



The Human Factor in Laptop Encryption: UK Study

Sponsored by
Absolute Software

Independently conducted by Ponemon Institute LLC

Publication Date: December 2008

The Human Factor in Laptop Encryption: UK 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 Laptop 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 also was conducted in the United States and Canada. The results are published in separate reports.

What we learned is that a high percentage of employees we surveyed in 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 screen shield, keeping their laptop physically safe when traveling or locking their laptops to their desks 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-six percent of IT security practitioners report that someone in their organization has had a laptop lost or stolen and 56% report that it resulted in a data breach. Only 45% report that the organization was able to prove the contents were encrypted.
- Fifty-nine percent of business managers surveyed strongly agree and agree that encryption stops cyber criminals from stealing data on laptops versus 46% of IT security practitioners who strongly agree or agree.
- Sixty-five percent of business managers surveyed record their encryption password on a private document such as a post-it note to jog their memory 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.
- Fifty percent of business managers have disengaged their laptop's encryption solution and 40% admit this is in violation of their company's security policy.
- Fifty-two 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 645 IT security practitioners and 499 business managers in the U.K. 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.

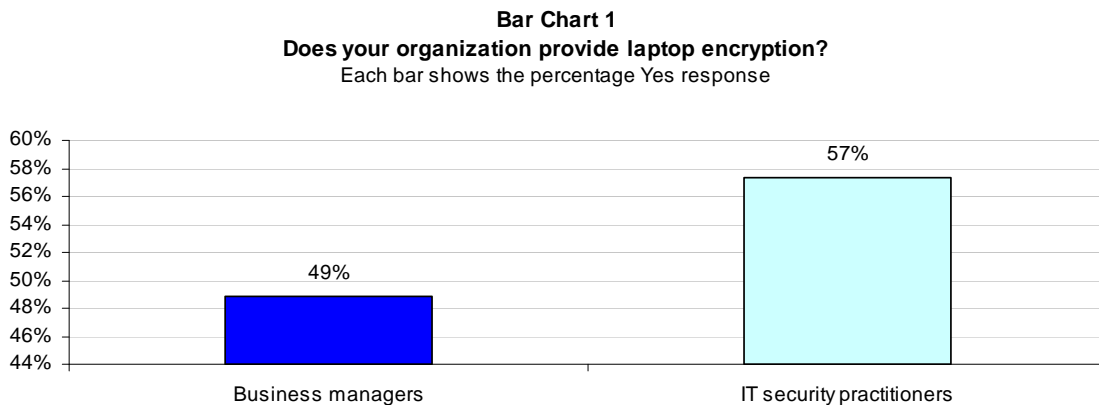
- Perceptions business managers have about the use of encryption to protect information assets.
- The procedures business managers follow or not follow to safeguard the sensitive and confidential information on their laptops.

Key Findings

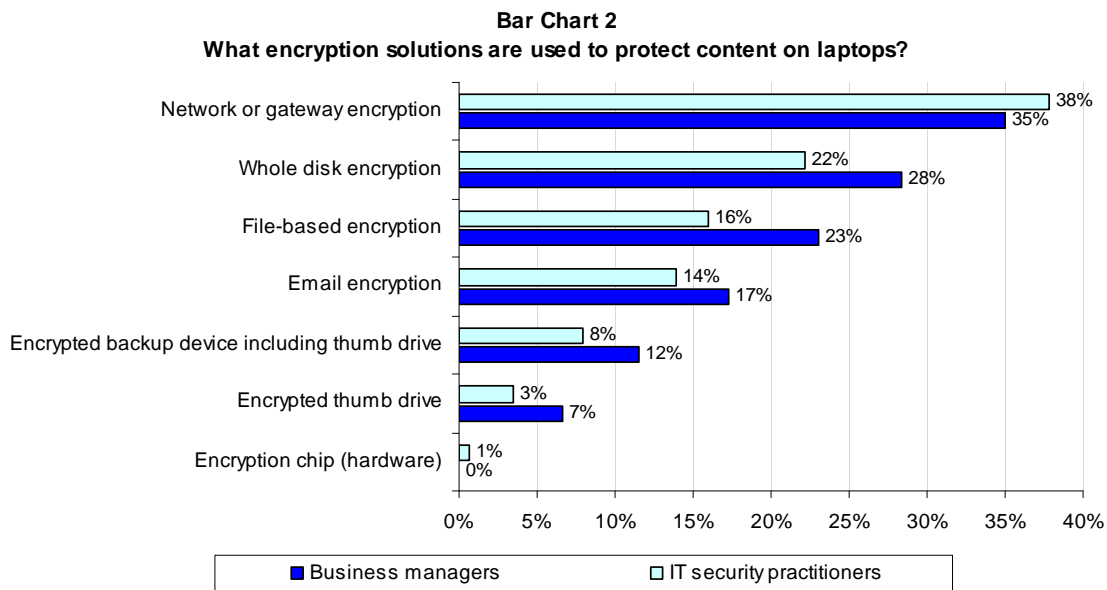
Following are the key findings of this survey research. Please note that most of the results are displayed in a bar or line chart format. The actual data utilized in each figure and referenced in the paper can be found in the percentage frequency tables attached as Appendix I to this paper.

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

As shown in Bar Chart 1, 57% of IT security practitioners and 49% of business managers have employer-provided encryption solutions on their laptops.

