



The Human Factor in Laptop Encryption: Canada Study

Sponsored by
Absolute Software

Independently conducted by Ponemon Institute^{LLC}

Publication Date: December 2008

The Human Factor in Laptop Encryption: Canada Study

Executive Summary by Dr. Larry Ponemon, December 2008

Encryption is one of the most important security tools in the defense of information assets. Ponemon Institute has conducted numerous studies on organizations' use of encryption to prevent the loss of sensitive and confidential information. These studies have shown that encryption can be an effective deterrent. However, our studies also show that in order to be effective, encryption requires organizations and users to take appropriate steps to make sure sensitive and confidential information is protected as much as possible.

Ponemon Institute conducted this study sponsored by Absolute Software on *The Human Factor in the Use of Encryption* to understand employees' perceptions about ensuring that information assets entrusted to their care are effectively managed in encryption environments, especially the use of whole disk encryption on laptop computers. The study was also conducted in the United States and the United Kingdom. The results are published in separate reports.

What we learned is that a high percentage of employees we surveyed in non-IT business functions (referred to as business managers in this report) are not taking such precautionary steps as using complex passwords, not sharing passwords, using a privacy shield, keeping their laptop physically safe when traveling or locking their laptop to protect sensitive and confidential data. Further, many respondents believe that encrypted solutions make it unnecessary to take other security measures.

In contrast, their colleagues in IT and IT security functions (referred to as IT security practitioners in this report) are diligent in taking all or most precautionary steps to safeguard the sensitive and confidential information on their laptops. They believe encryption is an important security tool, but believe it is critical to follow certain procedures to ensure that data is protected if a laptop is lost or stolen.

The following are some of the most salient findings:

- Eighty-nine percent of IT security practitioners report that someone in their organization has had a laptop lost or stolen and 47% report that it resulted in a data breach. Only 49% report that the organization was able to prove the contents were encrypted.
- Fifty-four percent of business managers surveyed strongly agree and agree that encryption stops cyber criminals from stealing data on laptops versus 50% of IT security practitioners who strongly agree or agree.
- Fifty-one percent of business managers surveyed record their encryption password on a private document to jog their memory such as a post-it note or share the key with other individuals. Virtually none of the IT security practitioners record their password on a private document or share it with another person.
- Forty-eight percent of business managers have disengaged their laptop's encryption solution and 42% admit this is in violation of their company's security policy.
- Fifty-six percent of business managers sometimes or often leave their laptop with a stranger when traveling.

We believe this research is particularly timely because previous studies conducted by Ponemon Institute have shown that the laptop is the number one cause of data loss. In this study we surveyed 435 IT security practitioners and 348 business managers in Canada. on the following topics related to individuals' use of laptop encryption:

- The use of encryption tools to protect information contained on the laptop computers assigned to them by their employer.
- Perceptions IT security practitioners have about the use of encryption to protect information assets.

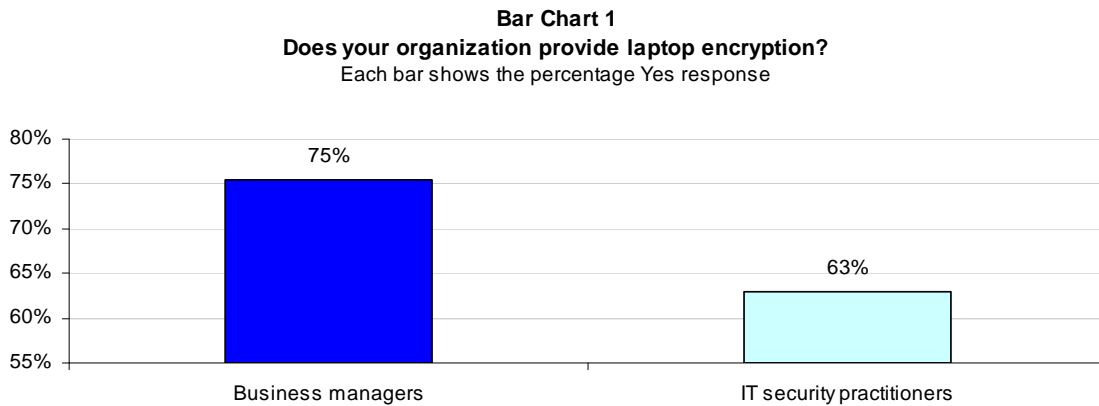
- Perceptions business managers have about the use of encryption to protect information assets.
- The procedures business managers follow or do not follow to safeguard the sensitive and confidential information on their laptops.

Key Findings

Following are the most salient findings of this survey research. Please note that most of the results are displayed in a bar or line chart format. The actual data utilized in each figure and referenced in the paper can be found in the percentage frequency tables attached as Appendix I to this paper.

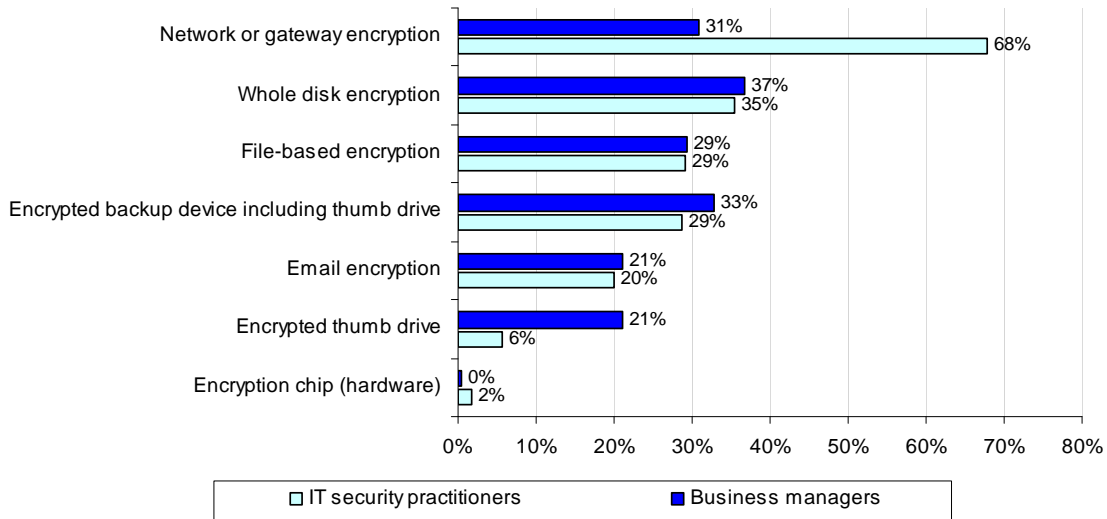
A large number of employees in participating organizations have encryption solutions on their laptops.

As shown in Bar Chart 1, 75% of IT security practitioners and 63% of business managers have employer-provided encryption solutions on their laptops.



