main focus of the study was on the adoption and impact of privacy laws, the survey was designed to contact senior decision makers with responsibility or knowledge of their company's privacy and security practices.

The survey instrument was designed in close consultation with the Office of the Privacy Commissioner (OPC). Once the questionnaire items were approved, the questionnaire was programmed into EKOS' computer assisted telephone interviewing (CATI) software. In addition to programming the actual text of each question, instructions to the survey interviewer (such as instruction to read or not read available responses), question/response randomization (batteries of questions and some responses to questions are randomized to minimize an order bias) and skip logic were integrated at this stage. In order to gauge the flow and clarity of the survey instrument, the questionnaire was pre-tested through a series of telephone interviews with actual respondents in English and French. The objective of the pre-test was to ascertain the clarity of the questions, the flow of the sequencing, the overall length of the interviews and any factors that may affect the response rate. No significant changes to the questionnaire were required as a result of the pretest. The final version of this survey is appended to this report in Appendix A.

Since medium and large sized businesses together account for less than 15 per cent of all businesses, the sample was stratified by company size (based on number of employees) in order to ensure that there were enough respondents from both of these two size segments. For purposes of the study, the following definitions of size were adopted: small (1-19 employees), medium (20-99 employees), and large (100 or more employees). The results are based on the following samples:

- 555 surveys with small businesses;
- 302 surveys with medium businesses; and
- 148 surveys with large businesses.

The findings were then weighted by size, region and industry code to align the data to a 'truer' reflection of Canadian businesses. The weighted findings tend to reflect more closely the responses of small-sized businesses as these businesses account for more than four in five businesses in Canada.

With a sample size of 1,005, results may be considered statistically accurate to within +/- 3.1 percentage points, 19 times out of 20. The margin of error rises when results are examined for a particular sub-sample.

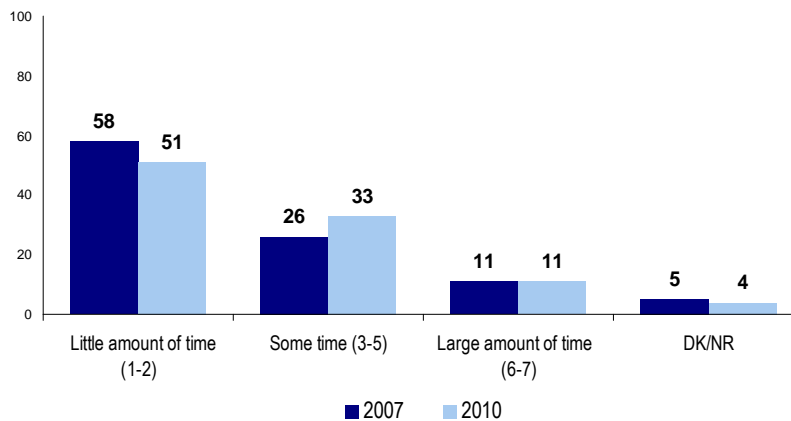
2. PRIVACY AND PERSONAL INFORMATION

2.1 TIME SPENT ON PRIVACY-RELATED ISSUES

Businesses were first asked how much time their company spends in a typical month dealing with privacy related issues. Results suggest that most Canadian businesses spend little time dealing with privacy issues: only 11 per cent say they spend a great deal of time on these issues, and the majority (51 per cent) say they spend little time dealing with privacy issues in a typical month. However, tracking reveals a seven per cent decrease since 2007 in the proportion of businesses who spend little time on privacy issues, and a corresponding seven point increase (to 33 per cent) in the proportion of businesses who spend some time dealing with privacy issues.

Time Spent on Privacy-Related Issues

“How much time does your company spend on dealing with PRIVACY ISSUES in a TYPICAL month?”



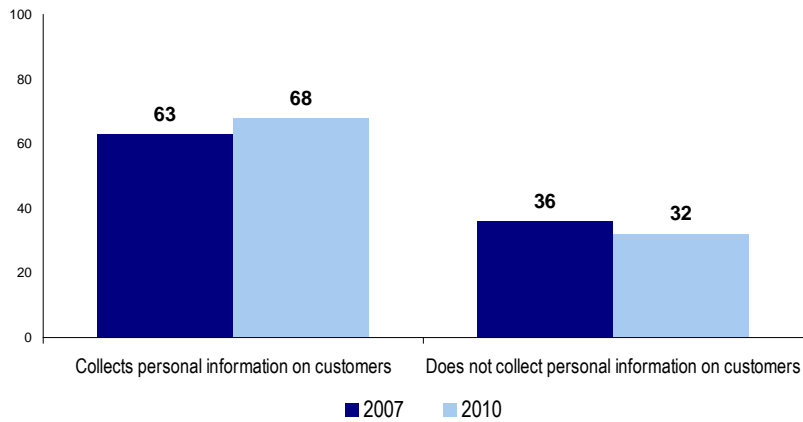
2.2 COLLECTION OF PERSONAL INFORMATION

The survey went on to ask Canadian businesses whether or not their company collects personal information on their customers. Survey results reveal that most of the companies surveyed collect personal information on their customers (68 per cent), and this is up five per cent since 2007.

- The collection of personal information from customers does not vary significantly across company size.

Collection of Personal Information

“Which of the following best describes your company’s activities in relation to your customer’s personal information? Would you say your company collects...?”



EKOS Research Associates Inc.

n=1005

		Collects personal information on customers	Does not collect personal information on customers
Company Size	Small	69	31
	Medium	67	32
	Large	74	26

Q: And would you say your company collects ...
(Base: All Businesses; Mar. 2010, n=)

2.3 AMOUNT OF PERSONAL INFORMATION COLLECTED

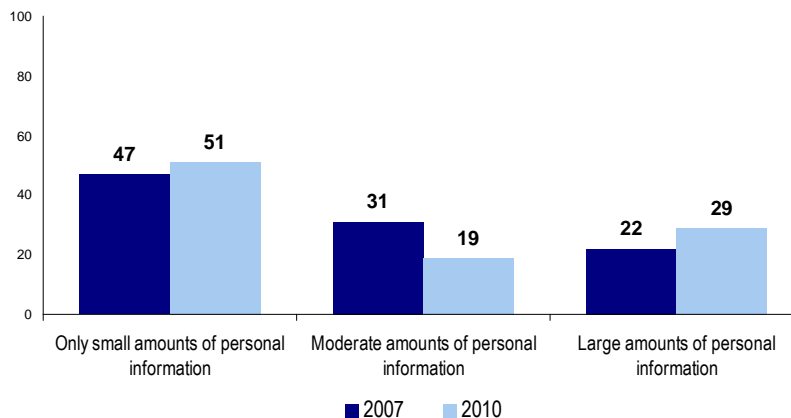
Results further reveal that half of the businesses that collect personal information on their customers say they collect only small amounts of personal information (51 per cent). About one in five (19 per cent) collect moderate amounts of information, and three in ten (29 per cent) say they collect large amounts of personal information from their customers.

Interestingly, tracking reveals a polarization in terms of the personal information collected by Canadian businesses. The proportion of businesses that report they collect both small and large amounts of personal information is up since 2007, while those companies that indicate they collect “moderate” amounts of information is down 12 per cent since 2007.

- Smaller firms are more likely to indicate they collect only small amounts of personal information.

Amount of Personal Information Collected

“And would you say your company collects...?”



EKOS Research
Associates Inc.

