Ponemon INSTITUTE

The Cyber Readiness of Canadian Organizations

Sponsored by Scalar

Independently conducted by Ponemon Institute LLC

Publication Date: December 2014

The Cyber Readiness of Canadian Organizations

Ponemon Institute, December 2014

Part 1. Introduction

Would a cyber attack make it impossible for Canadian organizations to stay in business? Which organizations are most prepared to deal with an attack and prevent the loss or theft of sensitive information? Based on the findings of this study, the organizations achieving the greatest cyber readiness are more likely to invest in cutting-edge technologies based on ROI, have a cyber security strategy that is aligned with the organizations' business objectives and mission and proactively recruit skilled IT security professionals.

Sponsored by Scalar and independently conducted by Ponemon Institute, the purpose of this research is to study how Canadian organizations are responding to cyber security threats and the need to invest in enabling security technologies. While we determined that many have a strong security posture, 52 percent of the organizations represented in this research would have difficulty continuing to operate if they experienced a major attack.[1]

We surveyed 623 IT and IT security practitioners in Canada. To ensure a knowledgeable respondent, these participants play a role in directing the IT function, improving IT security in their organizations, setting IT priorities and managing budgets participated in the study.

Cyber crimes are believed by the majority of respondents to be increasing in frequency, sophistication and severity. A major concern for respondents is malware. Seventy-seven percent of respondents say their organizations experienced situations when exploits and malware have evaded their intrusion detection systems (IDS) and/or anti-virus (AV) solutions.

When asked to describe the attacks experienced in the past 12 months, 61 percent say they were APTs and their organizations had an average of 10 in the past 12 months. The most common consequences were IT downtime (56 percent of respondents) and business interruption (49 percent of respondents).

Following are key takeaways from this research:

Respondents believe criminal syndicates and lone wolf hackers are considered most likely to launch an attack against their organizations. On average, organizations in this study have had 34 cyber attacks in the past 12 months—almost one attack per week. Forty-six percent of respondents say these attacks have resulted in the loss or exposure of sensitive information.

Most companies do not think they are winning the cyber security war. Only 41 percent of respondents believe their organizations are winning the cyber security war. The primary reason is a lack of in-house expertise. Other challenges are a lack of collaboration with other functions, insufficient personnel and a lack of clear leadership. Almost half (49 percent) of respondents believe they do not have a sufficient number of in-house personnel who have such critical qualifications as job experience, professional certifications and specialized training.

The loss of intellectual property can affect an organization's competitiveness and bottom line. Thirty-five percent of respondents say their firm experienced a loss of intellectual property or other commercially sensitive business information due to cyber attacks within the past 12 months. Thirty-two percent of these respondents believe that this theft caused a loss of competitive advantage. However, 38 percent were not able to determine if the loss affected their organizations' competitiveness.

[1]We define a major or material cyber attack as one preventing an organization from fulfilling its mission. Consequences can include disruption of services, leakage of sensitive or confidential information and a significant financial burden to remediate.

Restoring reputation and marketplace image is the most costly consequence of a cyber attack. Organizations represented in this research had approximately 34 cyber incidents in the past 12 months. These cyber security compromises are costly and the average spent on each incident was approximately $208,432 on the following: clean up or remediation ($19,883), lost user productivity ($29,035), disruption to normal operations ($38,310), damage or theft of IT assets and infrastructure ($45,117) and damage to reputation and marketplace image ($76,087).

Are organizations spending enough on security? On average, respondents estimate that about 10 percent of their organizations' IT budget is allocated to investments in IT security. Big data analytics is expected to realize an increase in funding. Security information and event management (SIEM), network traffic surveillance and identity management and authentication will also have more money allocated for their investment.

Certain technologies have a higher ROI. Organizations that measure the ROI of their security technology investments say the best investments are SIEM, network traffic surveillance, identity management and authentication. These are investments that are expected to receive more funding. While only 15 percent of respondents say big data analytics has a good ROI, 47 percent say this technology will have more budget allocated to its purchase

Part 2. Key findings

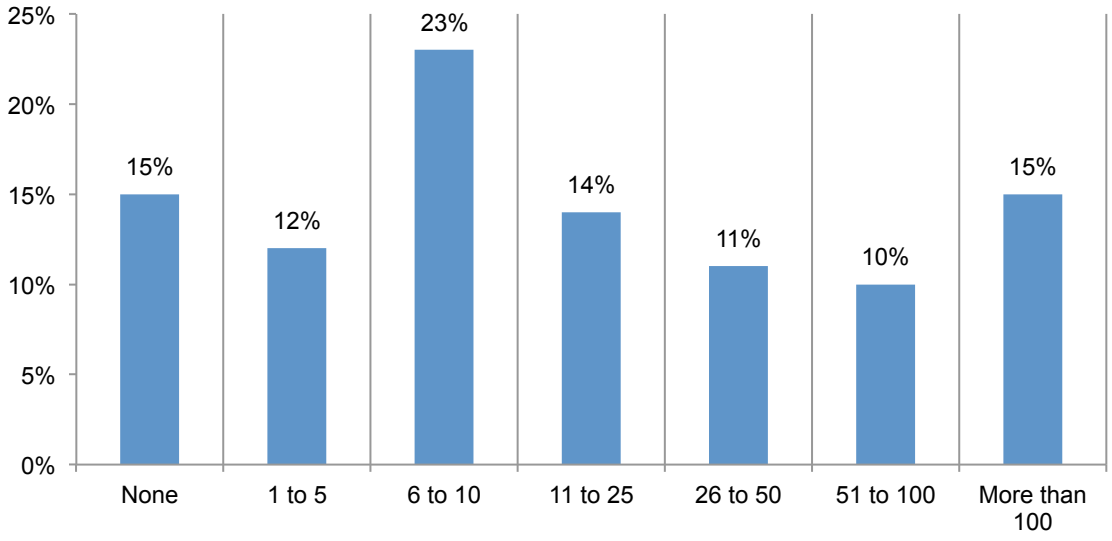
In this section, we analyze the findings of this research. The complete audited findings are presented in the appendix of this report. The report is organized according to the following themes:

- Challenges to winning the cyber security war
- The financial consequences of cyber crime
- Characteristics of a strong cyber security posture