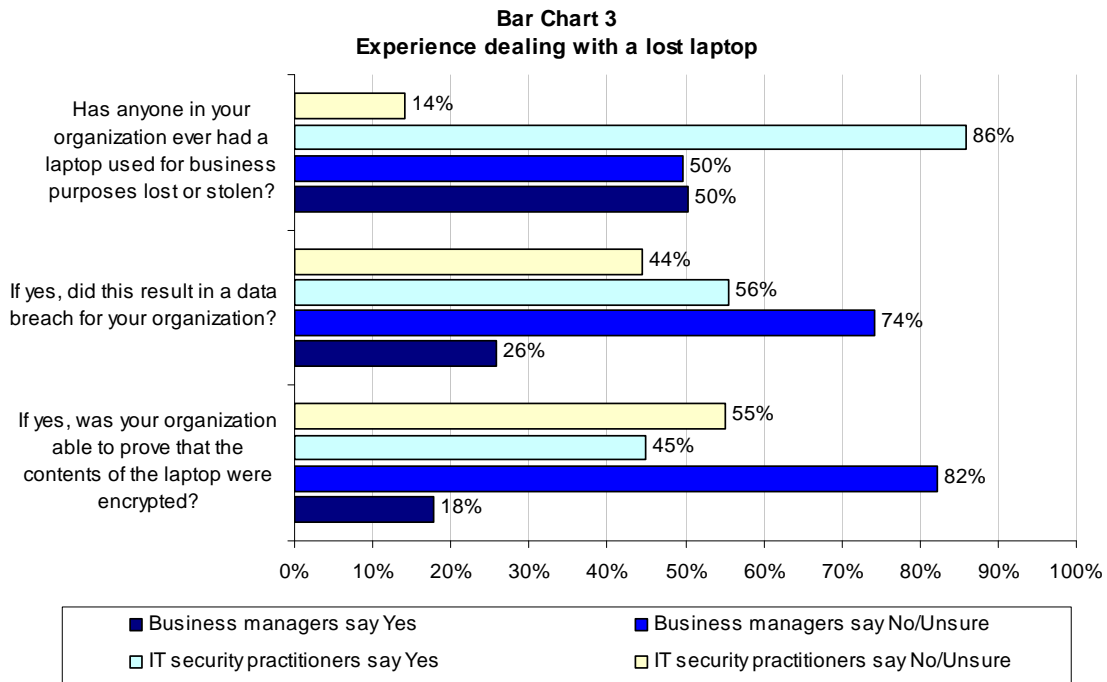


Bar Chart 2 reports the most widely-used encryption solutions for both groups. They are network or gateway encryption (38% IT security practitioners and 35% of business managers). This is followed by whole disk encryption (22% IT and 28% for business managers) and file-based encryption (16% IT and 23% business managers).



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

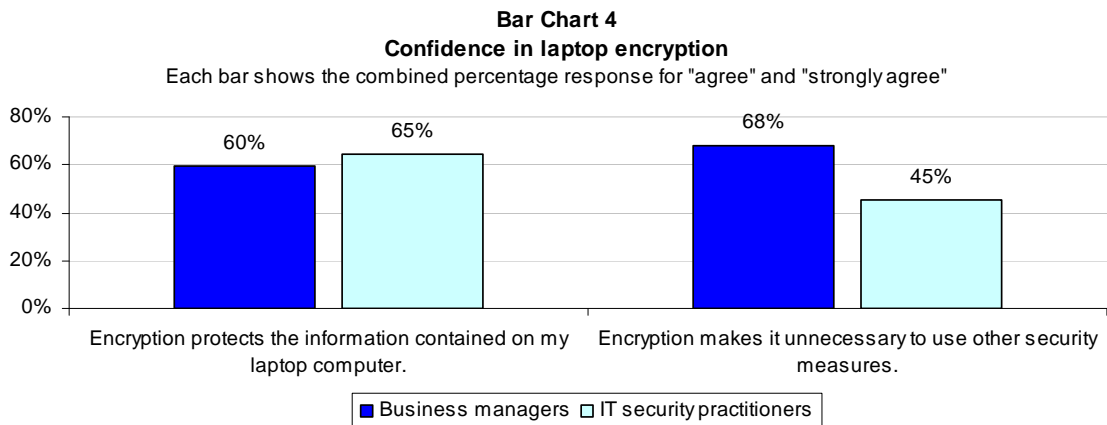
Bar Chart 3 reports that according to 86% of IT security practitioners, someone in their organization has had a laptop used for business purposes lost or stolen and 56% report that it resulted in a data breach for the organization. Only 45% report that their organization was able to prove the contents of the laptop were encrypted.



The above chart also shows that 50% of business managers report that someone in their organization had their laptop lost or stolen and 26% say it resulted in a data breach. Only 18% report that the organization was able to prove that the contents of the laptop were encrypted.

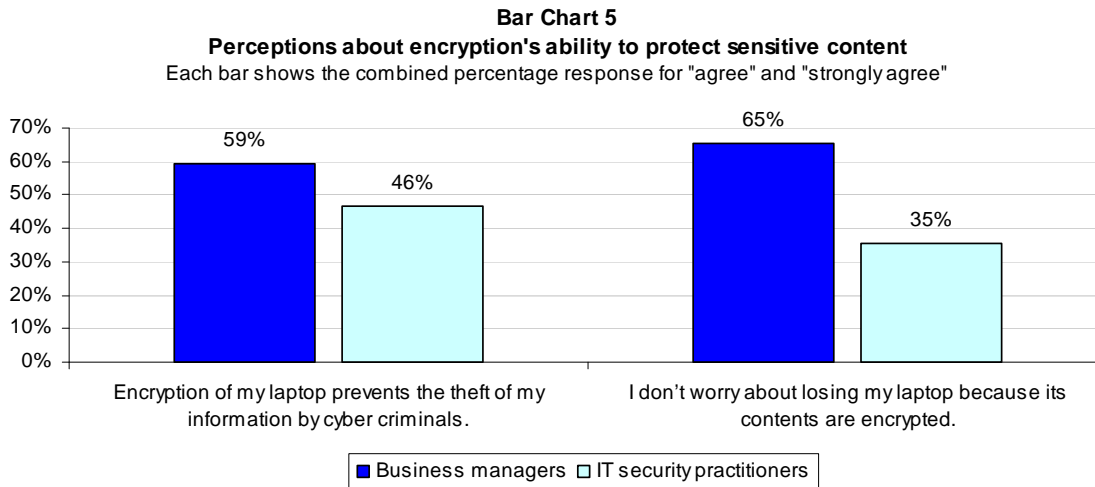
There is more confidence among IT security practitioners in the ability of encryption to protect the sensitive and confidential information that resides on their laptops.