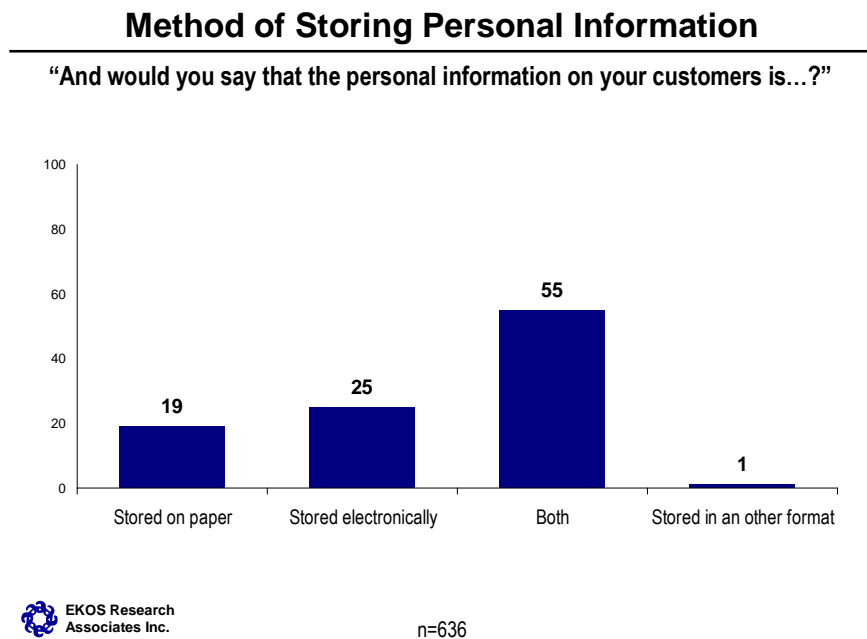
n=636

		Small amounts of information	Moderate amounts of information	Large amounts of information
Company Size	Small	52	18	30
	Medium	45	25	28
	Large	34	37	29

Q: And would you say your company collects ...
(Base: Businesses that collect personal information; Mar. 20107, n=)

2.4 METHOD OF STORING PERSONAL INFORMATION

Businesses which collect personal information on their clients were also asked if the personal information they collect on their customers was stored on paper, stored electronically or both. The majority (55 per cent) say they collect this information both on paper and electronically. About one in five (19 per cent) say they store this information on paper only, and one in four (25 per cent) maintain this information only in an electronic format.



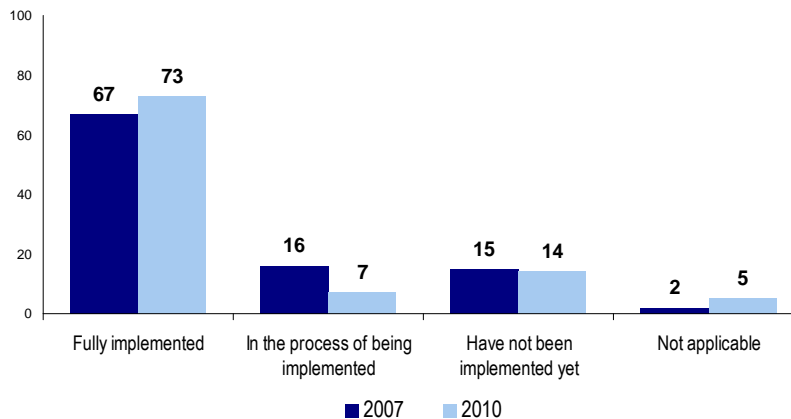
2.5 IMPLEMENTATION OF POLICIES RE. COLLECTION, USAGE AND DISCLOSURE

Businesses which indicated they collect personal information from their clients were asked a series of questions examining at what stage their company was in terms of putting in place clear privacy policies to deal with this information. Results suggest that the majority of these companies (73 per cent) have fully implemented privacy policies to oversee how the company and its employees collect, use, and disclose personal information, and this is up six per cent since 2007. Only 14 per cent indicate that these policies have yet to be implemented.

- Smaller businesses are more likely than their larger counterparts to indicate they have not yet implemented these policies.

Implementation of Policies re. Collection, Usage and Disclosure

“What stage is your company at putting in place clear privacy policies to oversee how the company and its employees collect, use and disclose personal information...?”



EKOS Research Associates Inc.

n=636

		Fully implemented	In the process of being implemented	Have not been implemented yet	Not applicable
Company Size	Small	73	6	14	5
	Medium	77	11	10	2
	Large	87	8	4	0

Q: What stage is your company at putting in place clear privacy policies to oversee how the company and its employees collect, use and disclose personal information?

(Base: Businesses that collect personal information; Mar. 2010, n=)

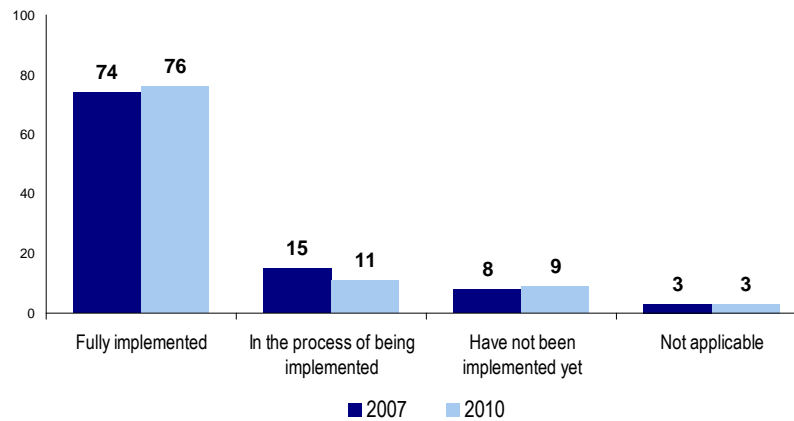
2.6 IMPLEMENTATION OF SAFEGUARDS RE. PROTECTING INFO FROM UNAUTHORIZED ACCESS

In terms of implementing safeguards to protect personal information from unauthorized use, more than three in four businesses which collect personal information (76 per cent) say they have a fully implemented policy in this area (up two per cent since 2007). Fewer than one in ten (nine per cent) say these safeguards have not yet been put in place.

- Smaller businesses are more likely than their larger counterparts to indicate they have not yet put safeguards to protect personal information in place.

Implementation of Safeguards re. Protecting Info from Unauthorized Access

“What stage is your company at putting in place safeguards to protect personal information from unauthorized access?”



EKOS Research Associates Inc.

n=636

		Fully implemented	In the process of being implemented	Have not been implemented yet	Not applicable
Company Size	Small	76	10	9	3
	Medium	83	9	5	2
	Large	92	6	0	1

Q: What stage is your company at putting in place safeguards to protect personal information from unauthorized access?
(Base: Businesses that collect personal information; Mar. 2010, n=)

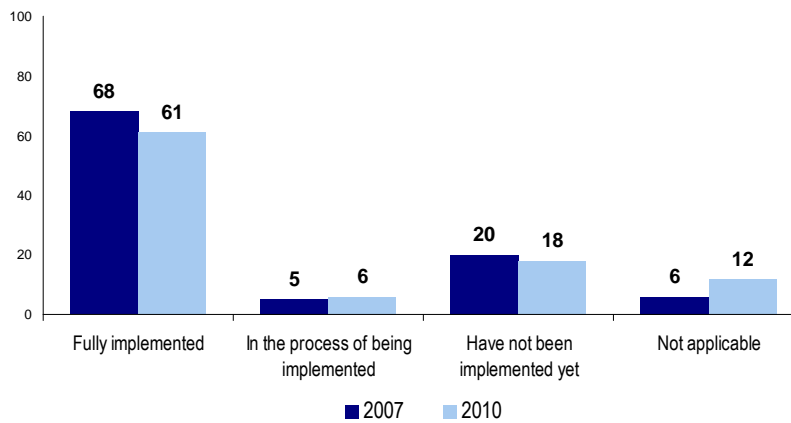
2.7 IMPLEMENTATION OF ACCESSIBILITY OF PERSONAL INFORMATION PROVISIONS

A majority of businesses which collect personal information also indicate that they have a fully implemented policy in place to allow customers to request and access any personal information that the company holds on its customers (61 per cent), however, this is down seven per cent since 2007.