Bar Chart 2 reports the most widely-used encryption solutions deployed by respondents' organizations. For IT security practitioners they are: network or gateway encryption (68%) followed by whole disk encryption (35%), file-based encryption (29%) and encrypted backup device including thumb drive (29%).

Bar Chart 2
What encryption solutions are used to protect content on laptops?

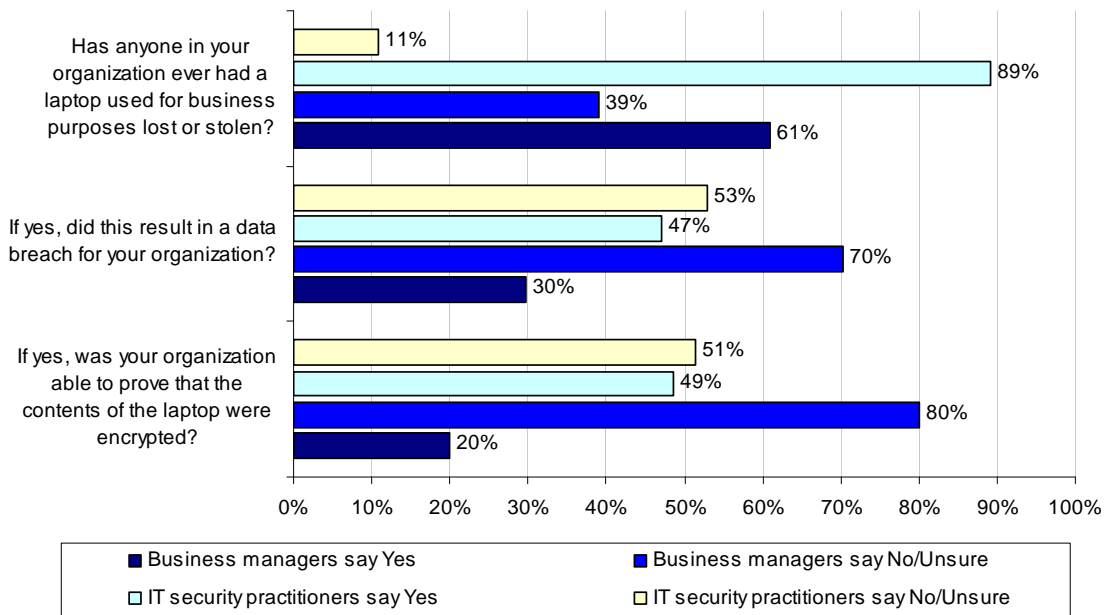


The most widely used solutions for business managers are whole disk encryption (37%), encrypted backup device including thumb drive (33%), network or gateway encryption (31%) and file-based encryption ((29%).

Organizations often are not able to prove data on lost or stolen computers was encrypted.

Bar Chart 3 reports that according to 89% of IT security practitioners, someone in their organization has had a laptop used for business purposes lost or stolen and 47% report that it resulted in a data breach for the organization. Only 49% report that their organization was able to prove the contents of the laptop were encrypted.

Bar Chart 3
Experience dealing with a lost laptop

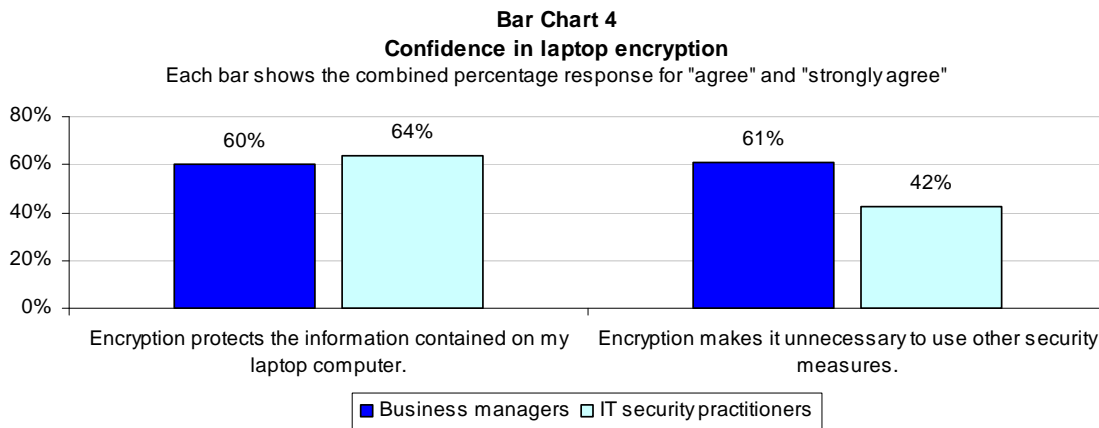


The above chart also shows that 61% of business managers report that someone in their organization had their laptop lost or stolen and 30% say it resulted in a data breach. Only 20% report that the organization was able to prove that the contents of the laptop were encrypted.

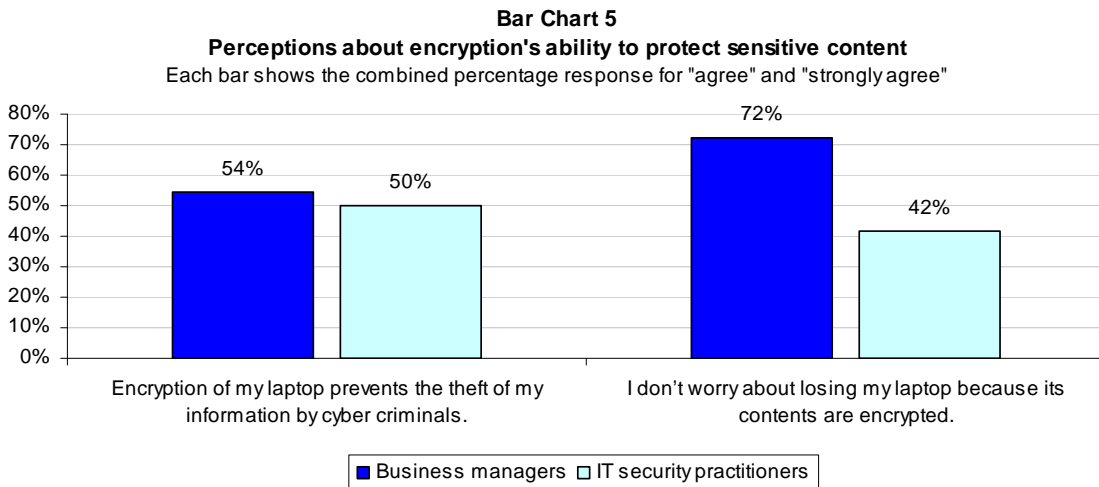
There is a high level of confidence among business managers in the belief that an encryption solution fully protects the sensitive and confidential information that resides on their laptops.

As shown in Bar Chart 4, 60% of business managers strongly agree or agree that encryption protects the information contained on their laptops and 61% of this same group strongly agree or agree it is not necessary to use other security solutions.