Challenges to winning the cyber security war

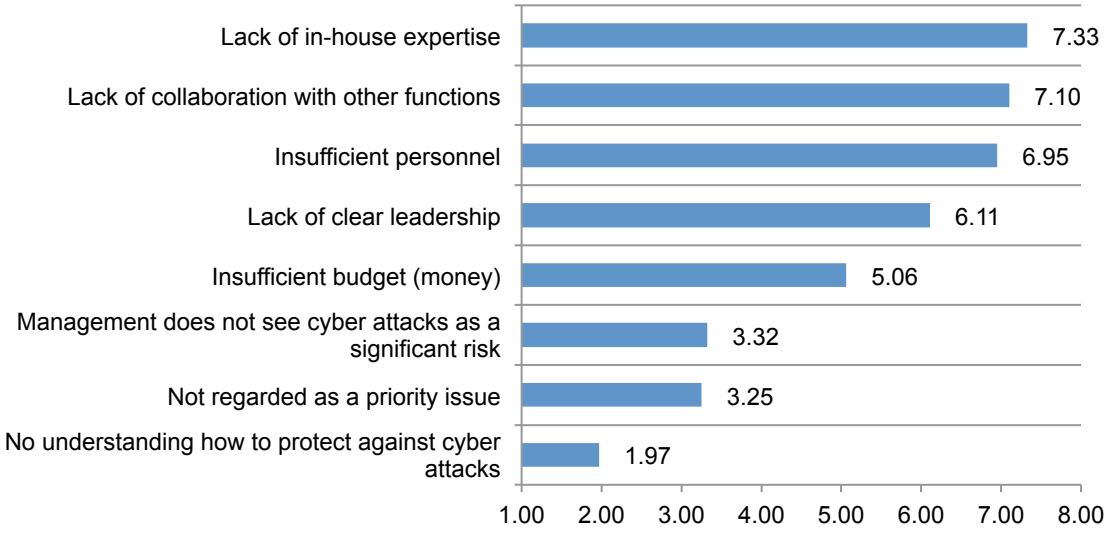
Respondents believe it is very difficult to achieve cyber security readiness. As shown in Figure 1, on average organizations represented in this research experienced 34 cyber attacks in the past 12 months—almost one attack per week. Forty-six percent of respondents say these attacks have resulted in the loss or exposure of sensitive information. Criminal syndicates and lone wolf hackers are considered by respondents to be the most likely source of an attack against their organizations

Figure 1. How many cyber attacks has your organization experienced over the past 12 months?
Extrapolated value = 34.3



Most companies do not think they are winning the cyber security war. Only 41 percent of respondents believe their organizations are winning the cyber security war. The primary reason is a lack of in-house expertise, as shown in Figure 2. Other challenges are a lack of collaboration with other functions, insufficient personnel and a lack of clear leadership. Almost half (49 percent) of respondents believe they do not have a sufficient number of in-house personnel who have such critical qualifications as job experience, professional certifications and specialized training.

Figure 2. Challenges affecting cyber security effectiveness
1 = least challenging to 8 = most challenging



The loss of intellectual property can affect an organization's competitiveness and bottom line. Thirty-five percent of respondents say their firm experienced a loss of intellectual property or other commercially sensitive business information due to cyber attacks within the past 12 months. As shown in Figure 3, 32 percent of these respondents believe that this theft caused a loss of competitive advantage. However, 38 percent were not able to determine if the loss affected their companies' competitiveness.

Figure 3. Do you think the loss of intellectual property has caused your firm to lose a competitive advantage?

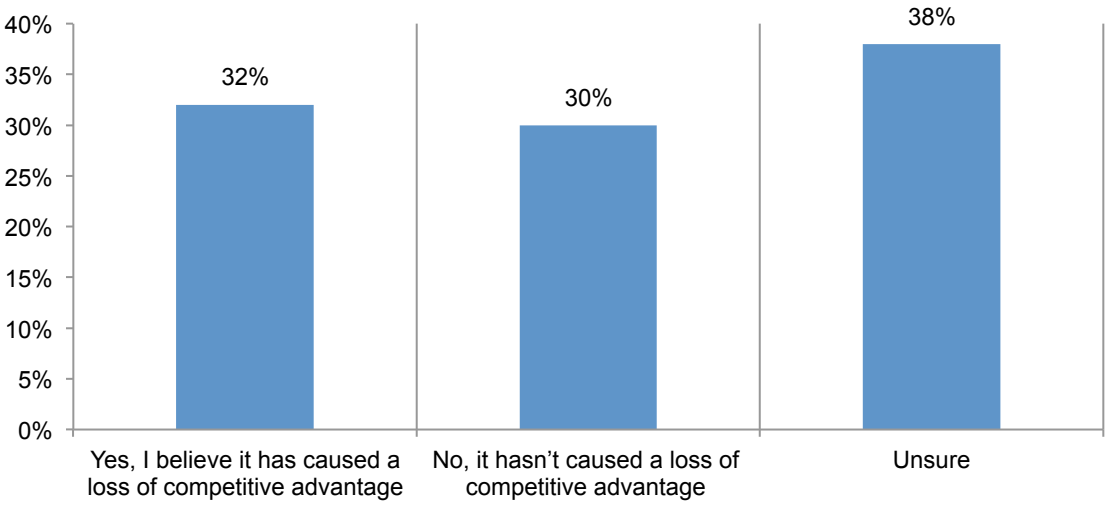
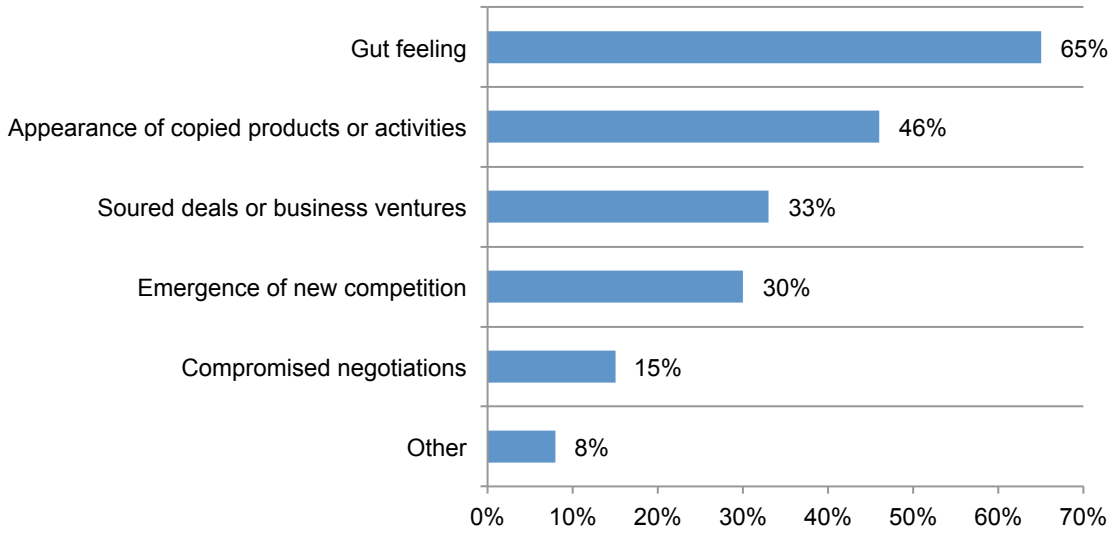