- Small and medium-sized businesses are more likely than large companies to indicate they have not yet implemented procedures to allow customers to access their personal information.

Implementation of Accessibility of Personal Information Provisions

“What stage is your company at putting in place ways for customers to be able to request and access any personal information that your company holds on them?”



EKOS Research Associates Inc.

n=636

		Fully implemented	In the process of being implemented	Have not been implemented yet	Not applicable
Company Size	Small	61	6	17	14
	Medium	63	3	25	5
	Large	77	5	9	4

Q: What stage is your company at putting in place ways for customers to be able to request and access any personal information that your company holds on them?

(Base: Businesses that collect personal information; Mar. 2010, n=)

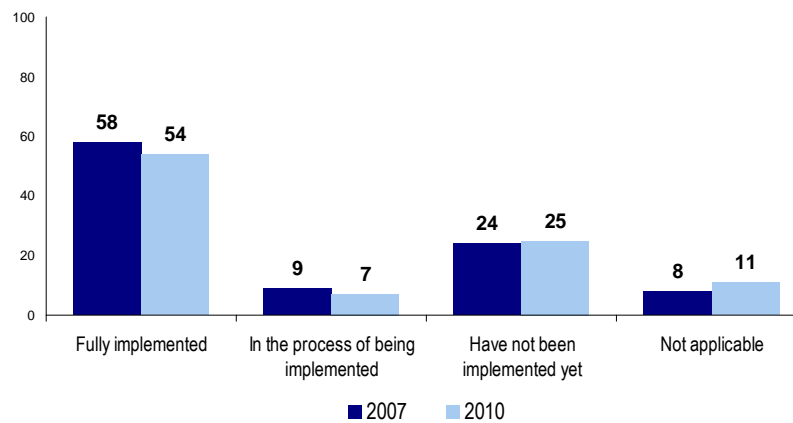
2.8 IMPLEMENTATION OF WAYS FOR CUSTOMERS TO CONTACT COMPANY

A slight majority of these businesses (54 per cent) also report that they have fully implemented procedures that enable customers to make complaints should they feel that their personal information has been handled inappropriately, however, this is down four per cent since 2007. One in four (25 per cent) indicate these procedures have yet to be put in place.

- Smaller businesses are more likely than their larger counterparts to indicate they have not yet put these procedures in place.

Implementation of Ways for Customers to Contact Company

“What stage is your company at putting in place procedures that enables customers to make complaints should they feel that their personal information has been handled inappropriately?”



EKOS Research Associates Inc.

n=636

		Fully implemented	In the process of being implemented	Have not been implemented yet	Not applicable
Company Size	Small	54	6	26	12
	Medium	71	7	16	3
	Large	80	5	8	4

Q: What stage is your company at putting in place procedures that enables customers to make complaints should they feel that their personal information has been handled inappropriately?

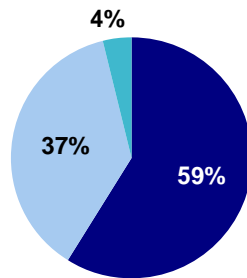
(Base: Businesses that collect personal information; Mar. 2010, n=)

2.9 PROCEDURES TO HANDLE PRIVACY-RELATED ISSUES

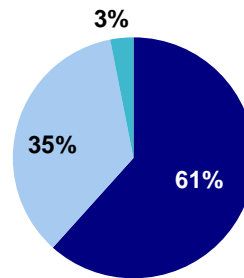
Survey results further reveal that most of the companies surveyed say they have procedures to handle privacy-related issues raised by both internal staff (59 per cent), and by customers and other external parties (61 per cent).

Procedures to Handle Privacy-Related Issues

“Does your company have procedures in place to handle privacy-related issues raised by internal staff?”



“And does your company have procedures in place to handle privacy-related issues raised by customers and other external parties?”



■ Yes
■ No
■ DK/NR

3. PRIVACY LEGISLATION

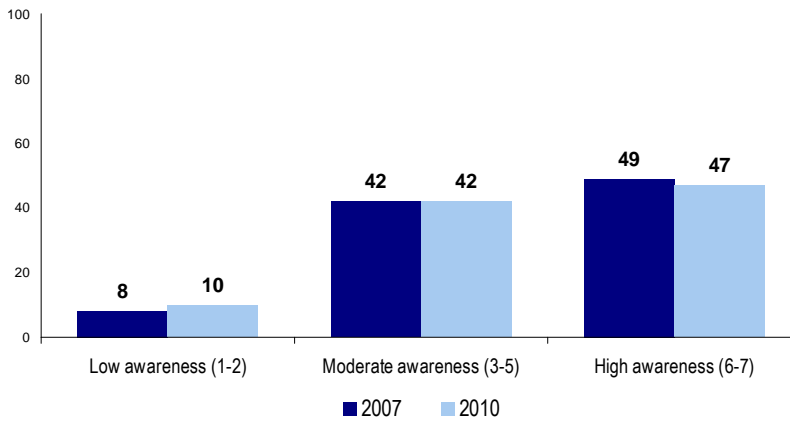
3.1 AWARENESS OF RESPONSIBILITIES OF PRIVACY LAWS

All respondents were provided with a brief description of PIPEDA and asked to rate their awareness of their responsibilities under Canada’s privacy laws. Results reveal that Canadian businesses are largely familiar with Canada’s privacy laws: almost half of the companies surveyed feel they have a high degree of awareness of their responsibilities under Canada’s privacy laws (47 per cent), and only 10 per cent rate their awareness in this area as low. These results have remained largely stable since 2007.

- Awareness of privacy laws is higher among larger Canadian businesses.

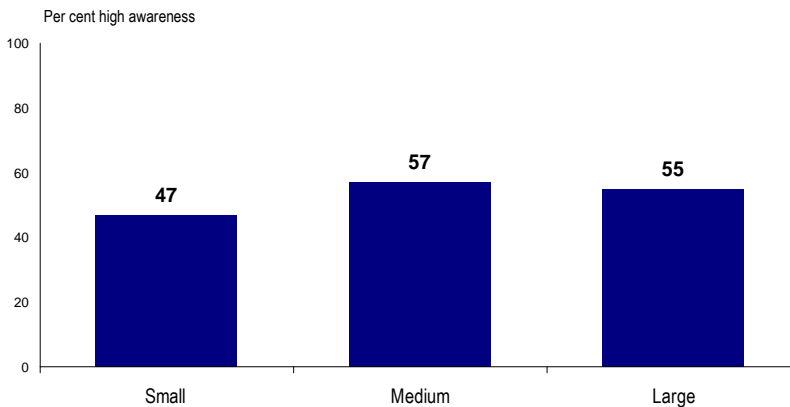
Awareness of Responsibilities of Privacy Laws

“How would you rate your company’s awareness of its responsibilities under Canada’s privacy laws?”