As shown in Bar chart 4, 60% of business managers strongly agree or agree that encryption protects the information contained on their laptops and 68% of this same group strongly agree or agree that with encryption no other security solutions are necessary.



While 65% of IT security practitioners strongly agree or agree that encryption protects the information contained on their laptops, only 45% strongly agree or agree encryption makes it unnecessary to use other security measures.

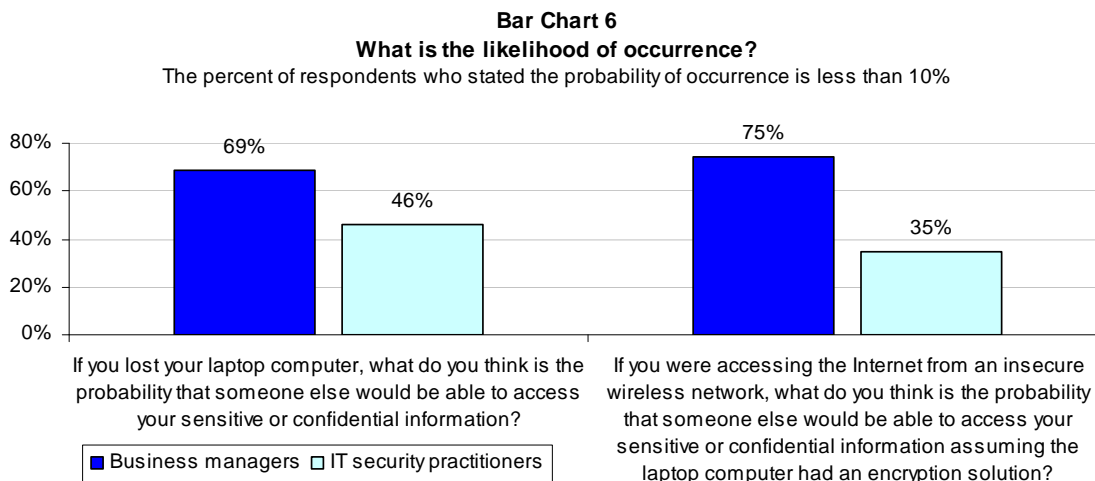
The gap in perceptions about the ability of encryption to protect information continues between these two groups when asked if encryption prevents theft by cyber criminals. As shown in Bar Chart 5, 59% of business managers strongly agree or agree with the statement that “encryption of my laptop prevents the theft of my information by cyber criminals” versus 46% of IT security practitioners who strongly agree or agree with this statement. Thirty-five percent of business managers are unsure if this is the case and 36% in the IT security practitioner are unsure.



When asked if they would worry if they lost a laptop that was encrypted, 65% percent of business managers strongly agree or agree that they would not worry. However, only 35% of IT security practitioners would not worry.

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 69% of business managers versus 46% 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.

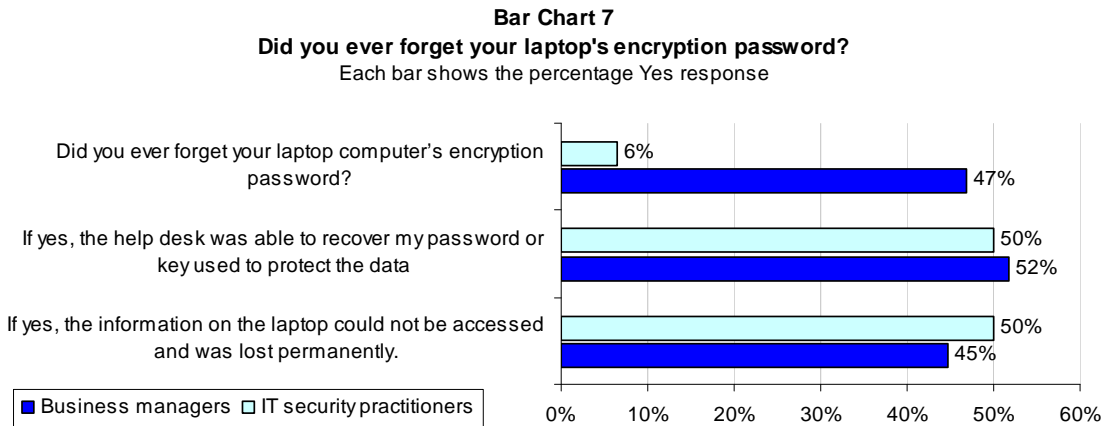


Assuming their laptops are encrypted, 75% of business managers believe that there is no chance or less than a 10% chance of having their sensitive information accessed if they should access an