Figure 4 reveals how companies determined the loss of competitive advantage as a result of the loss of their intellectual property following a cyber attack. By far it was based primarily on a gut feeling. Another indication was the appearance of copied products or activities (46 percent). Despite the loss of their intellectual property, almost half (48 percent) of these respondents say the loss of intellectual property has not affected their firm's propensity to make investments in research and development.

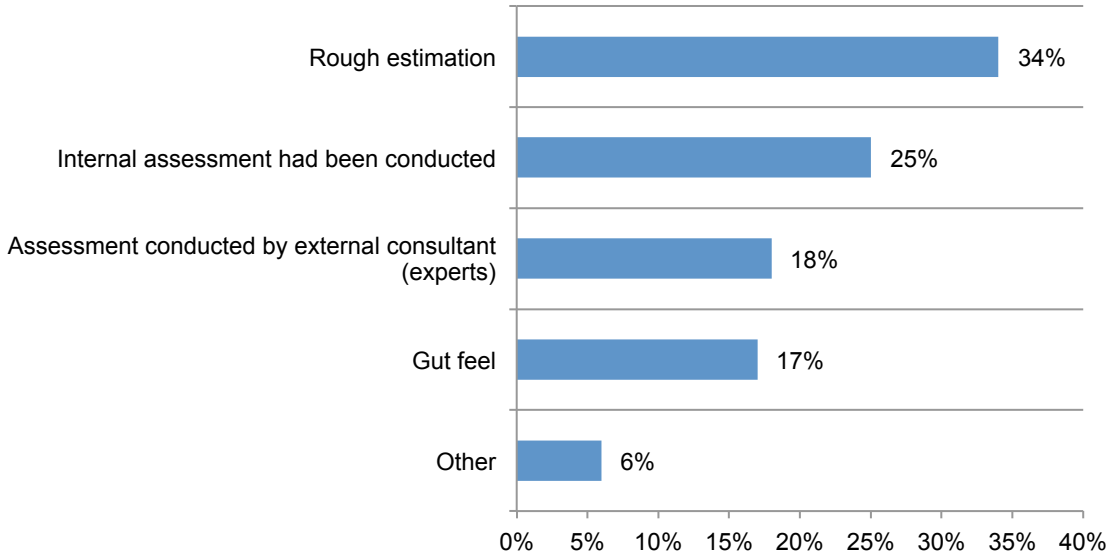
Figure 4. How did the company determine the loss of competitive advantage following a cyber attack?
More than one response permitted



Of those organizations that had their intellectual property stolen in the past 12 months, the average estimated cost to the organization was about $9 million. Examples of such costs are loss of business due to new competition and damage to their brand or marketplace image.

How did the organization determine the financial consequences of the theft? Figure 5 reveals that this estimate was based on a rough estimation (34 percent of respondents), internal assessment (25 percent of respondents), assessment conducted by consultants (18 percent of respondents) and gut feel (17 percent of respondents).

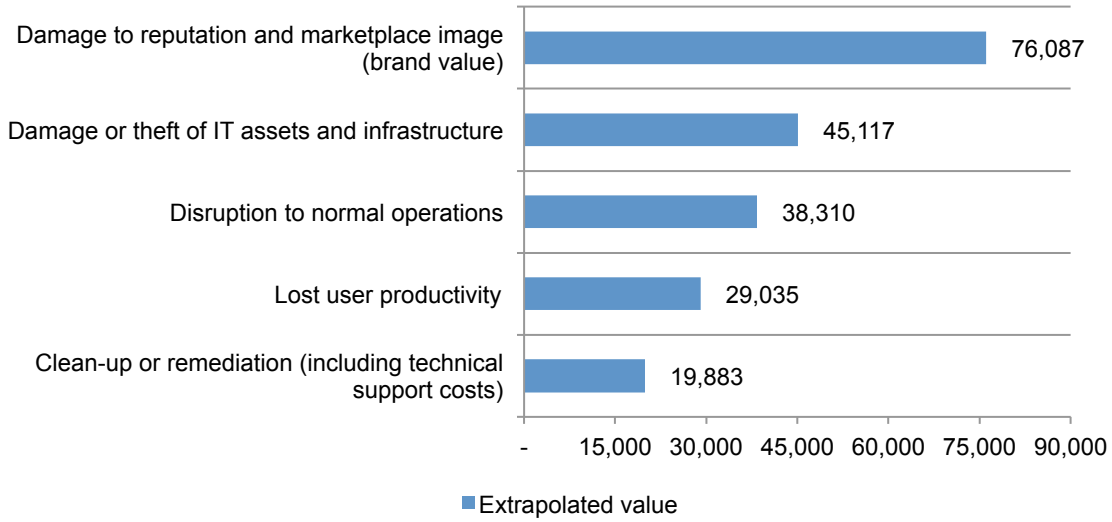
Figure 5. How did the company estimate the cost of stolen intellectual property?