EKOS Research Associates Inc.

n=1005



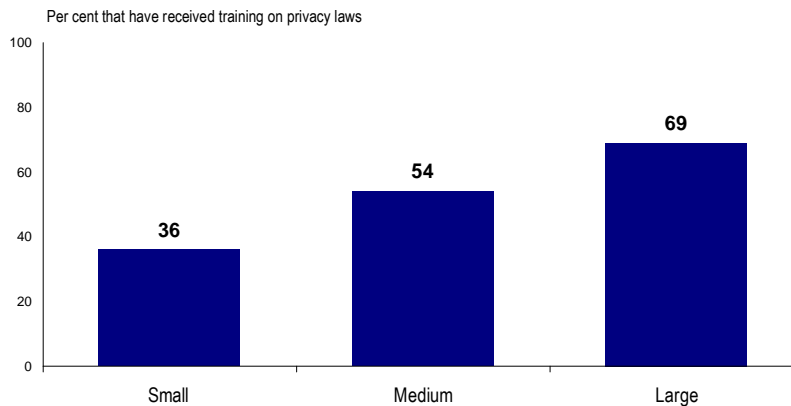
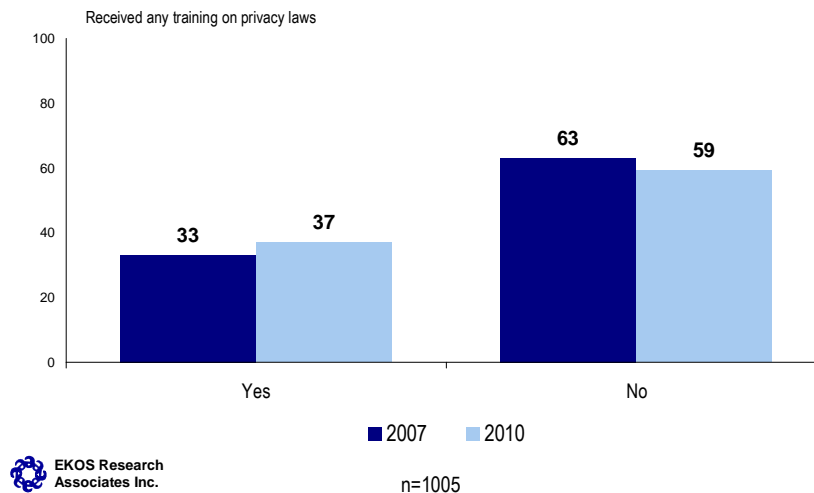
3.2 TRAINING ON RESPONSIBILITIES UNDER PRIVACY LAWS

Businesses were also asked if any of their staff had received training on appropriate information practices and responsibilities under Canada's privacy laws. Fewer than four in ten (37 per cent) reported they had provided this type of training to their staff (although this is up four per cent since 2007), while about six in ten (59 per cent) said they had not (down a corresponding four points since 2007).

- Large businesses are more likely to have provided training to staff on appropriate information and practices under Canada's privacy laws.

Training on Responsibilities Under Privacy Laws

"Have any of your staff received training on appropriate information practices and responsibilities under Canada's privacy laws?"

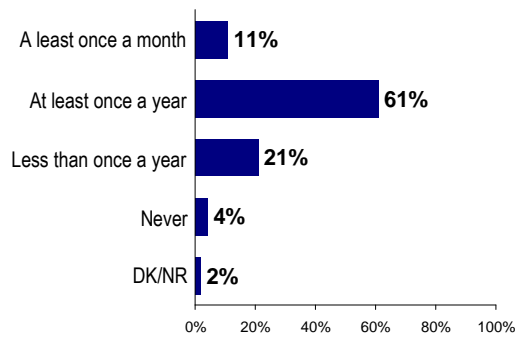


3.3 FREQUENCY OF REVIEWING TRAINING

Those companies which indicated that their staff did receive training on appropriate information and practices under Canada’s privacy laws were asked how often they reviewed their training modules and procedures in this area. Results suggest that this is done on a fairly infrequent basis: only 11 per cent indicated they review this information at least once a month, and almost twice as many (21 per cent) say it is reviewed less than once a year. Most say they review this information about once a year (61 per cent).

Frequency of Reviewing Training

[IF YES] “How often do you review your training modules/manuals/ procedures on appropriate information and practices under Canada’s privacy laws?”

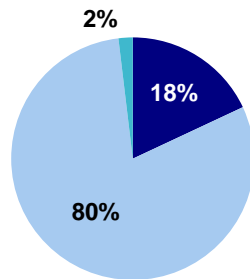


3.4 PROPORTION OF COMPANIES WHICH COLLECT PERSONAL INFORMATION AND SEND TO ANOTHER COMPANY

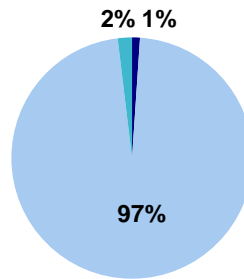
Canadian businesses were also asked if their company collects personal information from clients and sends to another company within Canada or outside Canada for processing. Relatively few (18 per cent) say that they send personal information to another company in Canada for processing, and virtually none (one per cent) send this information outside of Canada for processing.

Proportion of Companies Which Collect Personal Information and Send to Another Company

“Does your company collect personal information from clients and send to another company within Canada for processing?”



“Does your company collect personal information from clients and send to another company outside of Canada for processing?”



■ Yes
■ No
■ DK/NR

EKOS Research Associates Inc.

n=1005

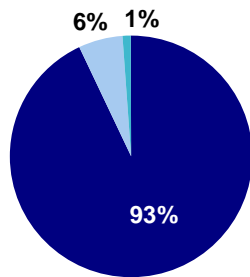
3.5 AWARENESS OF MEASURES TO PROTECT PERSONAL INFORMATION

Those companies that indicated they send personal information to another company for processing were asked if they were aware of any measures they must take to ensure that this personal information is protected. The vast majority of these companies (93 per cent) reported that they were aware of these measures.

However, among those companies that indicated they were aware of these measures, only half (50 per cent) have put in place a contract, or other means, to ensure there is a comparable level of protection while the information is being processed by this other company. The remainder (49 per cent) said they had not established such a contractual arrangement.

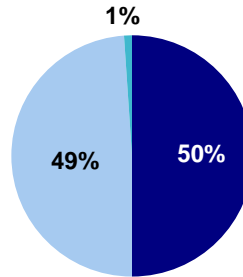
Awareness of Measures to Protect Personal Information

[IF YES] “Are you aware of any measures you must take to ensure that this personal information is protected?”



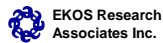
n=126

[IF YES] “Have you put in place a contract, or other means, to ensure there is a comparable level of protection while the information is being processed by this other company ?”



n=111

■ Yes
■ No
■ DK/NR

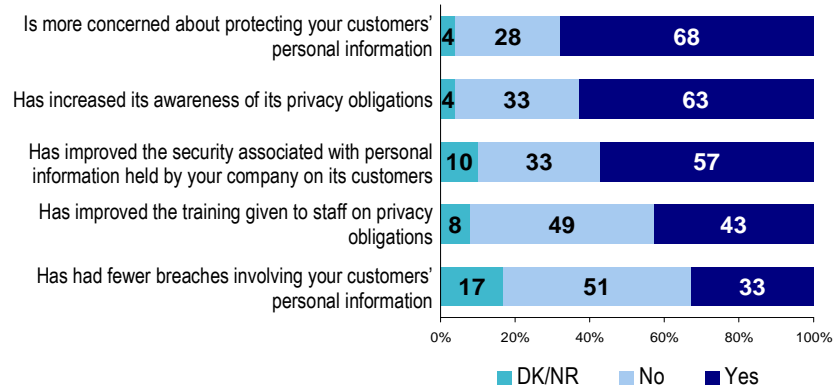


3.6 IMPACT OF PIPEDA

All respondents were asked about the impact of PIPEDA on their company. Results suggest PIPEDA has had a positive impact on Canadian businesses' handling of customers' personal information (although the extent of the impact varies across the issues examined). About two in three of the companies surveyed indicated they were more concerned about protecting their customers' personal information (68 per cent), and had increased their awareness of privacy obligations (63 per cent) as a result of PIPEDA. Just over half (57 per cent) said the introduction of PIPEDA has resulted in improved security associated with personal information held by the company on its customers. More than four in ten (43 per cent) felt PIPEDA had helped improve the training given to staff on privacy obligations, and one in three (33 per cent) felt that the introduction of PIPEDA had resulted in fewer breaches involving their customers' personal information.