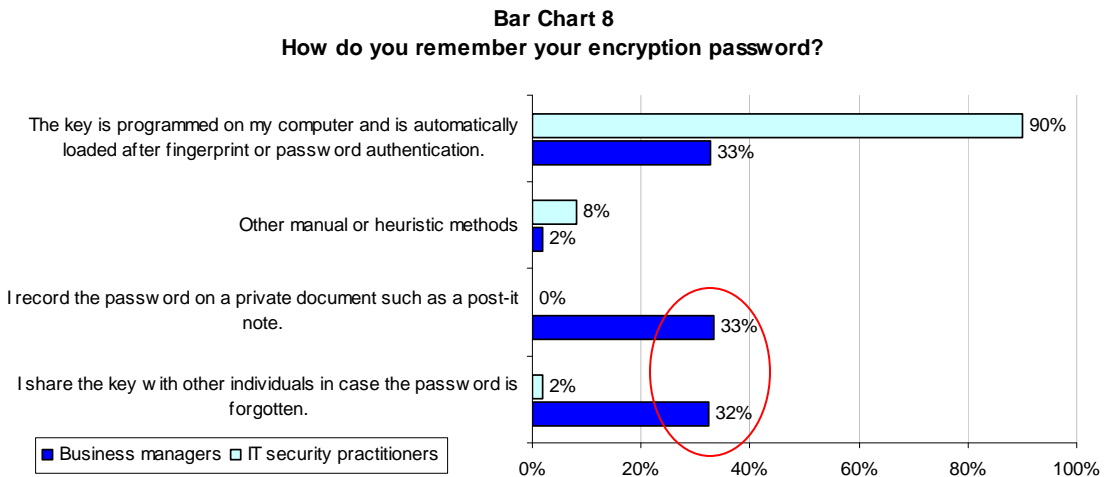
insecure wireless network. In contrast, only 35% of IT security practitioners are confident that there would be zero or less than a 10% chance of losing data when accessing an insecure wireless network.

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

As shown in Bar Chart 7, 47% of business managers in our study admit to forgetting their laptop's encryption password. While 52% were able to recover their password or key used to protect the data by contacting their organizations' help desk, 45% could not gain access and information was lost permanently.

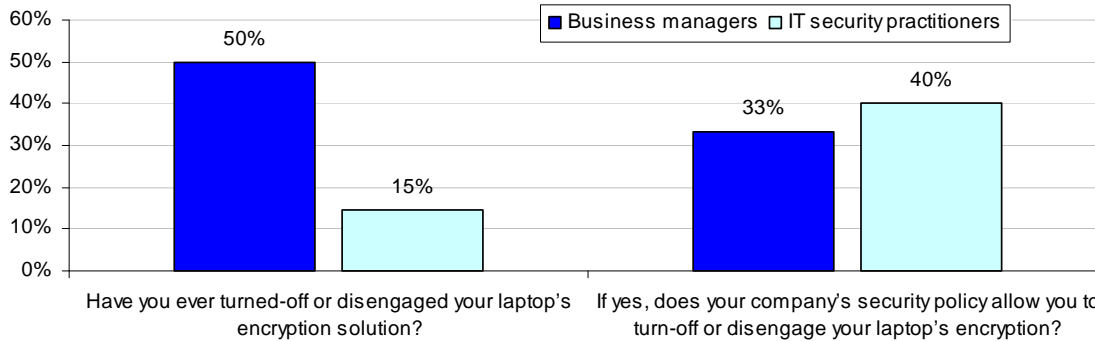


To manage their passwords, business managers circumvent security procedures. As shown in Bar Chart 8, 65% record their password on a private document such as a post-it note to jog their memory or share the key with other individuals in case they forget the password. Virtually none of the IT security practitioners record their password on a private document or share it with another person.



Bar Chart 9 shows that 50% of business managers have disengaged their laptop's encryption solution. Thirty three percent of those who turned off the encryption solution report that this practice is in violation of their company's security policy and 27% are unsure. In contrast, only 15% of IT security practitioners have disengaged the encryption solution and 40% report that it is not in violation of their company's security policy.

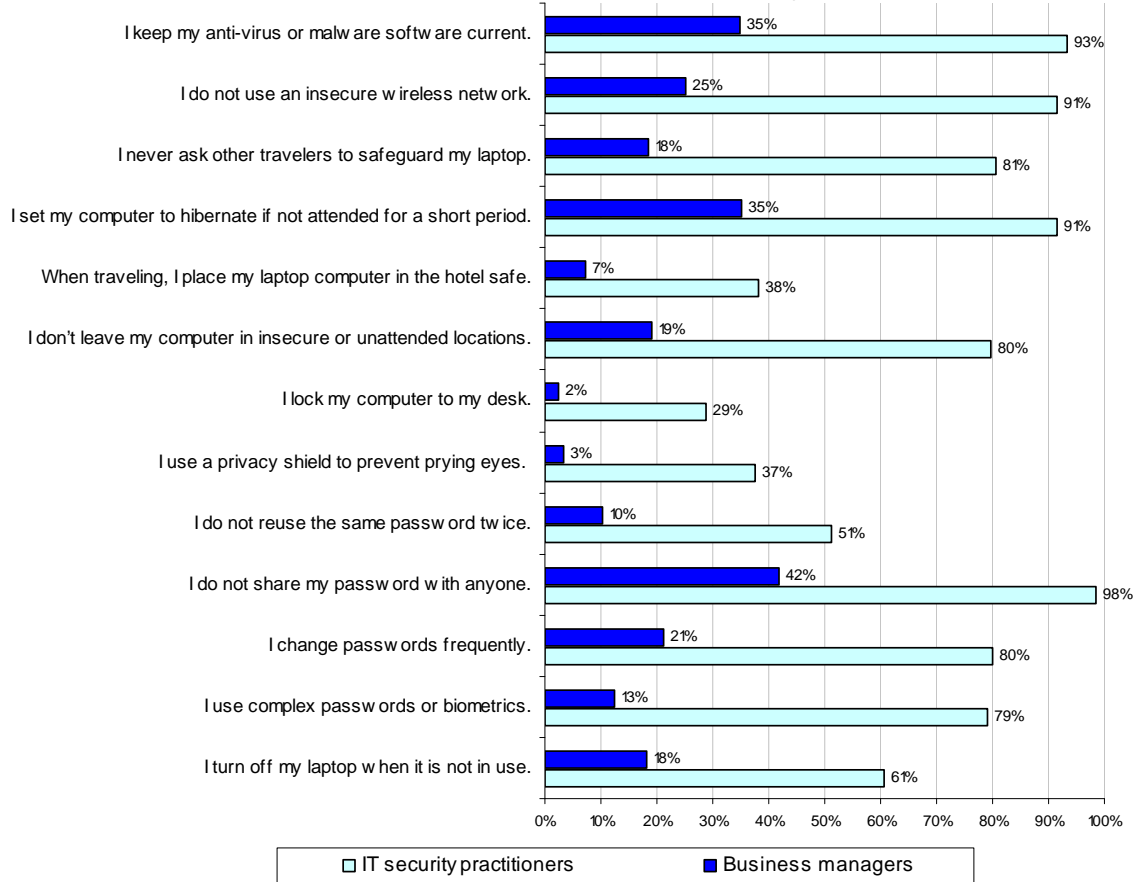
Bar Chart 9
Have you ever disengaged your laptop's encryption solution?
 Each bar shows the percentage Yes response