The financial consequences of cyber attacks

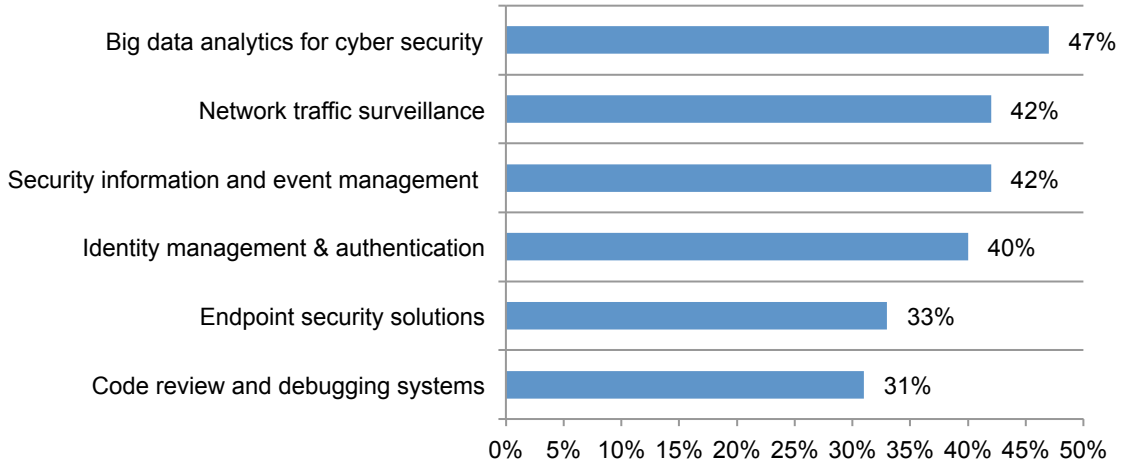
Restoring reputation and marketplace image is the most costly consequence of a cyber attack. Organizations represented in this research had approximately 34 cyber incidents in the past 12 months. These cyber security compromises are costly and the average spent on each incident was approximately $208,432 on the following: clean up or remediation ($19,883), lost user productivity ($29,035), disruption to normal operations ($38,310), damage or theft of IT assets and infrastructure ($45,117) and damage to reputation and marketplace image ($76,087).

Figure 6. What is the average cost of one cyber attack?
Extrapolated value



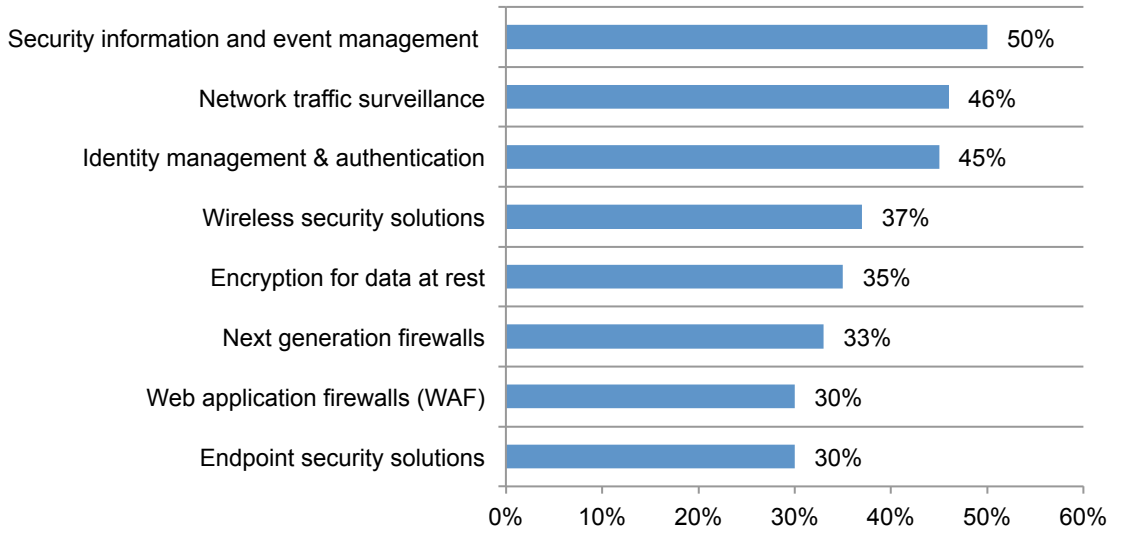
Are organizations spending enough on security? On average, respondents estimate that about 10 percent of their organizations' IT budget is allocated to investments in IT security. Figure 7 shows the technologies expected to receive the most funding. Big data analytics will benefit the most. Security information and event management (SIEM), network traffic surveillance and identity management and authentication will also have more money allocated for their investment.

Figure 7. Technologies that will experience an increase in budget allocation over the next 12 months More than one response permitted



Is it helpful to measure a technology's ROI? The majority of respondents (53 percent) say their organizations do not (46 percent) or are unsure (7 percent) if they measure the ROI of their security technology investments. According to Figure 8, of the 47 percent of respondents who say they do measure ROI believe the best investments are SIEM, network traffic surveillance, identity management and authentication. These are investments that also are expected to receive more funding.

Figure 8. Eight security technologies with the highest ROI
Five choices permitted

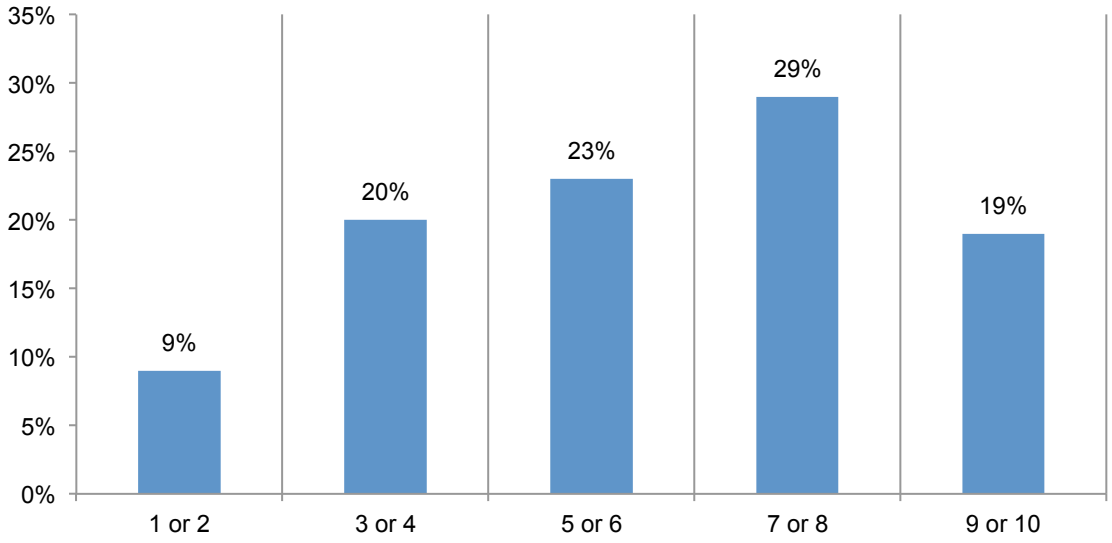


Part 3. Do certain organizations achieve a stronger cyber security posture?