Impact of PIPEDA

“As a result of the introduction of PIPEDA, would you say your company...?”



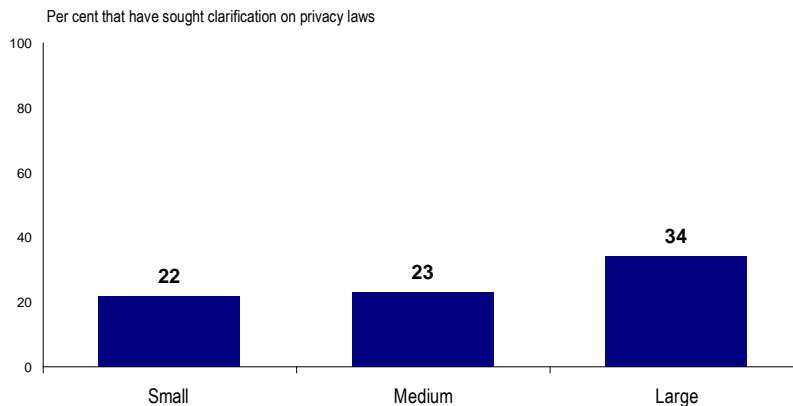
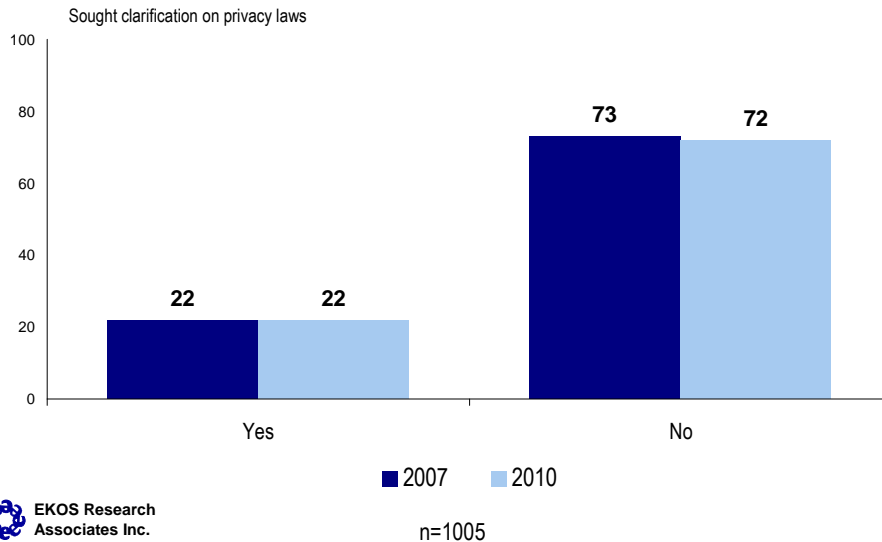
3.7 SEEKING CLARIFICATION ON PRIVACY LAWS

Businesses were also asked if their company had ever sought clarification of its responsibilities under Canada’s privacy laws. The majority of businesses report that they have not looked for this type of information (72 per cent), while about one in five (22 per cent) indicate they have. Results are largely stable since 2007.

- Large businesses are particularly likely to indicate that they have sought clarification of their responsibilities under Canada’s privacy laws.

Seeking Clarification on Privacy Laws

“Has your company ever sought clarification of its responsibilities under Canada’s privacy laws?”

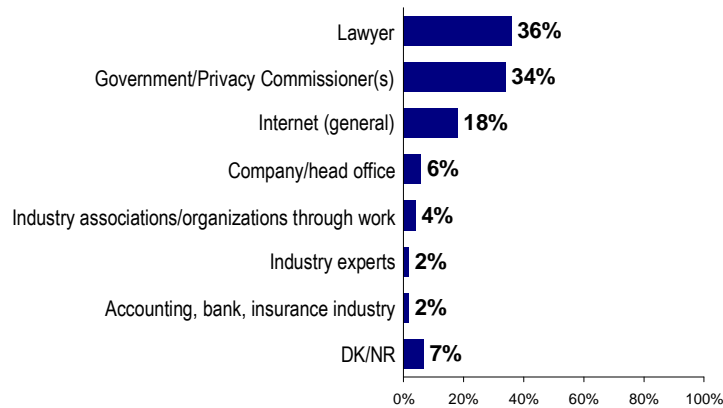


3.8 SOURCE OF CLARIFICATION

Among those companies that did seek a clarification of their privacy obligations, most indicated that they looked for this information from a lawyer (36 per cent) or from the Privacy Commissioner/government in general (34 per cent). About one in five (18 per cent) also looked for this information through a general Internet search.

Source of Clarification

[IF YES] "Where did you go to seek this clarification?" [Open]



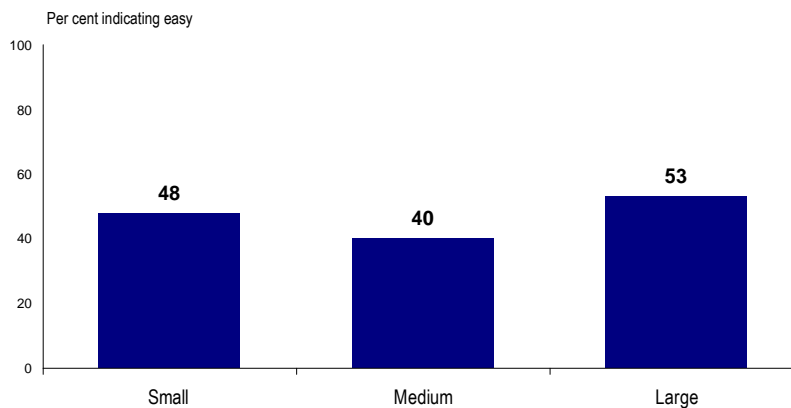
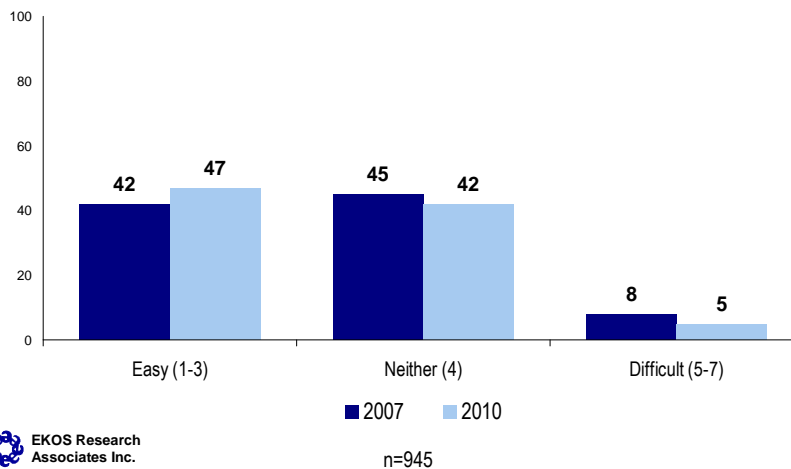
3.9 DIFFICULTIES IN ADAPTING TO PRIVACY LAWS

Canadian businesses with at least some awareness of Canada's privacy laws (2 to 7 on the 7-point awareness scale) were asked how difficult it had been for their company to bring its information practices into compliance with these privacy laws. The plurality feel it has been fairly easy to comply with these laws (47 per cent), and this is up five per cent since 2007. Only five per cent feel it has been difficult to comply with privacy laws (down three per cent since 2007).

- Perceived difficulties in adapting to privacy laws does not vary significantly across company size.