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.

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



As is shown above, 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, 13% of business managers always use complex passwords or biometrics to prevent unauthorized access to their laptop, 21% always change passwords frequently, 42% never share their passwords, 10% never reuse the same passwords, 3% always use a privacy shield to prevent prying eyes, 2% always physically lock their computer to their desk. Only 35% always keep their anti-virus or malware software current and 35% always set their computer to hibernate if not attended in a very short period of time.

When traveling, 19% never leave their computer in an insecure or unattended location, 7% always place their laptop in the hotel safe, 18% never leave their laptop with a stranger, and 25% never use an insecure wireless network. It is uncertain whether business managers' negligence is due to an over-reliance on encryption solutions. Based on their responses, many in this group believe that encryption is all that is needed to protect the information on their laptops.

In contrast, according to responses from IT security practitioners, 61% always turn off their computers when not in use, 79% always use complex passwords or biometrics to prevent unauthorized access to their laptop, 80% always change passwords frequently, 98% never share their passwords, 51% never reuse the same passwords. However, 37% always use a privacy shield and 29% always physically lock their computer to their desk.

Ninety-three percent keep their anti-virus or malware software current and 91% always set their computer to hibernate if not attended to in a very short period of time. When traveling, 80% never leave their computer in an insecure or unattended location, 38% always place their laptop in the hotel safe, 81% never leave their laptop with a stranger and 91% never use an insecure wireless network.

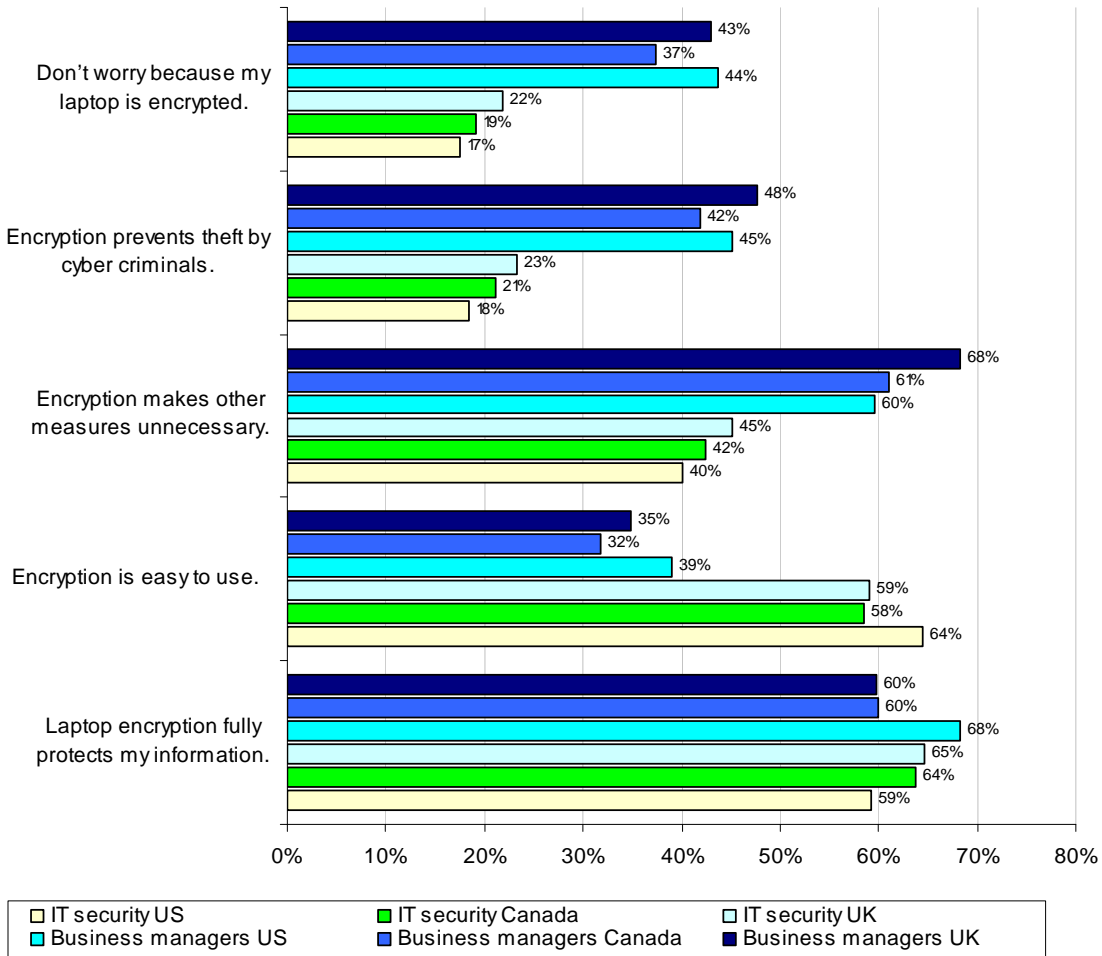
Comparisons of UK, US and Canada

In addition to this UK study, we completed concurrent surveys for IT security practitioners and business managers from organizations in the US and Canada.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 the UK, US, and Canada about various attributions of encryption. In the UK, there are gaps 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.