As part of the research, we identified certain organizations represented in this study that self-reported they have achieved a more effective cyber security posture and are better able to mitigate risks, vulnerabilities and attacks.

As shown in Figure 9, high-performing organizations represent 48 percent of the organizations in this study (a self-reported effectiveness rating of higher than 7 on a scale of 1 = not effective to 10 = very effective). Respondents in these high-performing organizations seem to be much more confident in their ability to withstand the consequences of such an attack. As a result, they believe it is much less likely they will have a cyber attack in the next 12 months that will make it difficult to stay in business

Figure 9. How do you rate the effectiveness of your organization's cyber security posture and its ability to mitigate risks, vulnerabilities and attacks across the enterprise?
1= Not effective to 10 = Very effective
Extrapolated value = 6.08

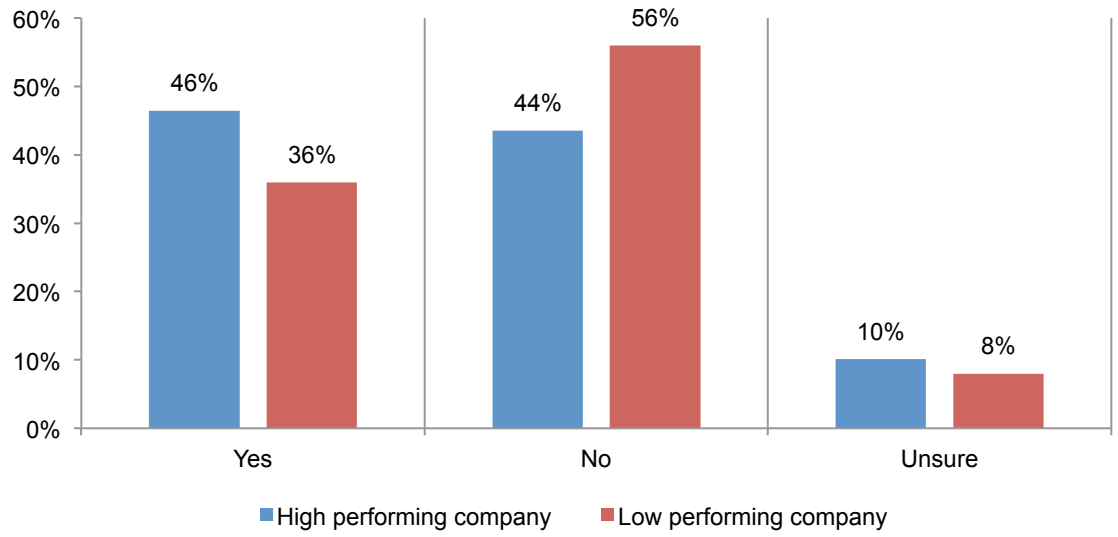


What are the characteristics of a high-performing organization?

In general, high performing organizations have a greater awareness of the cyber security threat landscape, spend more on security and measure the ROI of their technology investments. A possible reason for their ability to have additional funding is the fact that their cyber security strategy is supportive of their organizations' business goals and mission.

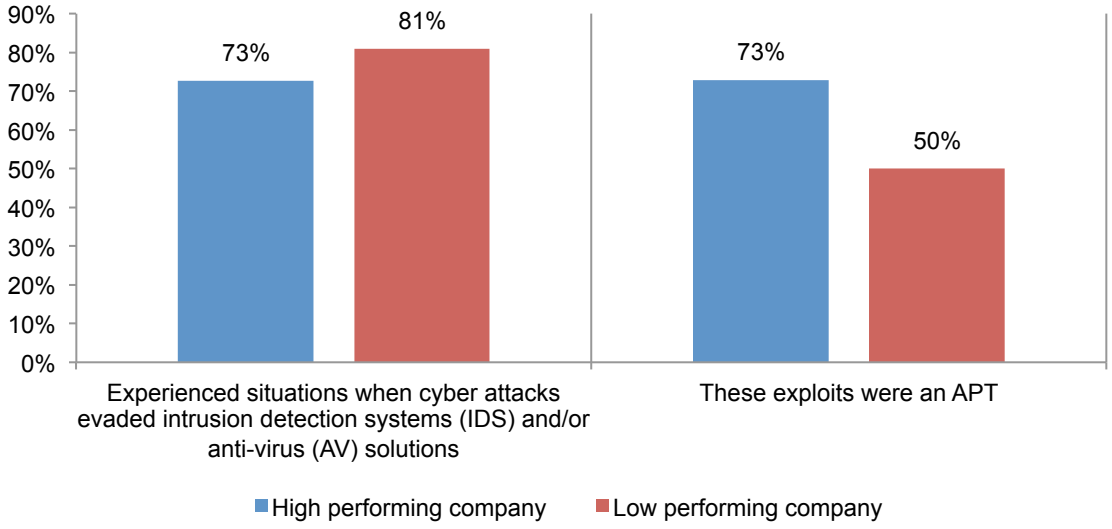
High performing organizations actually report having more cyber attacks (an average of 38 attacks in the past 12 months vs. 31 attacks for low performing organizations). However, as shown in Figure 9, 46 percent of high performing companies say they are winning the cyber security war. In contrast, only 36 percent of respondents say they are winning.

Figure 10. Do you believe your organization is winning the cyber security war?