Difficulties in Adapting to Privacy Laws

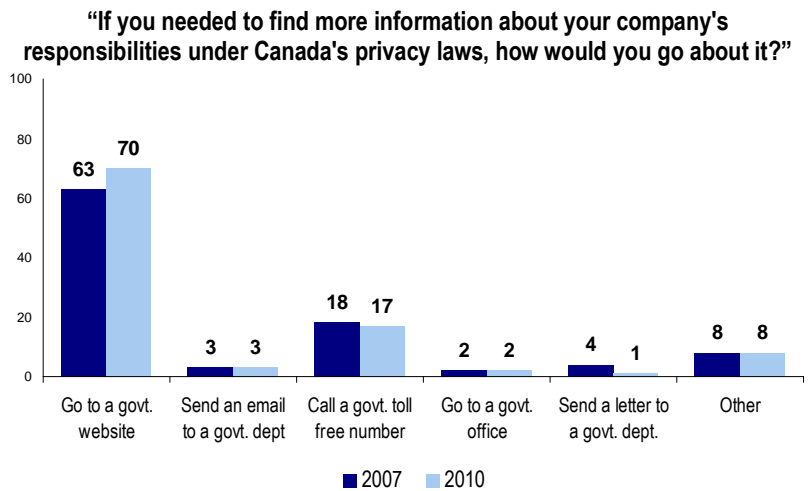
“How difficult has it been for your company to bring its information practices into compliance with Canada's privacy laws?”



3.10 HOW BUSINESSES WOULD FIND OUT MORE INFORMATION ON PRIVACY LAWS

All companies were asked how they would go about finding more information about their company’s responsibilities under Canada’s privacy laws. Government websites were mentioned most often (70 per cent – up seven per cent since 2007), followed distantly by a government toll free number (17 per cent – down one per cent since 2007).

How Businesses Would Find Out More information on Privacy Laws



EKOS Research Associates Inc.

n=986

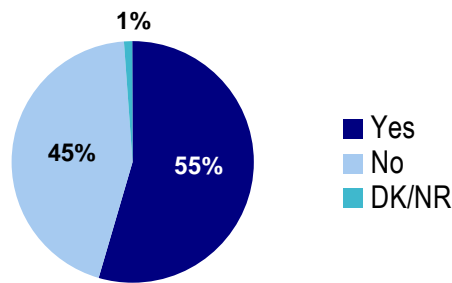
3.11 AWARENESS OF OPC INFORMATION AND TOOLS

Respondents were further asked if they were aware that the Office of the Privacy Commissioner has information and tools available to companies to help them comply with their privacy obligations. Just over half of the businesses surveyed (55 per cent) indicated they were aware of this information, and about four in ten (45 per cent) said they were not.

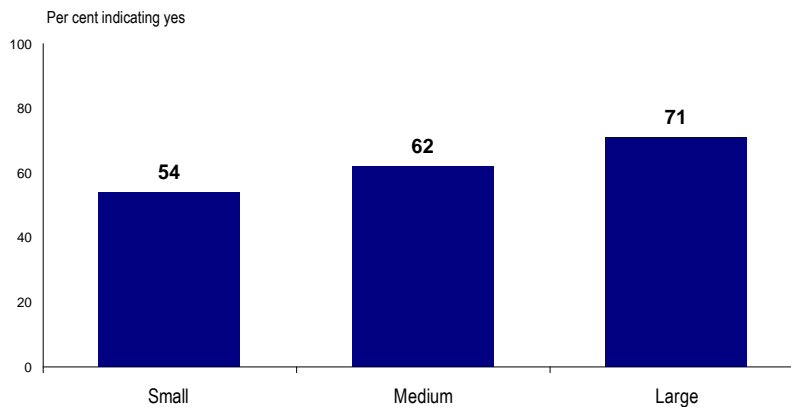
- Larger businesses are more likely to express awareness of OPC information and tools.

Awareness of OPC Information and Tools

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



n=1005



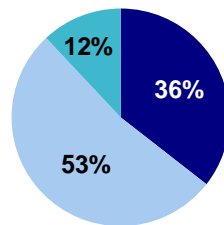
3.12 USE OF OPC INFORMATION AND TOOLS

Those businesses that indicated they were aware of OPC information and tools to help companies comply with privacy obligations were asked if they had ever accessed this information. Just over a third of these companies (36 per cent) indicated they had accessed this OPC information, and half (53 per cent) said they had not.

Those who had accessed this information were asked to rate the usefulness of this information in helping their company meet its privacy obligations. Over half of these companies (55 per cent) found the information to be useful, and fewer than one in ten (eight per cent) found this information to be of little use.

Use of OPC Information and Tools

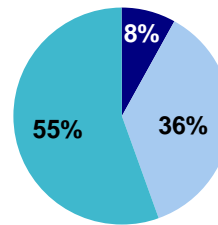
[IF YES] "Has your company ever accessed this information?"



■ Yes
■ No
■ DK/NR

n=556

[IF YES] "How useful was this information in helping your company meet its privacy obligations?"



■ Not useful (1-3)
■ Somewhat (4)
■ Useful (5-7)

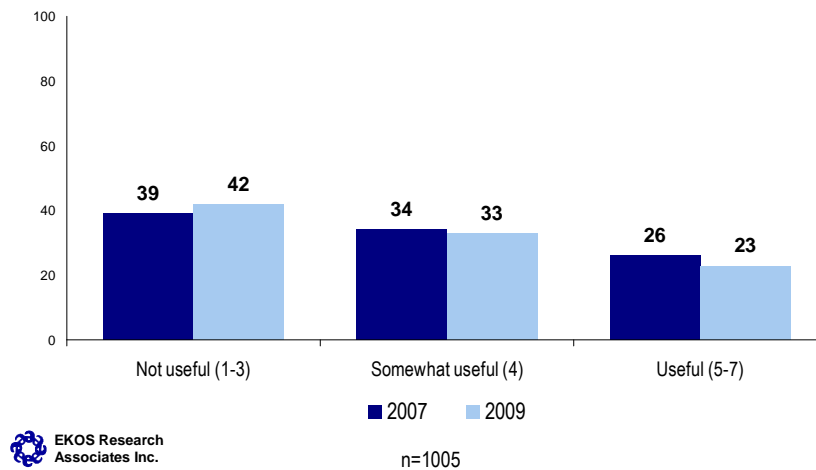
n=188

3.13 USEFULNESS OF TRAINING

All companies were asked how useful it would be to get training on what companies need to do to comply with Canada's privacy laws. Despite fairly high levels of satisfaction with the information provided by the OPC among companies that accessed this information (as discussed in the previous question), most Canadian companies do not see the need for training in this area. Only about one in four (23 per cent) feel that training on what companies need to do to comply with Canada's privacy laws would be useful, and more than four in ten (42 per cent) feel it would be of little use.

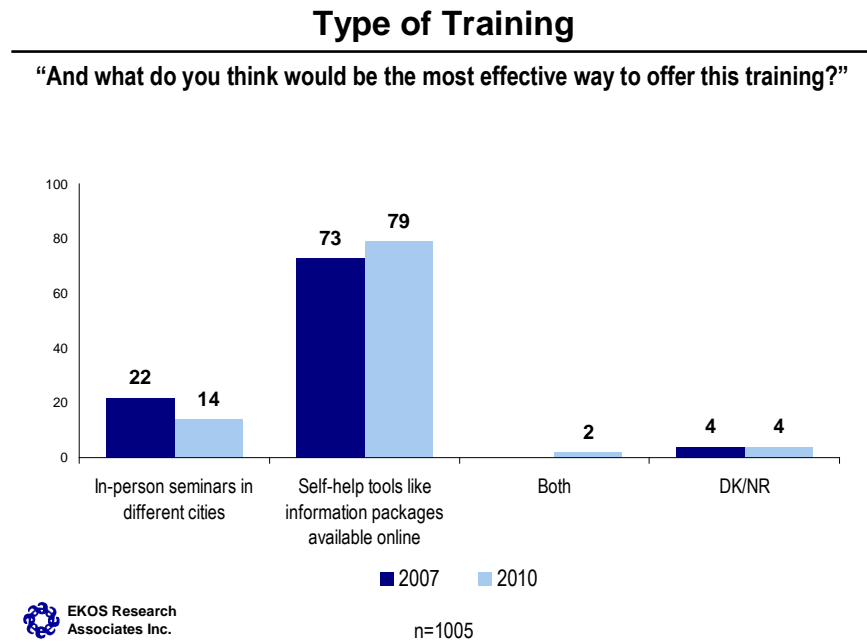
Usefulness of Training

"How useful would it be for your company to be able to get training on what companies need to do to comply with Canada's privacy laws?"