Sixty-three percent of IT security practitioners strongly agree or agree that encryption protects information contained on their laptop computers. But only 42% of this group strongly agree or agree that no other solutions are necessary.



When asked if encryption prevents theft by cyber criminals, 54% of business managers strongly agree or agree with the statement that "encryption of my laptop prevents the theft of my information by cyber criminals" versus 50% of IT security practitioners who strongly agree or disagree (Bar Chart 5). Thirty-two percent of respondents in the business manager group are uncertain and 34% in the IT security practitioners are uncertain if encryption of their laptops prevents theft by cyber criminals.

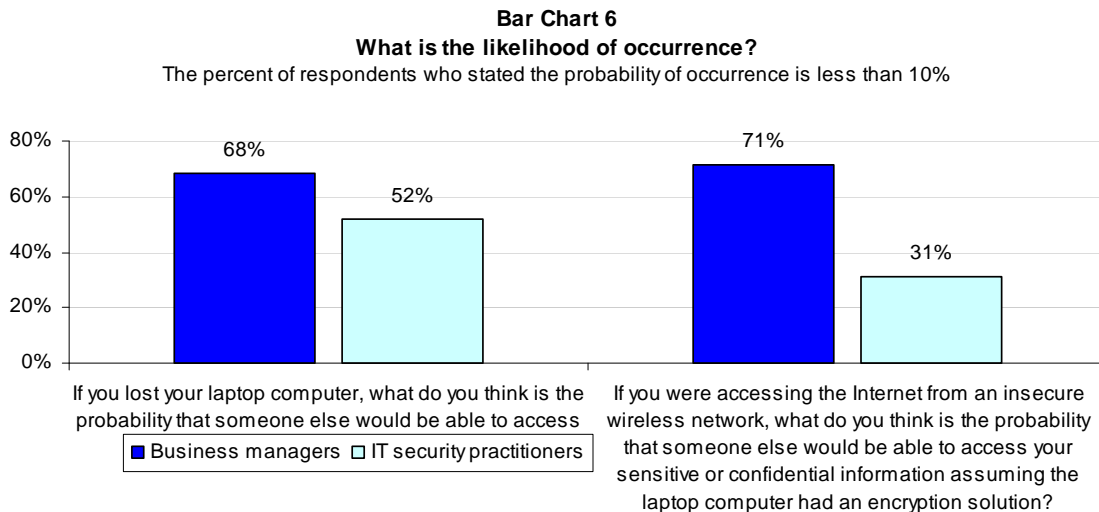


When asked if they would worry if they lost a laptop that was encrypted, 72% of business managers strongly agree or agree that they would not worry. However, only 42% of IT security practitioners would not worry if they lost their laptop.

IT security practitioners believe there is a higher probability than business managers believe that a lost laptop or access to an insecure wireless network will result in data loss.

Bar Chart 6 reports that 68% of business managers versus 52% of IT security practitioners believe that there is zero or less than a 10% chance of someone having the ability to access sensitive and confidential information if they lost their laptop.

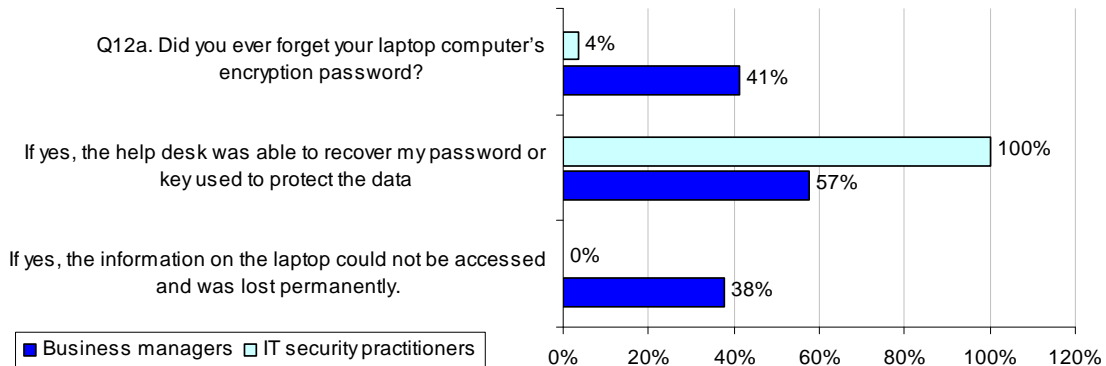
Assuming their laptops are encrypted, 72% of business managers believe that there is no chance or less than a 10% chance of having their sensitive information accessed if they should log on to an insecure wireless network. In contrast, only 32% of IT security practitioners are confident that there would be zero or less than a 10% chance of losing data when accessing an insecure wireless network.



Business managers put data at risk by not using encryption properly.

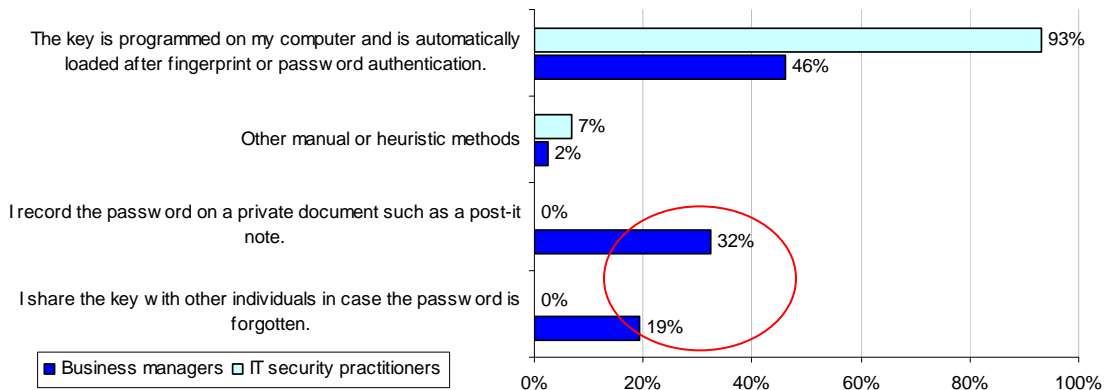
As shown in Bar Chart 7, 41% of business managers in our study admit to forgetting their laptop's encryption password. While 57% were able to recover their password or key used to protect the data by contacting their organizations' help desk, 38% could not gain access and information was lost permanently.