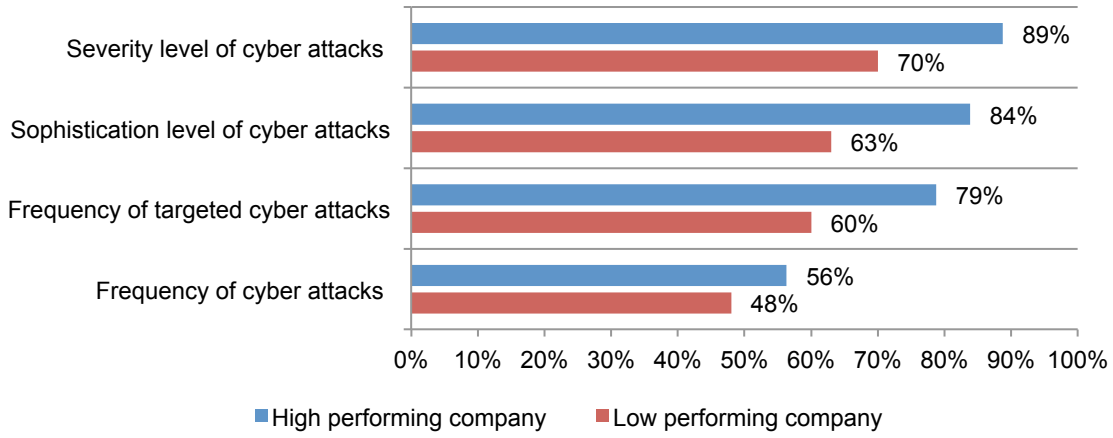
Both high and low performing organizations have experienced situations when cyber attacks have evaded intrusion detection systems (IDS) and/or anti-virus (AV) solutions. However, high performing organizations have had slightly fewer instances (an average of 73 percent vs. an average of 81 percent), as shown in Figure 10. High performing organizations are far more likely to believe these exploits were an APT (an average of 73 percent vs. 50 percent).

Figure 11. Have cyber attacks evaded IDS and AV solutions and were they APTs?
Yes responses only



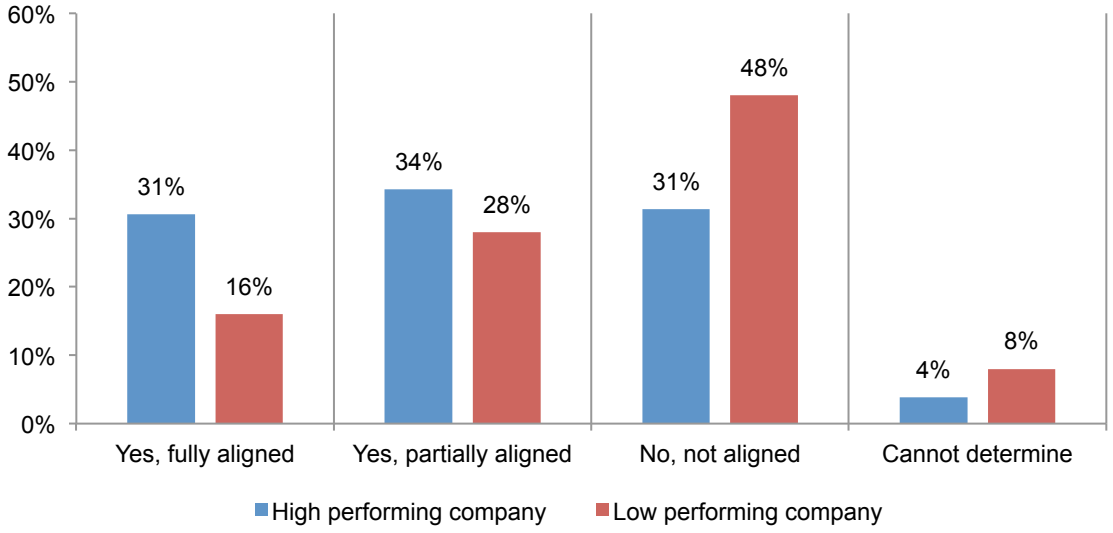
High performing organizations are smarter about the threat landscape. These organizations have a greater awareness of the threats facing their organizations. According to Figure 11, high-performing organizations are more likely to believe the following have increased: frequency of cyber attacks, frequency of targeted cyber attack, sophistication level and severity.

Figure 12. Changes in cyber attacks over the previous 12 months
Increased responses



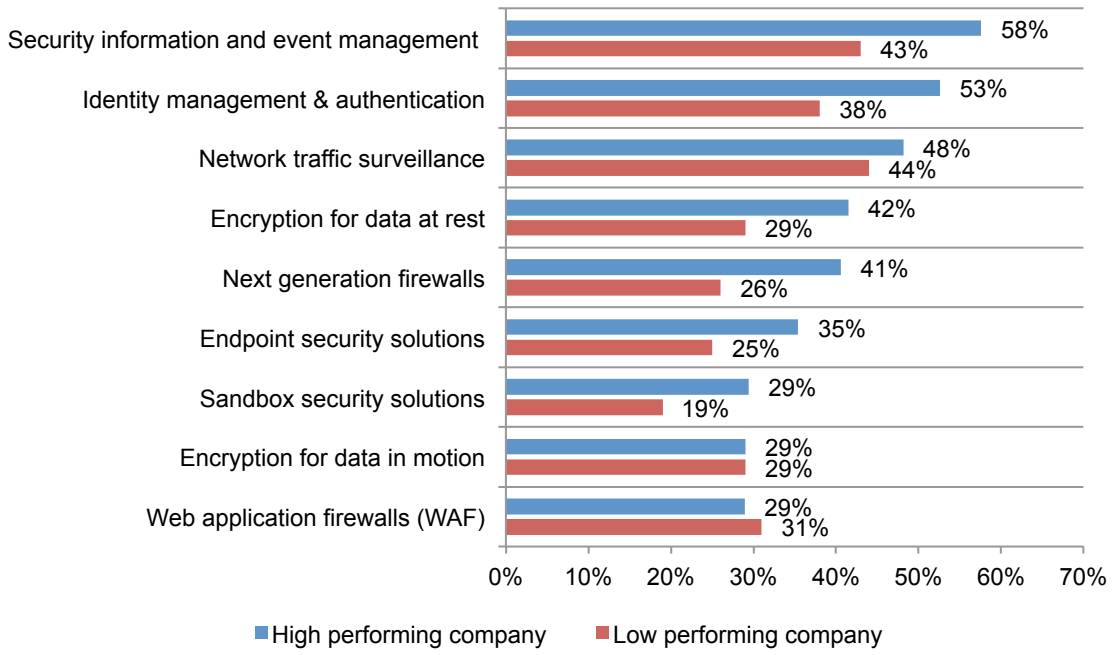
Cyber security strategy supports their organizations' business goals. High-performing organizations are more likely to have their organization's cyber security strategy either fully or partially aligned with its business objectives and mission (an average of 65 percent vs. an average of 44 percent), as shown in Figure 12.

Figure 13. Is your organization's cyber security strategy aligned with its business objectives and mission?