3.14 TYPE OF TRAINING

Businesses were also asked what would be the most effective way to offer training to help them comply with Canada's privacy laws. Online self-help tools are clearly preferred over in-person seminars (79 per cent vs. 14 per cent, respectively), and preference for self-help tools has increased six per cent since 2007.

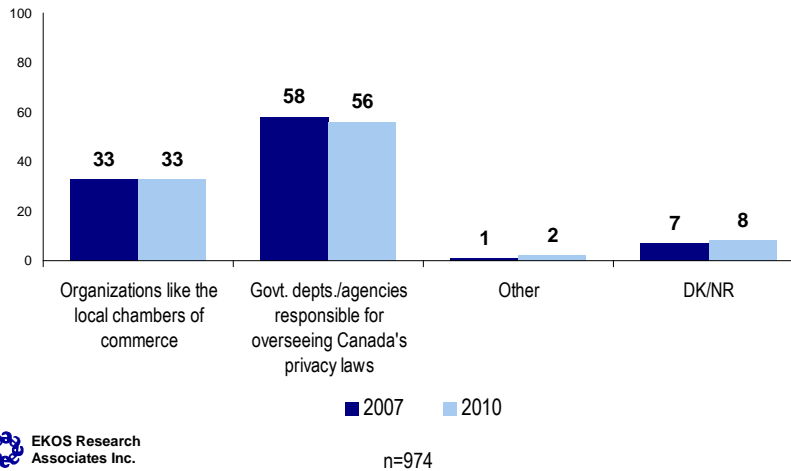


3.15 DELIVERY OF TRAINING

In terms of who should provide training to help businesses comply with privacy laws, government departments and agencies responsible for overseeing Canada's privacy laws are preferred over organizations like the Chamber of Commerce (56 per cent vs. 33 per cent, respectively).

Delivery of Training

“And who do you think would be the most effective at delivering this type of training?”



4. SECURITY BREACHES

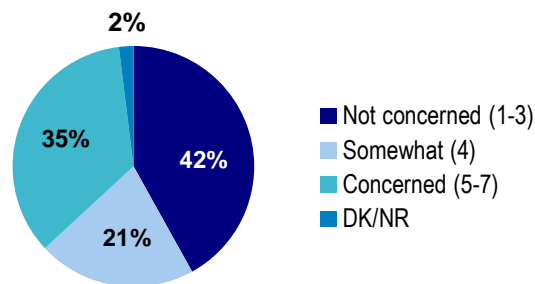
4.1 CONCERN ABOUT SECURITY BREACHES

The survey also asked a number of questions about security breaches where the personal information of customers is compromised. Results reveal that the plurality of the companies surveyed are not concerned about this type of security breach (42 per cent), although a sizeable minority (35 per cent) does express concern about this issue.

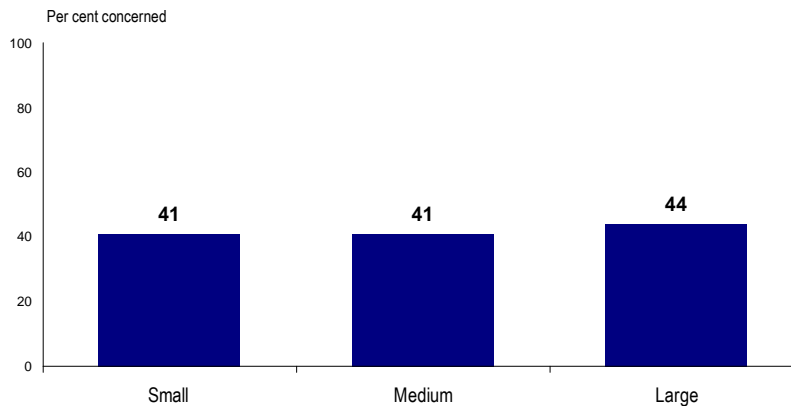
- Concern with information breaches does not vary significantly by company size.

Concern About Security Breaches

“How concerned are you about a breach where the personal information of customers is compromised?”



n=1005



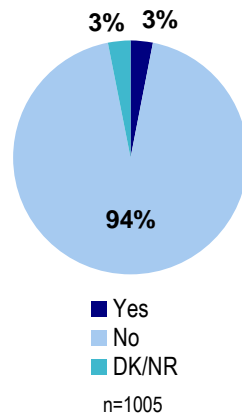
4.2 EXPERIENCE WITH SECURITY BREACHES

Businesses were also asked if their company had ever experienced a breach where the personal information of customers was compromised. The vast majority of the businesses surveyed (94 per cent) indicated they had not, and only three per cent reported that they had experienced this type of information breach.

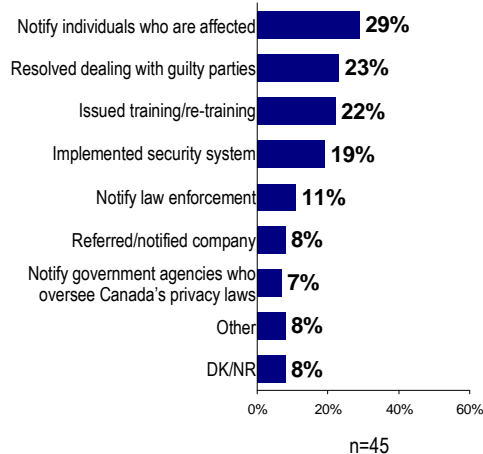
Those few who indicated they had experienced a data breach were asked, unprompted, what their company did to address this situation. Most said they notified the individuals who were affected, dealt with the guilty parties directly, or provided training to staff in addressing this situation.

Experience with Security Breaches

“Has your company ever experienced a breach where the personal information of your customers was compromised?” [IF YES] **“What did your company do to address this situation...”** [Open]



EKOS Research Associates Inc.

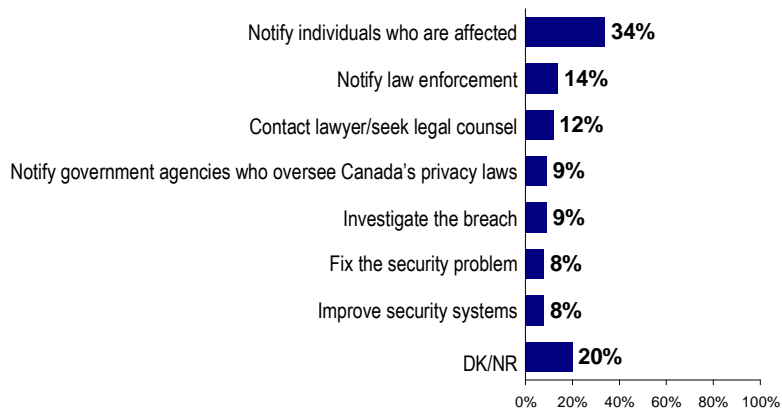


4.3 ACTIONS TAKEN IN EVENT OF SECURITY BREACH

Those companies which had not experienced a security breach were asked, unprompted, if they were to experience a breach involving the personal information of their customers, what actions would they take. Most indicate they would notify the individuals affected (34 per cent), notify law enforcement officials (14 per cent), or contact their lawyer/seek legal counsel (12 per cent).