Bar Chart 7
Did you ever forget your laptop's encryption password?
 Each bar shows the percentage Yes response

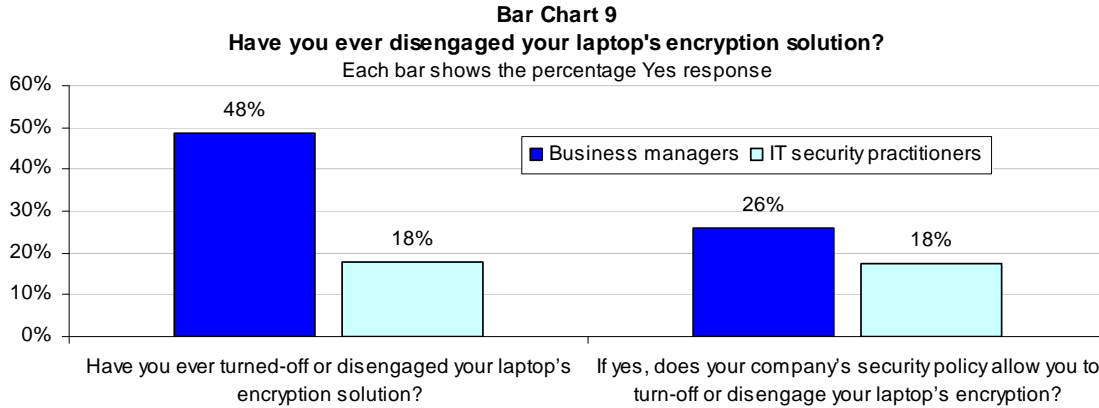


To manage their passwords, business managers may circumvent certain critical laptop security procedures. As shown in Bar Chart 8 below, 51% record their password on a private document such as a post-it note to jog their memory or share the key with other individuals in case they forget the password. Virtually none of the IT security practitioners record their password on a private document or share it with another person.

Bar Chart 8
How do you remember your encryption password?



Bar Chart 9 shows that 48% of business managers have disengaged their laptop's encryption solution. Twenty-six percent of those who turned off the encryption solution report that this practice is allowed in their company's security policy and 32% are unsure. In contrast, only 18% of IT security practitioners have disengaged the encryption solution, and 18% report that this practice is allowed by their company's security policy.



Business managers often don't take precautions and could be considered negligent in taking steps to safeguard the sensitive and confidential information on their laptops.

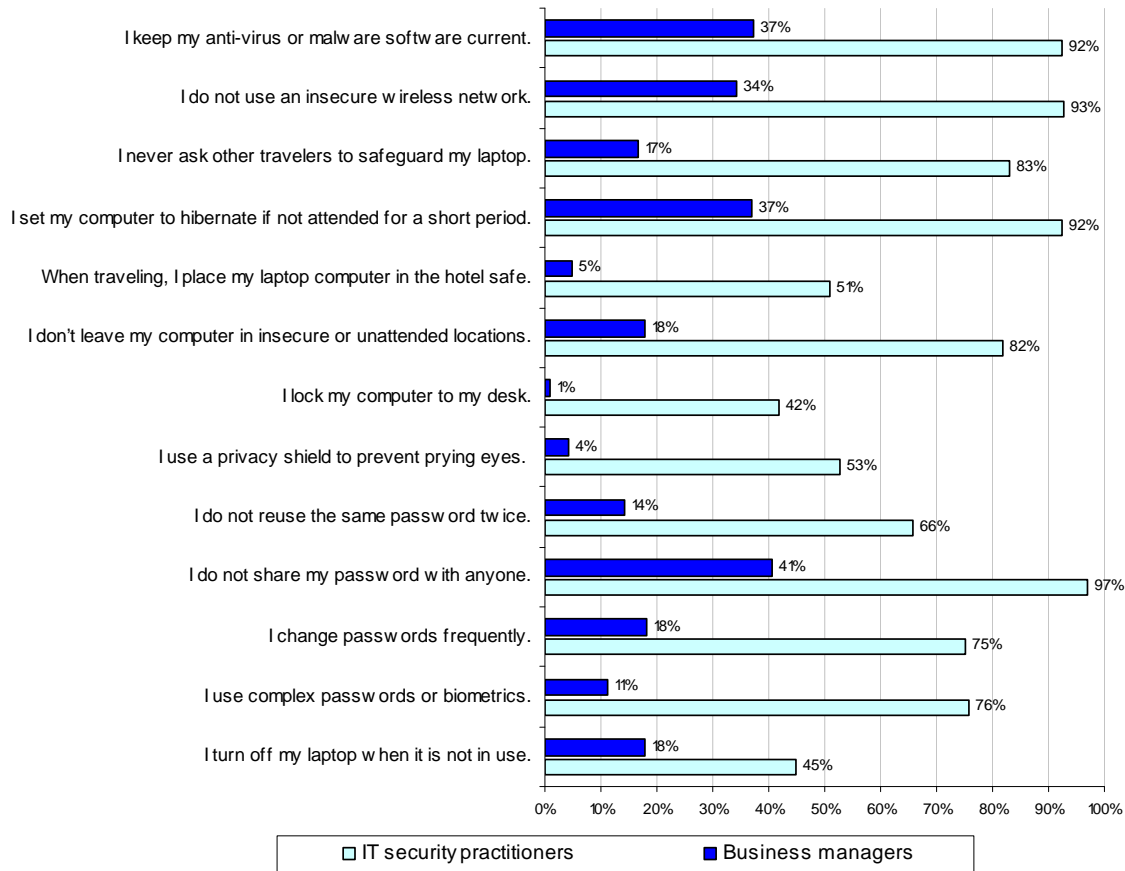
In this study, we asked both business managers and IT security practitioners to respond to questions about typical laptop security procedures. Bar Chart 10 shows the differences between these two groups. As is shown, business managers are putting their laptops at serious risk because of their tendency not to protect their passwords, to leave their laptops in unguarded situations and to access insecure wireless connections.

Specifically, among business managers, only 18% always turn off their computers when not in use, 11% of business managers always use complex passwords or biometrics to prevent unauthorized access to their laptop, 18% always change passwords frequently, 41% never share their passwords, 14% never reuse the same passwords, 4% always use a privacy shield to prevent prying eyes, 1% always physically lock their computer to their desk.

Bar Chart 10

The human factor in laptop security

Each bar is the percent of respondents who say that they take the following security precautions



When traveling, 18% never leave their computer in an insecure or unattended location, 5% always place their laptop in the hotel safe, 17% never leave their laptop with a stranger, 34% never use an insecure wireless network, 37% always keep their anti-virus or malware software current and 37% set their computer to hibernate if not attended in a very short period of time.

It is uncertain if business managers' negligence, as evidenced by the responses described above, is due to an over-reliance on encryption solutions. Although many in this group of respondents do believe that encryption is all that is needed to protect the information on their laptops. What is the conclusion here is that the human factor is the weakest link in any organizations' efforts to defend data at risk.

Among IT security practitioners, 45% always turn off their computer when not in use, 76% always use complex passwords or biometrics to prevent unauthorized access to their computers, 75% always change passwords frequently, 97% never share their passwords, 66% never reuse the same password, 53% always use a privacy shield to prevent prying eyes, 42% always physically lock their computer to their desk, and 82% never leave their computer alone in an insecure or unattended location. Ninety-two percent set their computer to hibernate if not attended to for a very short period of time and the same percentage always keeps their anti-virus or malware software current.