¹ The US study involved 874 business managers and 720 IT security practitioners. The Canadian study included 348 business managers and 435 IT or IT security practitioners.

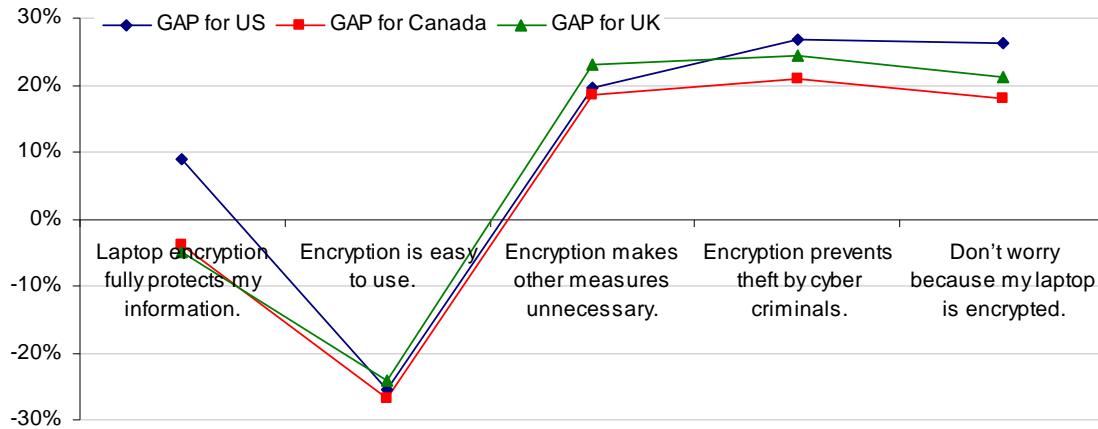
Bar Chart 11
Comparison of laptop encryption attributions for the US, Canada and UK
 Each bar represents the combined percentage of "Strongly Agree" and "Agree" responses



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

Line Chart 1
Difference in the perception of encryption among IT security practitioners and business managers in the US, Canada and UK, respectively
 GAP = the average percent response for business managers minus response for IT security



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 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 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 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 within the United Kingdom 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	9,963	8,302
Bounce-back	2,001	1,240
Total returns	680	531
Rejected surveys	35	32
Final sample	645	499
Response rate	6.5%	6.0%

Table 1 shows 645 respondents in IT security and 499 in 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 6.5% net response rate for IT security and 6.0% net response rate for business managers. The margin of error on all adjective scale and Yes/No/Unsure responses is ≤ 4 percent.

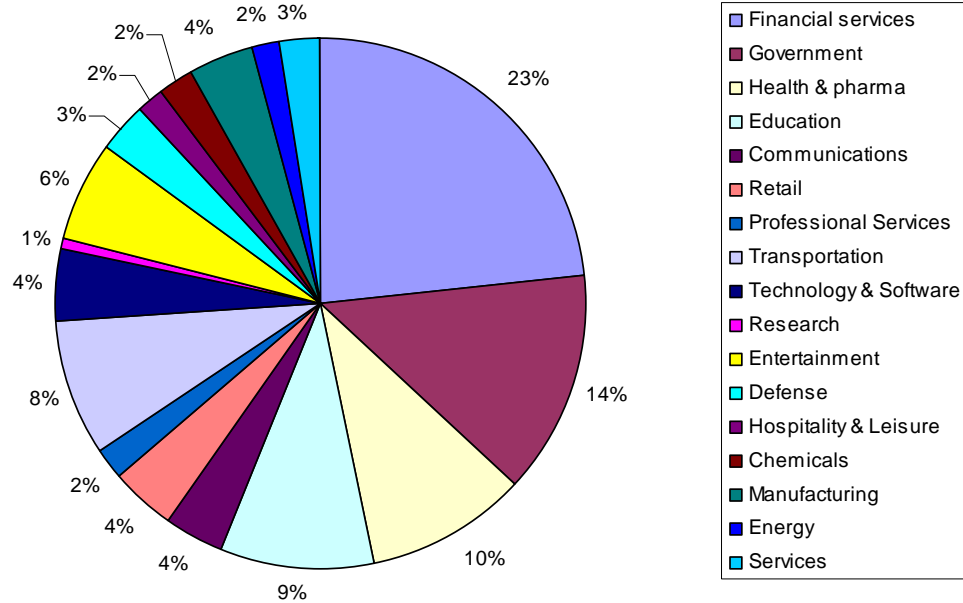
The mean experience level for both the IT security and the business samples is 11 years. Over 95% of respondents completed all survey items within 15 minutes. Following are key demographics and organizational characteristics for U.K. respondents. Table 2 reports the organizational level of respondents 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	1%	1%
Vice President	2%	3%
Director	21%	18%
Manager/Supervisor	43%	54%
Associate/Staff/Technician	28%	25%
Other	5%	-1%
Total	100%	100%

Pie Chart 1 reports the average distribution of respondents in both samples by their organization's primary industry classification. As shown, 23% of respondents are employed by financial service companies (including insurance, banking, credit cards, brokerage and investment management), and 14% work for national or local governments.