More money is available for investments in technologies. High-performing organizations have a higher portion of the total IT budget dedicated to security (an average of 12 percent of the IT budget vs. 8 percent). Figure 13 shows that ROI is measured more often by high performing organizations and reveals that the best investments for both groups are security information and event management (SIEM), identity management and authentication and network traffic surveillance.

Figure 14. Security technologies that your organization procured with the highest ROI
More than one response permitted



Part 4. Conclusion

The practices of high-performing organizations provide guidance on how organizations can improve their cyber security effectiveness. These include:

- Align the cyber security strategy with the overall mission of the organization.
- Invest in cutting-edge technologies such as SIEM, network intelligence, IDS with reputation feeds, big data analytics, dynamic and static scanning of applications and endpoint security tools (including mobile device management, active sync controls and secure container solutions).
- Proactively recruit experts to help lead the organization's cyber security team.
- Secure adequate resources for investment in practices and technologies determined to be critical to achieving a strong cyber security posture.
- Conduct risk assessment and audits to understand areas where the organization is most vulnerable to an attack.
- Since negligent insiders are considered to pose the greatest risk to the loss and theft of sensitive information, make training and awareness programs a priority. Apply metrics to track the effectiveness of these programs.
- Ensure the necessary in-house expertise exists and have specialized training for IT and IT security practitioners on staff.

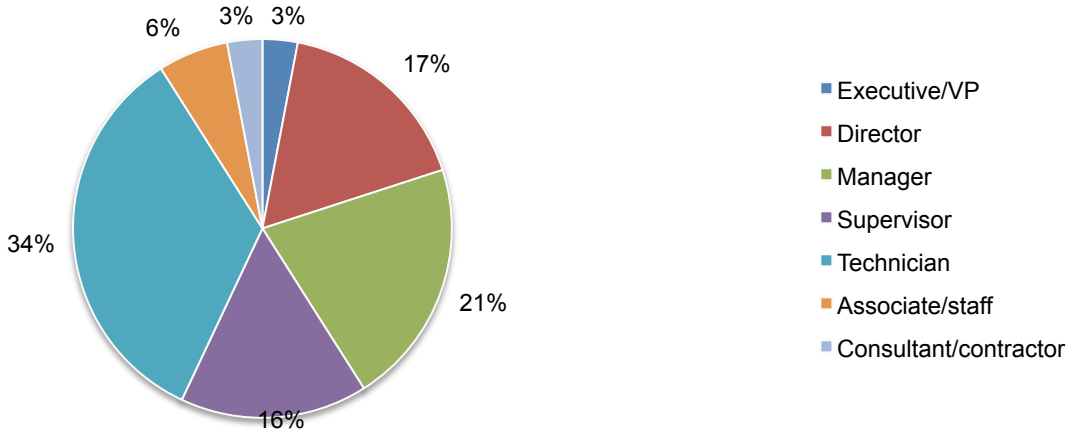
Part 5. Methods

A sampling frame composed of 15,816 IT and IT security practitioners located in Canada were selected for participation in this survey. To ensure a knowledgeable respondent, participants that play a role in directing the IT function, improving IT security in their organizations, setting IT priorities and managing budgets were selected for this study. As shown in the following table, 701 respondents completed the survey. Screening removed 78 surveys. The final sample was 623 surveys (or a 3.9 percent response rate).

Table 1. Sample response	Freq	Pct%
Total sampling frame	15,816	100.0%
Total returns	701	4.4%
Rejected or screened surveys	78	0.5%
Final sample	623	3.9%

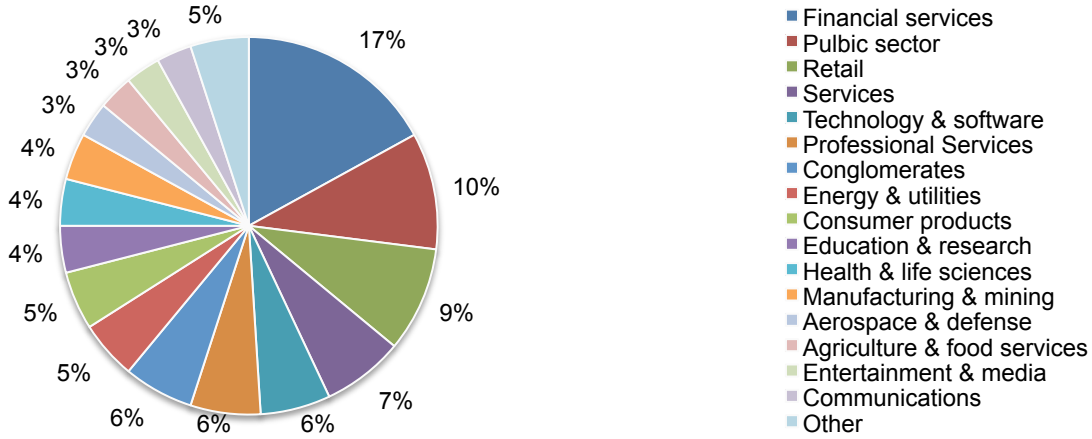
Pie chart 1 reports the current position or organization level of respondents. By design, 57 percent of respondents reported their current position is at or above the supervisory level.

Pie Chart 1. Current position or organizational level



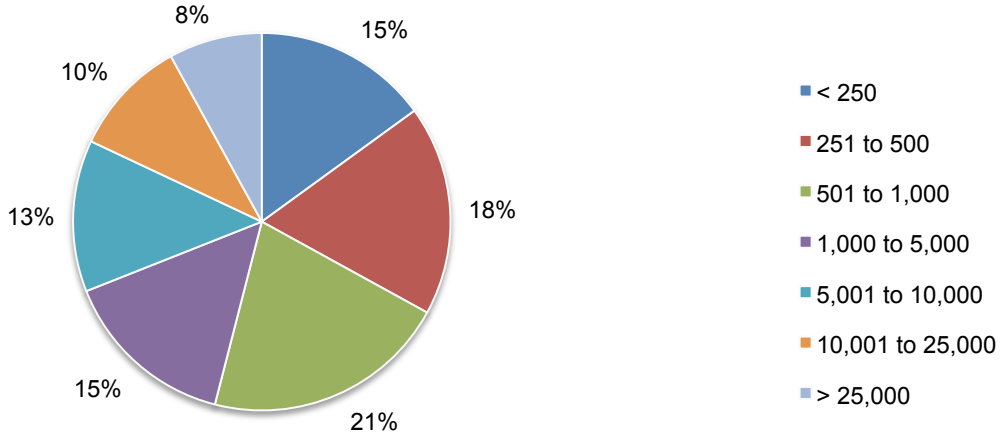
Pie Chart 2 reports the primary industry classification of respondents' organizations. This chart identifies financial services (17 percent) as the largest segment, followed by public sector (10 percent) and retail (9 percent).