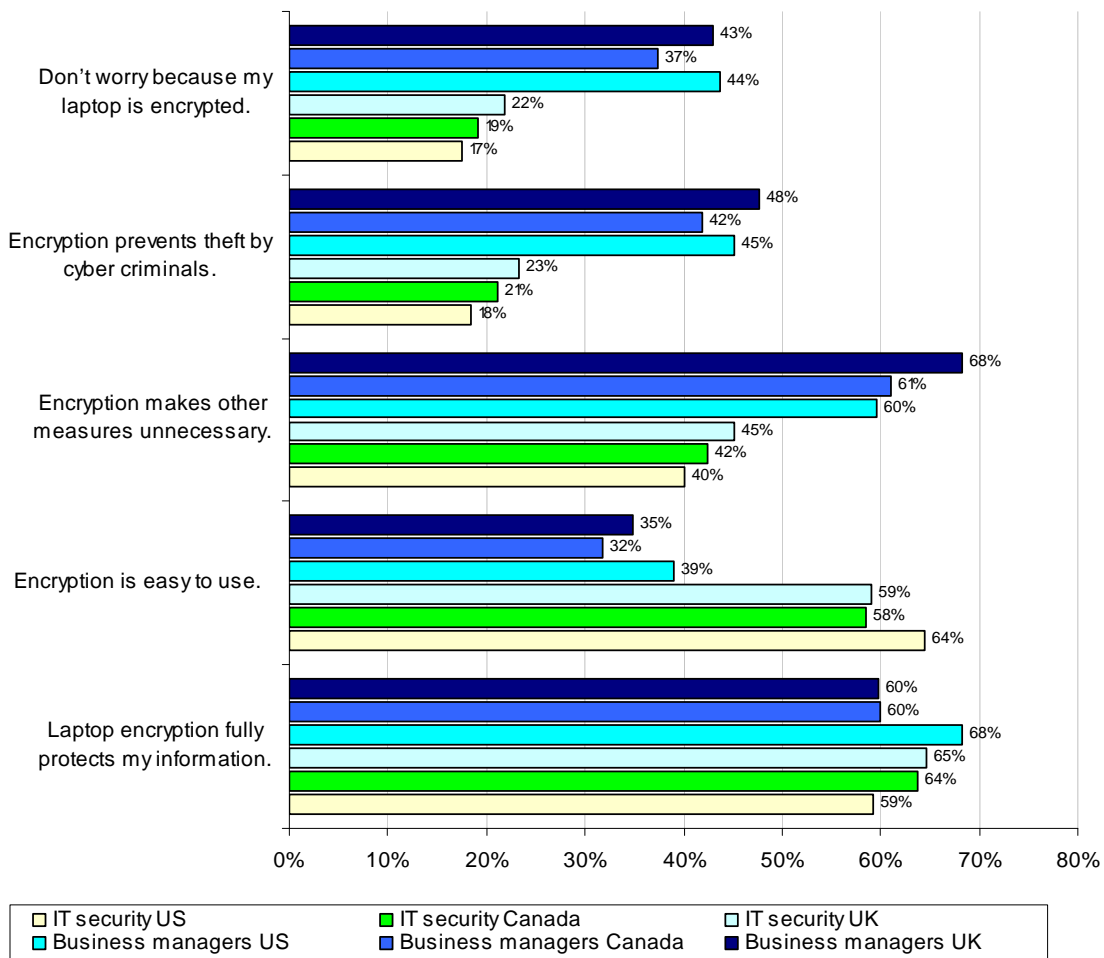
When traveling, 51% always put their laptop in a hotel safe, 83% never leave their computer alone with a stranger and 93% never use an insecure wireless network.

Comparisons of Canada, US and UK

In addition to this Canada study, we completed concurrent surveys for IT security practitioners and business managers from organizations in the US and UK.¹ In all three countries, IT security practitioners face the same challenge of keeping sensitive and confidential information safeguarded in spite of the actions of business managers who may be relying on encryption to protect data and not following critical security procedures. There are significant gaps between the security practices of business managers and IT security practitioners in all three countries.

Bar Chart 11 shows differences between business managers and IT security practitioners in Canada, US, and the United Kingdom about various attributions of encryption. In Canada, there is slightly more of a gap between business managers and IT security practitioners in how worried respondents would be if an encrypted laptop was lost or stolen and prevention of cyber criminals from stealing information.

Bar Chart 11
Comparison of laptop encryption attributions for the US, Canada and UK
 Each bar represents the combined percentage of "Strongly Agree" and "Agree" responses

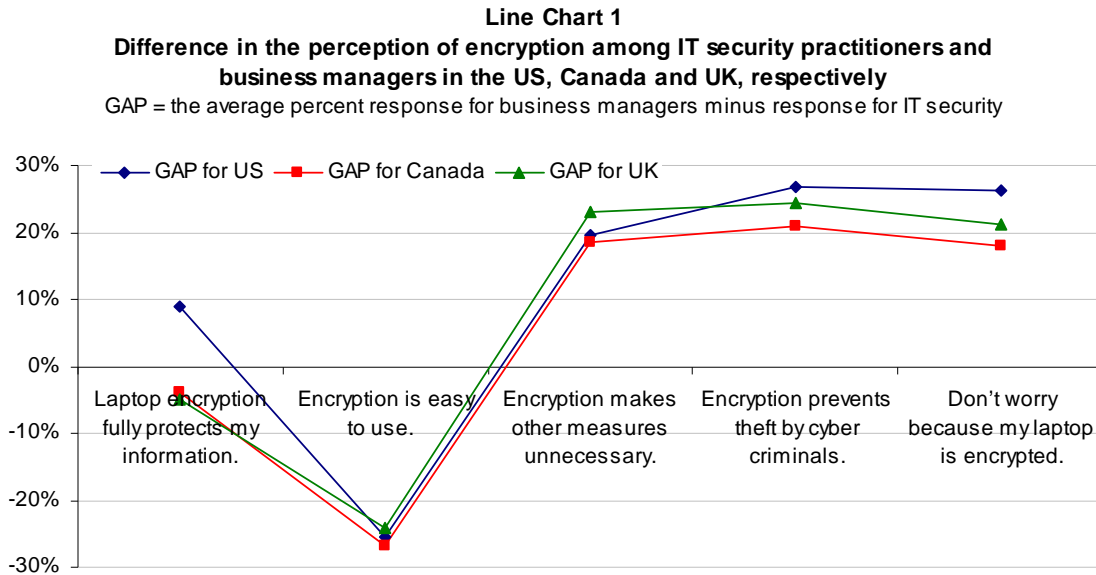


¹ The US study included 720 IT security practitioners and 874 business managers. The UK study involved 499 business managers and 645 IT security practitioners.

Line Chart 1 recasts the average results shown in the above bar chart to highlight the differences or gaps between the IT security practitioner and business manager samples in three countries.