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

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



In total, 60% of respondents were males and 40% 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 Europe.

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, 64% of the IT security sample and 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	6%	5%
1,001 to 5,000 people	29%	30%
5,001 to 25,000 people	32%	35%
25,001 to 75,000 people	23%	20%
More than 75,000 people	9%	9%
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 645 practitioners in IT security and 499 in non-IT business functions. By design, at the time of this survey, all respondents were employed by organisations located in the United Kingdom.

Part I. Background & screening		
	IT Security Practitioners	Non-IT Business Managers
Q1. Does your job require you to use a laptop computer?		
Yes	78%	93%
No (stop)	22%	7%
Total	100%	100%

	IT Security Practitioners	Non-IT Business Managers
Q2a. Does your organisation provide encryption tools to help protect information contained on your laptop computer?		
No (go to Q2b)	40%	43%
Yes (go to Q2c)	57%	49%
Unsure (stop)	3%	8%
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	14%	10%
I can't remember the encryption password	1%	3%
Encryption slows down my computer's performance	17%	25%
Encryption causes my operating system to crash	20%	18%
Encryption is not necessary because of other controls such as biometrics or system passwords	25%	29%
Encryption is too expensive for my company	23%	9%
Don't know why	1%	5%
Other (please specify)	1%	2%
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	22%	28%
Email encryption	14%	17%
File-based encryption	16%	23%
Network or gateway encryption	38%	35%
Encryption chip (hardware)	1%	0%
Encrypted thumb drive	3%	7%
Encrypted backup device including thumb drive	8%	12%
Other (please specify)	2%	1%
Total	104%	123%

Part II. Your experiences using encryption		
Q3a. Has anyone in your organisation ever had a laptop used for business purposes lost or stolen?	IT Security Practitioners	Non-IT Business Managers
Yes	86%	50%
No	14%	50%
Total	100%	100%

Q3b. If yes, did this result in a data breach for your organisation?	IT Security Practitioners	Non-IT Business Managers
Yes	56%	26%
No	30%	36%
Unsure	14%	38%
Total	100%	100%

Q3c. If yes, was your organisation able to prove that the contents of the laptop were encrypted?	IT Security Practitioners	Non-IT Business Managers
Yes	45%	18%
No	42%	53%
Unsure	13%	30%
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%	28%
Agree	35%	32%
Unsure	24%	26%
Disagree	10%	14%
Strongly disagree	2%	0%
Total	100%	100%

Q5. My laptop's encryption solution is easy to use.	IT Security Practitioners	Non-IT Business Managers
Strongly agree	20%	11%
Agree	39%	24%
Unsure	17%	20%
Disagree	18%	38%
Strongly disagree	6%	7%
Total	100%	100%

	IT Security Practitioners	Non-IT Business Managers
Q6. Encryption makes it unnecessary to use other security measures.		
Strongly agree	23%	48%
Agree	22%	21%
Unsure	32%	29%
Disagree	15%	1%
Strongly disagree	8%	1%
Total	100%	100%

	IT Security Practitioners	Non-IT Business Managers
Q7. Encryption of my laptop prevents the theft of my information by cyber criminals.		
Strongly agree	22%	43%
Agree	25%	16%
Unsure	36%	35%
Disagree	17%	6%
Strongly disagree	0%	0%
Total	100%	100%

	IT Security Practitioners	Non-IT Business Managers
Q8. I don't worry about losing my laptop because its contents are encrypted.		
Strongly agree	11%	35%
Agree	24%	30%
Unsure	10%	16%
Disagree	36%	16%
Strongly disagree	18%	2%
Total	100%	100%

	IT Security Practitioners	Non-IT Business Managers
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?		
No additional time required	5%	5%
Less than 30 seconds	33%	36%
Between 31 to 60 seconds	32%	28%
Between 1 to 2 minutes	22%	18%
Between 2 to 3 minutes	5%	5%
More than 3 minutes.	2%	8%
Total	100%	100%

	IT Security Practitioners	Non-IT Business Managers
Q10a. Have you ever turned-off or disengaged your laptop's encryption solution?		
Yes	15%	50%
No	85%	50%
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	40%	33%
No	59%	40%
Unsure	0%	27%
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)	18%	41%
Less than 10%	28%	28%
Between 11 and 20%	16%	15%
Between 21% and 30%	21%	11%
Between 31% and 40%	9%	2%
Between 41% and 50%	3%	3%
More than 50%	5%	0%
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%	43%
Less than 10%	21%	31%
Between 11 and 20%	35%	15%
Between 21% and 30%	17%	11%
Between 31% and 40%	10%	0%
Between 41% and 50%	2%	0%
More than 50%	1%	0%
Total	100%	100%

Q12a. Did you ever forget your laptop computer's encryption password?	IT Security Practitioners	Non-IT Business Managers
Yes	6%	47%
No	94%	53%
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	50%	52%
Information on the laptop could not be accessed and was lost permanently.	50%	45%
Other (please specify)	0%	4%
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.	90%	33%
I record the password on a private document such as a post-it note.	0%	33%
I share the key with other individuals in case the password is forgotten.	2%	32%
Other (please specify)	8%	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	61%	18%
Sometimes do this	38%	33%
Rarely do this	2%	35%
Never do this	0%	14%
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	79%	13%
Sometimes do this	21%	24%
Rarely do this	0%	44%
Never do this	0%	19%
Total	100%	100%

	IT Security Practitioners	Non-IT Business Managers
Q16. I change passwords frequently (90 days or less).		
Always do this	80%	21%
Sometimes do this	20%	21%
Rarely do this	0%	42%
Never do this	0%	16%
Total	100%	100%