Actions Taken in Event of Security Breach

[IF NO] "If your company were to experience a breach involving the personal information of customers, what would your company do?" [Open]



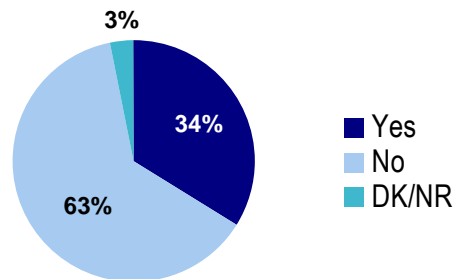
4.4 GUIDELINES IN EVENT OF SECURITY BREACH

All Canadian businesses were also asked if their company had any guidelines in place in the event of a security breach. Only about one-third of the companies surveyed (34 per cent) indicate they have formal guidelines to deal with a breach where the personal information of their customers is compromised. The majority (63 per cent) do not have any such guidelines in place.

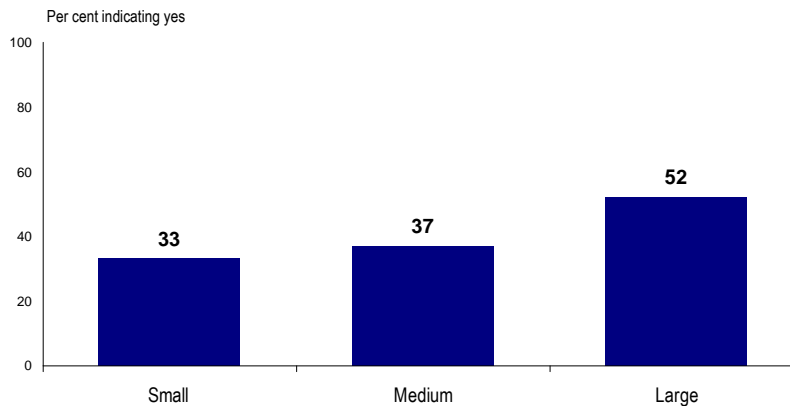
- Larger businesses are more likely to say they have guidelines in place in the event of a data breach.

Guidelines in Event of Security Breach

“Does your company have any guidelines in place in the event of a breach where the personal information of your customers is compromised?”



n=1005

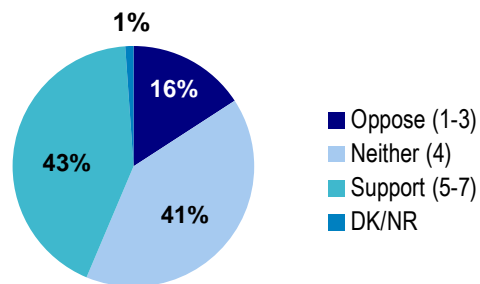


4.5 SUPPORT FOR MANDATORY BREACH REPORTING

Businesses were also asked if they supported or opposed the idea of mandatory breach reporting. Results reveal fairly strong support for this idea: the plurality of the businesses surveyed (43 per cent) support the notion of mandatory breach reporting, and only about one in six (16 per cent) oppose such a mandatory requirement (the remainder are neutral or did not provide a response).

Support for Mandatory Breach Reporting

“Do you support or oppose the idea of mandatory breach reporting for Canadian companies?”

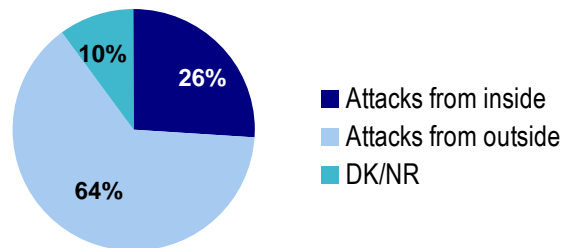


4.6 SOURCE OF THREAT OF SECURITY BREACH

In terms of the primary perceived threat of data breaches, most Canadian businesses feel that attacks from outside the company are a much greater threat than those from inside the company (64 per cent vs. 26 per cent, respectively). The remainder (10 per cent) are unsure.

Source of Threat of Security Breach

“Still thinking about data breaches, which of the following do you think pose a greater threat to your organization?”

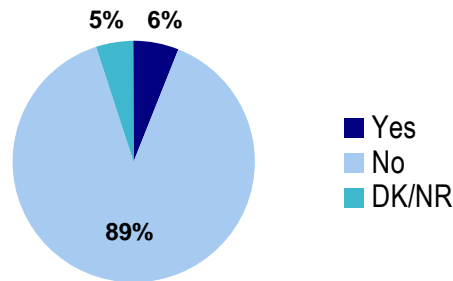


4.7 REDUCTION IN SPENDING ON SECURITY MEASURES

In light of the recent downturn in the economy, businesses were asked if their company had spent less on security measures to protect their customers personal information. The vast majority of the companies surveyed (89 per cent) report that the poor economic situation over the past year and a half did not result in reduced spending on measures to protect customer information. Only six per cent said the economic downturn affected their spending on security measures to protect customer information.

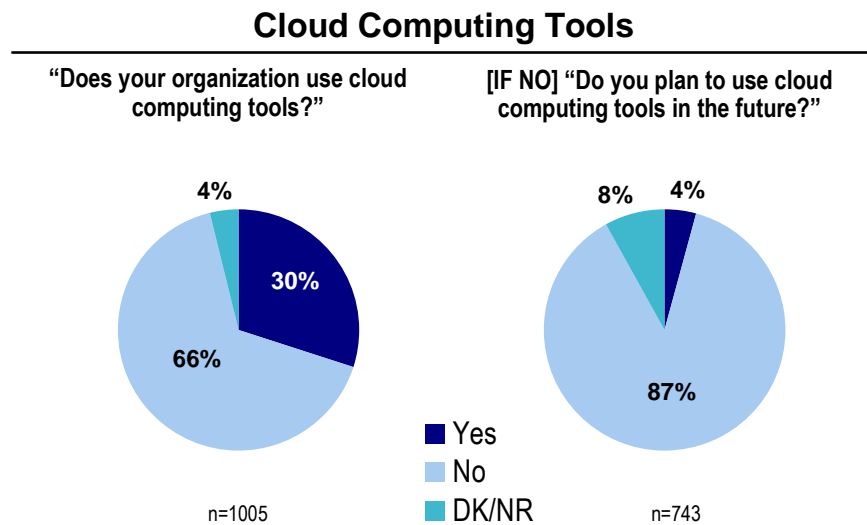
Reduction in Spending on Security Measures

“Has your company spent less on security measures to protect your customers’ personal information because of the economic downturn?”



4.8 CLOUD COMPUTING TOOLS

Canadian businesses were also asked if their company used cloud computing tools. Most of the companies surveyed indicated they did not (66 per cent), although three in ten (30 per cent) said their organization did use these tools. Those who indicated they did not currently use cloud computing tools were asked if they plan to do so in the future. The overwhelming majority of these businesses (87 per cent) said they had no plan to use cloud computing tools in the future.



4.9 PRIVACY CONSIDERATION IN DEVELOPMENT OF NEW TECHNOLOGY

Finally, Canadian businesses were asked if their company were to develop a new technology or product that could potentially have privacy implications, would they take privacy regulations into consideration before the launch of the product/technology. The majority of the businesses surveyed (84 per cent) say that they would take privacy regulations into consideration, and only one in ten indicated they would not take privacy-related issues into account before the launch of a new product or technology.

Privacy Consideration in Development of New Technology

“If your company were to develop a new technology or product that could potentially have privacy implications, would you take Canadian privacy regulations into consideration before the launch of the product/technology?”