As can be seen, the gaps – defined as the average percentage response for business managers minus the average percent response for IT security practitioners – are remarkably consistent for all three countries. As can be seen, business managers are much more likely than IT security practitioners to:

- Believe encryption makes it unnecessary to use other security measures for laptop protection
- Believe encryption is more likely to prevent the theft of information by cyber criminals
- Not worry about losing a laptop because the contents are encrypted



In contrast, IT security practitioners in the US, Canada and UK are much more likely than business managers to believe laptop encryption solutions are easy to use.

We believe the primary conclusion that can be drawn from this study is that business managers in all three countries are either negligent in the protection of sensitive and confidential information on their laptops or they may be overly dependent on encryption to keep this information secure. Encryption is an excellent security tool. However, if encryption is turned off, if passwords are shared or if other risks are taken, organizations that utilize encryption technologies alone to ensure the security of confidential information may not be well protected from the possibility of a public data breach.

Survey Caveats

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

- Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of managers in IT security and non-IT business functions, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

- **Sampling-frame bias:** The accuracy is based on contact information and the degree to which the sample is representative of individuals in the IT and non-IT business disciplines. We also acknowledge that the results may be biased by external events. We also acknowledge bias caused by compensating subjects to complete this research within a holdout period. Finally, because we used a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.
- **Self-reported results:** The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide a truthful response.

Sample

Two random sampling frames of adult-aged individuals who reside in Canada were used to recruit participants to this web survey.² Our randomly selected sampling frames were selected from three national lists of IT, security, compliance and data protection professionals.

Table 1 Sample description	IT Security	Non-IT Business
Total sampling frame	6,982	5,916
Bounce-back	1,854	1,305
Total returns	456	368
Rejected surveys	21	20
Final sample	435	348
Response rate	6.2%	5.9%

Table 1 shows 435 respondents in IT security and 348 in non-IT business functions successfully completed the survey within an eight-day research period. Of returned instruments, less than 1.5% was omitted because of poor reliability. The final samples represent a 6.2% net response rate for IT security and 5.9% net response rate for business managers. The margin of error on all adjective scale and Yes/No/Unsure responses is ≤ 5 percent.

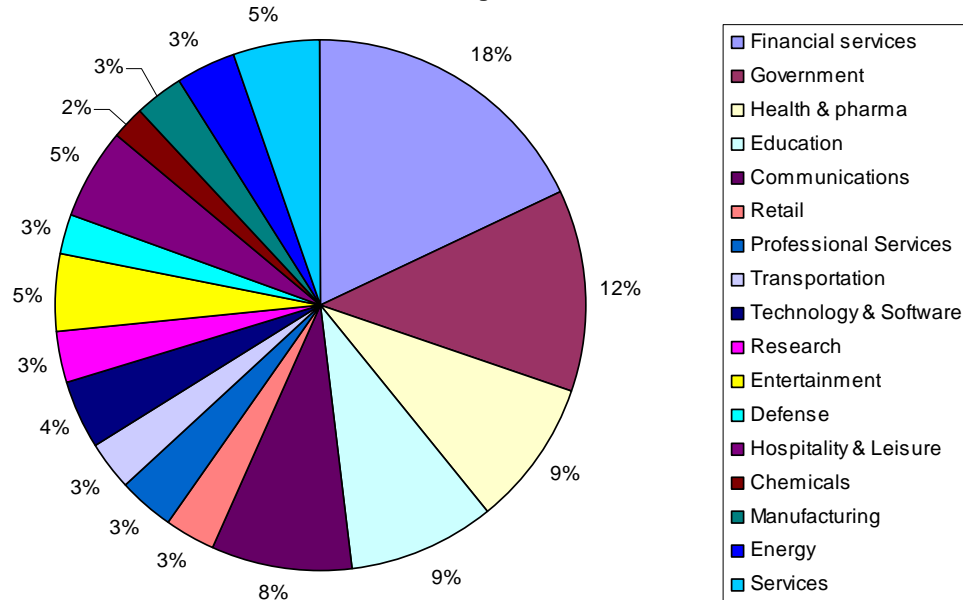
The mean experience level for the IT security sample is 14.3 years and for the non-IT business sample is 11.7 years. Over 95% of respondents completed all survey items within 12 minutes. Following are key demographics and organizational characteristics for Canadian respondents. Table 2 reports the organizational level of respondents in both samples. As can be seen, the majority of respondents in both samples are at the director, manager or supervisor levels.

Table 2 What organizational level best describes your current position?	IT Security	Non-IT Business
Senior Executive	2%	2%
Vice President	3%	4%
Director	23%	17%
Manager/Supervisor	41%	52%
Associate/Staff/Technician	24%	22%
Other	6%	3%
Total	100%	100%

² Respondents were given nominal compensation to complete all survey questions.

Pie Chart 1 reports the average distribution of respondents in both samples by their organization's primary industry classification. As shown, 18% of respondents are employed by financial service companies (including insurance, banking, credit cards, brokerage and investment management), and 12% work for federal, provincial or local government.

Pie Chart 1
Industry Distribution of Combined Sample of IT security practitioners and non-IT business managers



In total, 59% of respondents were males and 41% females. While results are skewed on the gender variable (more male than female respondents), this result is consistent with known demographics about the corporate IT fields in North America.

Table 3 reports the approximate full time equivalent headcount of respondents' organizations for both the IT security and business manager samples, respectively. As can be seen, 66% of the IT security sample, and 64% of the business manager sample, are employed by larger-sized organizations with more than 5,000 employees.

Table 3 What is the worldwide headcount of your organization?	IT security practitioners	Business managers
Less than 500 people	1%	1%
500 to 1,000 people	5%	6%
1,001 to 5,000 people	28%	29%
5,001 to 25,000 people	36%	36%
25,001 to 75,000 people	21%	21%
More than 75,000 people	9%	7%
Total	100%	100%

The following Appendix provides additional organizational characteristics and demographics for respondents in IT security and business managers.

If you have questions or comments about this research report or you would like to obtain additional copies of the document (including permission to quote from or reuse this report), please contact us by letter, phone call or e-mail:

Ponemon Institute LLC
Attn: Research Department
2308 US 31 North
Traverse City, Michigan 49686
1.800.887.3118
research@ponemon.org

Ponemon Institute LLC

Advancing Responsible Information Management

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

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

Appendix 1: Detailed Survey Results

Field work completed on November 7, 2008

The following table describes the sample response from two independent panels consisting of 435 practitioners in IT security and 348 in non-IT business functions. By design, at the time of this survey, all respondents were employed by organizations located in Canada.