	IT Security Practitioners	Non-IT Business Managers
Q17. I do not share my password with anyone else.		
I never share	98%	42%
I rarely share	2%	31%
I sometimes share	0%	28%
I frequently share	0%	0%
Total	100%	100%

	IT Security Practitioners	Non-IT Business Managers
Q18. I do not reuse the same password.		
I never reuse the same password	51%	10%
I rarely reuse the same password	38%	21%
I sometimes reuse the same password	10%	33%
I frequently reuse the same password	1%	36%
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	37%	3%
I sometimes use a privacy shield on my computer	5%	6%
I rarely use a privacy shield on my computer	15%	17%
I never use a privacy shield on my computer	43%	74%
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	29%	2%
I sometimes physically lock my computer to my desk	24%	6%
I rarely physically lock my computer to my desk	3%	21%
I never physically lock my computer to my desk	44%	71%
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	80%	19%
I rarely leave my computer alone in an insecure location	11%	30%
I sometimes leave my computer alone in an insecure location	8%	24%
I frequently leave my computer alone in an insecure location	1%	27%
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	38%	7%
Sometimes do this	14%	4%
Rarely do this	3%	20%
Never do this	45%	69%
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	91%	35%
Sometimes do this	6%	36%
Rarely do this	3%	15%
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	81%	18%
I rarely leave my computer alone with a stranger	11%	29%
I sometimes leave my computer alone with a stranger	8%	23%
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	91%	25%
I rarely use an insecure wireless network while traveling	6%	35%
I sometimes use an insecure wireless network while traveling	1%	25%
I frequently use an insecure wireless network while traveling	1%	14%
Total	100%	100%

Q26. I keep my anti-virus or malware software current.	IT Security Practitioners	Non-IT Business Managers
Always do this	93%	35%
Sometimes do this	7%	42%
Rarely do this	0%	12%
Never do this	0%	11%
Total	100%	100%

Part IV. Organisation characteristics and respondent demographics		
What organisational level best describes your current position?	IT Security Practitioners	Non-IT Business Managers
Senior Executive	1%	1%
Vice President	2%	3%
Director	21%	18%
Manager/Supervisor	43%	54%
Associate/Staff/Technician	28%	25%
Other (please describe)	5%	-1%
Total	100%	100%

Check the Primary Person you or your supervisor reports to within your organisation.	IT Security Practitioners	Non-IT Business Managers
CEO/Executive Committee	0%	10%
Chief Financial Officer	15%	9%
Chief Information Officer	42%	28%
Compliance Officer	3%	11%
Chief Privacy Officer	0%	9%
Director of Internal Audit	1%	7%
General Counsel	0%	1%
Chief Technology Officer	18%	0%
Human Resources VP	0%	11%
Chief Security Officer	11%	2%
Chief Risk Officer	5%	10%
Other (please describe)	5%	1%
Total	100%	0%
		100%

Check the country or geographic region where your company's primary headquarters is located.	IT Security Practitioners	Non-IT Business Managers
UK London	23%	21%
UK England Midlands	23%	24%
UK England North	29%	28%
UK England South	16%	17%
UK Scotland	6%	5%
UK Wales	3%	4%
UK Northern Ireland	0%	0%
Total	100%	100%

Experience in years	IT Security Practitioners	Non-IT Business Managers
Total years of business experience	10.98	11.03
Total years in IT or data security	10.01	9.06
Total years in current position	4.65	4.42

Educational and career background:	IT Security Practitioners	Non-IT Business Managers
Compliance (auditing, accountant, legal)	5%	27%
IT (systems, software, computer science)	60%	13%
Security (law enforcement, military, intelligence)	22%	24%
Other non-technical field	5%	28%
Other technical field	8%	7%
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	3%	
Between 10 to 50 people	4%	
Between 50 to 100 people	11%	
Between 100 to 500 people	20%	
Between 500 to 1,000 people	28%	
Between 1,000 to 2,000 people	28%	
Over 2,000 people	6%	
Total	100%	
What industry best describes your organisation's industry concentration or focus?	IT Security Practitioners	Non-IT Business Managers
Airlines	2%	4%
Automotive	3%	6%
Agriculture	0%	0%
Brokerage	5%	2%
Cable	0%	0%
Chemicals	2%	3%
Credit Cards	2%	1%
Defense	5%	2%
Education	10%	9%
Entertainment	5%	7%
Services	3%	2%
Health Care	8%	8%
Hospitality & Leisure	1%	2%
Manufacturing	4%	4%
Insurance	7%	9%
Internet & ISPs	1%	1%
Government	16%	11%
Pharmaceutical	2%	2%
Professional Services	2%	2%
Research	1%	1%
Retail	4%	4%
Banking	10%	10%
Energy	1%	2%
Telecommunications	3%	2%
Technology & Software	5%	4%
Transportation	1%	2%
Wireless	0%	0%
Total	100%	100%

What best describes your role in managing privacy and data protection risks within your organisation? Check all that apply.	IT Security Practitioners	Non-IT Business Managers
Setting priorities	53%	52%
Managing budgets	56%	55%
Selecting vendors and contractors	54%	46%
Determining privacy and data protection strategy	47%	41%
Evaluating program performance	57%	57%
Total	268%	252%

What is the worldwide headcount of your organisation?	IT Security Practitioners	Non-IT Business Managers
Less than 500 people	1%	1%
500 to 1,000 people	6%	5%
1,001 to 5,000 people	29%	30%
5,001 to 25,000 people	32%	35%
25,001 to 75,000 people	23%	20%
More than 75,000 people	9%	9%
Total	100%	100%