Part I. Background & screening		
	IT Security Practitioners	Non-IT Business Managers
Q1. Does your job require you to use a laptop computer?		
Yes	85%	93%
No (stop)	15%	7%
Total	100%	100%

	IT Security Practitioners	Non-IT Business Managers
Q2a. Does your organization provide encryption tools to help protect information contained on your laptop computer?		
No (go to Q2b)	24%	30%
Yes (go to Q2c)	75%	63%
Unsure (stop)	1%	7%
Total	100%	100%

	IT Security Practitioners	Non-IT Business Managers
Q2b. If no, why don't you use encryption to protect information on your laptop? Please select your one best response.		
Encryption is too complex	16%	14%
I can't remember the encryption password	0%	4%
Encryption slows down my computer's performance	13%	29%
Encryption causes my operating system to crash	11%	23%
Encryption is not necessary because of other controls such as biometrics or system passwords	29%	24%
Encryption is too expensive for my company	28%	4%
Don't know why	2%	2%
Other (please specify)	1%	0%
Total	100%	100%

	IT Security Practitioners	Non-IT Business Managers
Q2c. If yes, what encryption solutions do you use to protect information on your laptop computer? Please check all that apply.		
Whole disk encryption	35%	37%
Email encryption	20%	21%
File-based encryption	29%	29%
Network or gateway encryption	68%	31%
Encryption chip (hardware)	2%	0%
Encrypted thumb drive	6%	21%
Encrypted backup device including thumb drive	29%	33%
Other (please specify)	4%	0%
Total	192%	173%

Part II. Your experiences using encryption		
Q3a. Has anyone in your organization ever had a laptop used for business purposes lost or stolen?	IT Security Practitioners	Non-IT Business Managers
Yes	89%	61%
No	11%	39%
Total	100%	100%

Q3b. If yes, did this result in a data breach for your organization?	IT Security Practitioners	Non-IT Business Managers
Yes	47%	30%
No	41%	42%
Unsure	12%	29%
Total	100%	100%

Q3c. If yes, was your organization able to prove that the contents of the laptop were encrypted?	IT Security Practitioners	Non-IT Business Managers
Yes	49%	20%
No	44%	39%
Unsure	8%	41%
Total	100%	100%

Please rate the following five statements using the scale found below each item.

Q4. Encryption protects the information contained on my laptop computer.	IT Security Practitioners	Non-IT Business Managers
Strongly agree	29%	29%
Agree	34%	31%
Unsure	23%	26%
Disagree	10%	12%
Strongly disagree	3%	2%
Total	100%	100%

Q5. My laptop's encryption solution is easy to use.	IT Security Practitioners	Non-IT Business Managers
Strongly agree	19%	10%
Agree	40%	22%
Unsure	15%	22%
Disagree	19%	40%
Strongly disagree	7%	6%
Total	100%	100%

Q6. Encryption makes it unnecessary to use other security measures.	IT Security Practitioners	Non-IT Business Managers
Strongly agree	21%	42%
Agree	21%	19%
Unsure	31%	30%
Disagree	19%	7%
Strongly disagree	8%	2%
Total	100%	100%

Q7. Encryption of my laptop prevents the theft of my information by cyber criminals.	IT Security Practitioners	Non-IT Business Managers
Strongly agree	19%	37%
Agree	31%	17%
Unsure	34%	32%
Disagree	14%	13%
Strongly disagree	2%	0%
Total	100%	100%

Q8. I don't worry about losing my laptop because its contents are encrypted.	IT Security Practitioners	Non-IT Business Managers
Strongly agree	13%	35%
Agree	28%	37%
Unsure	11%	16%
Disagree	34%	10%
Strongly disagree	13%	2%
Total	100%	100%

Q9. How much extra time is required to load your computer's encryption solution each time you use your laptop or launch the computer's browser?	IT Security Practitioners	Non-IT Business Managers
No additional time required	9%	5%
Less than 30 seconds	34%	33%
Between 31 to 60 seconds	30%	30%
Between 1 to 2 minutes	19%	16%
Between 2 to 3 minutes	6%	10%
More than 3 minutes.	1%	5%
Total	100%	100%

Q10a. Have you ever turned-off or disengaged your laptop's encryption solution?	IT Security Practitioners	Non-IT Business Managers
Yes	18%	48%
No	82%	52%
Total	100%	100%

Q10b. If yes, does your company's security policy allow you to turn-off or disengage your laptop's encryption?	IT Security Practitioners	Non-IT Business Managers
Yes	18%	26%
No	82%	42%
Unsure	0%	32%
Total	100%	100%

Q11a. If you lost your laptop computer, what do you think is the probability that someone else would be able to access your sensitive or confidential information?	IT Security Practitioners	Non-IT Business Managers
Zero (no chance whatsoever)	26%	42%
Less than 10%	26%	26%
Between 11 and 20%	18%	18%
Between 21% and 30%	18%	8%
Between 31% and 40%	9%	4%
Between 41% and 50%	1%	1%
More than 50%	2%	1%
Total	100%	100%

Q11b. If you were accessing the Internet from an insecure wireless network, what do you think is the probability that someone else would be able to access your sensitive or confidential information assuming the laptop computer had an encryption solution?	IT Security Practitioners	Non-IT Business Managers
Zero (no chance whatsoever)	13%	45%
Less than 10%	19%	27%
Between 11 and 20%	30%	12%
Between 21% and 30%	18%	9%
Between 31% and 40%	16%	5%
Between 41% and 50%	2%	2%
More than 50%	2%	0%
Total	100%	100%

Q12a. Did you ever forget your laptop computer's encryption password?	IT Security Practitioners	Non-IT Business Managers
Yes	4%	41%
No	96%	59%
Total	100%	100%

Q12b. If yes, what happened?	IT Security Practitioners	Non-IT Business Managers
The help desk was able to recover my password or key used to protect the data	100%	57%
Information on the laptop could not be accessed and was lost permanently.	0%	38%
Other (please specify)	0%	5%
Total	100%	100%

	IT Security Practitioners	Non-IT Business Managers
Q13. How do you remember your encryption password?		
The key is programmed on my computer and is automatically loaded after fingerprint or password authentication.	93%	46%
I record the password on a private document such as a post-it note.	0%	32%
I share the key with other individuals in case the password is forgotten.	0%	19%
Other (please specify)	7%	2%
Total	100%	100%

Part III. Please respond to each attribute using the four choices provided below each action.

	IT Security Practitioners	Non-IT Business Managers
Q14. I turn off my laptop computer when it is not in use.		
Always do this	45%	18%
Sometimes do this	48%	33%
Rarely do this	6%	33%
Never do this	1%	16%
Total	100%	100%

	IT Security Practitioners	Non-IT Business Managers
Q15. I use complex passwords or biometrics to prevent unauthorized access to my laptop.		
Always do this	76%	11%
Sometimes do this	24%	20%
Rarely do this	1%	46%
Never do this	0%	23%
Total	100%	100%

	IT Security Practitioners	Non-IT Business Managers
Q16. I change passwords frequently (90 days or less).		
Always do this	75%	18%
Sometimes do this	22%	22%
Rarely do this	0%	43%
Never do this	2%	18%
Total	100%	100%

	IT Security Practitioners	Non-IT Business Managers
Q17. I do not share my password with anyone else.		
I never share	97%	41%
I rarely share	1%	30%
I sometimes share	2%	21%
I frequently share	0%	8%
Total	100%	100%

	IT Security Practitioners	Non-IT Business Managers
Q18. I do not reuse the same password.		
I never reuse the same password	66%	14%
I rarely reuse the same password	34%	20%
I sometimes reuse the same password	0%	36%
I frequently reuse the same password	0%	30%
Total	100%	100%

	IT Security Practitioners	Non-IT Business Managers
Q19. I use a privacy shield (screen) to prevent prying eyes.		
I always use a privacy shield on my computer	53%	4%
I sometimes use a privacy shield on my computer	15%	6%
I rarely use a privacy shield on my computer	11%	13%
I never use a privacy shield on my computer	21%	77%
Total	100%	100%

	IT Security Practitioners	Non-IT Business Managers
Q20. I lock my computer to my desk.		
I always physically lock my computer to my desk	42%	1%
I sometimes physically lock my computer to my desk	25%	5%
I rarely physically lock my computer to my desk	4%	16%
I never physically lock my computer to my desk	29%	78%
Total	100%	100%

	IT Security Practitioners	Non-IT Business Managers
Q21. I don't leave my computer in insecure or unattended locations.		
I never leave my computer alone in an insecure location	82%	18%
I rarely leave my computer alone in an insecure location	14%	28%
I sometimes leave my computer alone in an insecure location	3%	29%
I frequently leave my computer alone in an insecure location	1%	25%
Total	100%	100%

	IT Security Practitioners	Non-IT Business Managers
Q22. When traveling, I place my laptop computer in the hotel safe.		
Always do this	51%	5%
Sometimes do this	18%	11%
Rarely do this	15%	18%
Never do this	16%	66%
Total	100%	100%

Q23. I set my computer to hibernate (shut down) if not attended in a very short period of time (usually less than 1 minute).	IT Security Practitioners	Non-IT Business Managers
Always do this	92%	37%
Sometimes do this	5%	31%
Rarely do this	3%	18%
Never do this	0%	14%
Total	100%	100%

Q24. When traveling, I never leave my computer under the watchful eyes of other travelers, even for a short period of time.	IT Security Practitioners	Non-IT Business Managers
I never leave my computer alone with a stranger	83%	17%
I rarely leave my computer alone with a stranger	13%	26%
I sometimes leave my computer alone with a stranger	4%	27%
I often leave my computer alone with a stranger	0%	29%
Total	100%	100%

Q25. When traveling on business with my laptop, I do not use an insecure wireless network.	IT Security Practitioners	Non-IT Business Managers
I never use an insecure wireless network while traveling	93%	34%
I rarely use an insecure wireless network while traveling	6%	34%
I sometimes use an insecure wireless network while traveling	1%	16%
I frequently use an insecure wireless network while traveling	0%	15%
Total	100%	100%

Q26. I keep my anti-virus or malware software current.	IT Security Practitioners	Non-IT Business Managers
Always do this	92%	37%
Sometimes do this	7%	39%
Rarely do this	0%	13%
Never do this	0%	11%
Total	100%	100%

Part IV. Organization characteristics and respondent demographics		
What organizational level best describes your current position?	IT Security Practitioners	Non-IT Business Managers
Senior Executive	2%	2%
Vice President	3%	4%
Director	23%	17%
Manager/Supervisor	41%	52%
Associate/Staff/Technician	24%	22%
Other (please describe)	6%	3%
Total	100%	100%

Check the Primary Person you or your supervisor reports to within your organization.	IT Security Practitioners	Non-IT Business Managers
CEO/Executive Committee	0%	12%
Chief Financial Officer	7%	8%
Chief Information Officer	53%	32%
Compliance Officer	4%	8%
Chief Privacy Officer	1%	10%
Director of Internal Audit	2%	8%
General Counsel	0%	2%
Chief Technology Officer	10%	0%
Human Resources VP	1%	9%
Chief Security Officer	12%	1%
Chief Risk Officer	4%	7%
Other (please describe)	6%	1%
Total	100%	1%
		100%

Regions	IT Security Practitioners	Non-IT Business Managers
Canada East	52%	54%
Canada Midwest	17%	18%
Canada West	25%	24%
Canada Atlantic	7%	4%
Total	100%	100%

Experience in years	IT Security Practitioners	Non-IT Business Managers
Total years of business experience	14.31	11.68
Total years in IT or data security	12.02	9.19
Total years in current position	4.98	4.28

Educational and career background:	IT Security Practitioners	Non-IT Business Managers
Compliance (auditing, accountant, legal)	2%	29%
IT (systems, software, computer science)	67%	12%
Security (law enforcement, military, intelligence)	18%	21%
Other non-technical field	4%	26%
Other technical field	9%	11%
Total	100%	100%

What is the approximate size of your IT department in terms of full-time equivalent (FTE) headcount?	IT Security Practitioners	
Less than 10 people	2%	
Between 10 to 50 people	5%	
Between 50 to 100 people	9%	
Between 100 to 500 people	19%	
Between 500 to 1,000 people	27%	
Between 1,000 to 2,000 people	30%	
Over 2,000 people	7%	
Total	100%	
What industry best describes your organization's industry concentration or focus?	IT Security Practitioners	Non-IT Business Managers
Airlines	1%	1%
Automotive	1%	0%
Agriculture	1%	0%
Brokerage	4%	3%
Cable	2%	3%
Chemicals	2%	2%
Credit Cards	4%	4%
Defense	4%	2%
Education	8%	10%
Entertainment	4%	5%
Services	4%	6%
Health Care	6%	7%
Hospitality & Leisure	5%	6%
Manufacturing	3%	3%
Insurance	3%	2%
Internet & ISPs	2%	5%
Government	13%	12%
Pharmaceutical	2%	2%
Professional Services	2%	5%
Research	2%	4%
Retail	4%	2%
Banking	8%	8%
Energy	4%	3%
Telecommunications	1%	2%
Technology & Software	5%	3%
Transportation	2%	1%
Wireless	1%	0%
Total	100%	100%

What best describes your role in managing privacy and data protection risks within your organization? Check all that apply.	IT Security Practitioners	Non-IT Business Managers
Setting priorities	49%	54%
Managing budgets	52%	55%
Selecting vendors and contractors	48%	51%
Determining privacy and data protection strategy	44%	47%
Evaluating program performance	60%	60%
Total	253%	267%

What is the worldwide headcount of your organization?	IT Security Practitioners	Non-IT Business Managers
Less than 500 people	1%	1%
500 to 1,000 people	5%	6%
1,001 to 5,000 people	28%	29%
5,001 to 25,000 people	36%	36%
25,001 to 75,000 people	21%	21%
More than 75,000 people	9%	7%
Total	100%	100%