Pie Chart 2. Primary industry classification



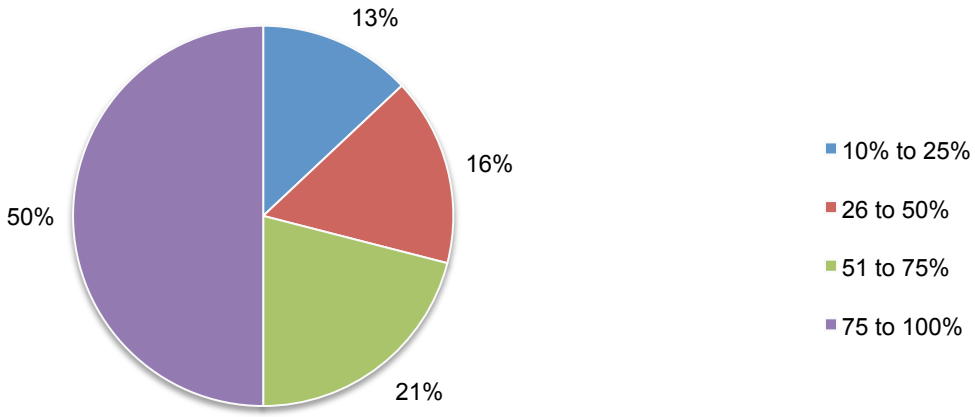
According to Pie Chart 3, almost half (46 percent) of the respondents are from organizations with a global headcount of over 1,000 employees.

Pie Chart 3. Worldwide headcount of the organization



Pie Chart 4 reveals that more 71 percent of respondents indicated that their organization has more than half of their employees located in Canada.

Pie Chart 4. Percentage of employees located in Canada



Part 6. 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 individuals, 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 list is representative of individuals who are IT or IT security practitioners located in various organizations in Canada. We also acknowledge that the results may be biased by external events such as media coverage. We also acknowledge bias caused by compensating subjects to complete this research within a specified time period.

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 accurate responses.

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured in November 2014.

Sample response	Freq
Total sampling frame	15,816
Total returns	701
Rejected or screened surveys	78
Final sample	623
Response rate	3.9%

S1. Which of the following best describes your role in managing the IT function within your organization? Check all that apply.	Pct%
Setting IT priorities	53%
Managing IT budgets	51%
Selecting vendors and contractors	46%
Determining IT strategy	33%
Evaluating programme performance	48%
Bolstering IT security	67%
None of the above [STOP]	0%
Total	298%

Part 1: Your organization's security posture	
Q1. How would you rate your organization's cyber security posture (in terms of its effectiveness at mitigating risks, vulnerabilities and attacks across the enterprise)?	Pct%
1 or 2	9%
3 or 4	20%
5 or 6	23%
7 or 8	29%
9 or 10	19%
Total	100%
Extrapolated value	6.08

Q2a. How does your organization determine the qualifications or expertise of personnel who manage cyber security risk? Please select all that apply.	Pct%
Professional certification	79%
Work histories (on the job experience)	95%
Specialized training	64%
Advanced degrees	39%
Other (please specify)	5%
Total	282%

Q2b. Does your organization have a sufficient number of in-house personnel who possess these qualifications?	Pct%
Yes	46%
No	49%
Unsure	5%
Total	100%

Part 2: Cyber attack experience

Q3. How many cyber attacks has your organization experienced over the past 12 months?	Pct%
None	15%
1 to 5	12%
6 to 10	23%
11 to 25	14%
26 to 50	11%
51 to 100	10%
More than 100	15%
Total	100%
Extrapolated value	34.3

Q4. Has your organization experienced an incident involving the loss or exposure of sensitive information in the past 12 months?	Pct%
Yes	46%
No	48%
Unsure	6%
Total	100%

Q5. Do you believe your organization is winning the cyber security war?	Pct%
Yes	41%
No	50%
Unsure	9%
Total	100%

Q6a. Has your organization ever experienced situations when cyber attacks have evaded intrusion detection systems (IDS) and/or anti-virus (AV) solutions?	Pct%
Yes	77%
No	20%
Unsure	3%
Total	100%

Q6b. Do you consider these any of these exploits an APT?	Pct%
Yes	61%
No	34%
Unsure	5%
Total	100%

Q7. How many separate APT-related incidents did your organization experience over the past 12 months?	Pct%
None (skip to Q9)	19%
1 to 5	26%
6 to 10	29%
11 to 25	18%
26 to 50	6%
51 to 100	2%
More than 100	0%
Total	100%
Extrapolated value	10.0

Q8. What happened to your organization as a result of the APTs it experienced? Please select all that apply.	Pct%
Nothing happened	36%
IT downtime	56%
Business interruption	49%
Exfiltration of confidential or sensitive information	38%
Theft of personal information	42%
Damage to IT infrastructure	10%
Damage to software (source code)	7%
Destruction of information asset	3%
Other (please specify)	2%
Total	243%

Q9. Please rank order the following types of attackers from 1 = most likely to launch to 6 = least likely to launch an attack against your company.	Avg Rank
Nation-state attackers	4.02
Criminal syndicates	2.10
Lone wolf hacker	2.94
Hacktivists	3.44
Cyber-terrorists	5.26
Other corporations (economic espianage)	3.19

Please rate the following statements using one of the three choices provided below each item. Note that the time period for estimating the net change is the previous **12 months** (relative to the prior years).	
Q10a. Within your organization, how has the **frequency of** cyber attacks changed?	Pct%
Increased	52%
Stayed the same	44%
Decreased	4%
Total	100%

Q10b. Within your organization, how has the **frequency of targeted** cyber attacks changed?	Pct%
Increased	69%
Stayed the same	26%
Decreased	5%
Total	100%

Q10c. Within your organization, how has the **sophistication level** of cyber attacks changed?	Pct%
Increased	73%
Stayed the same	23%
Decreased	4%
Total	100%

Q10d. Within your organization, how has the **severity level** of cyber attacks changed?	Pct%
Increased	79%
Stayed the same	21%
Decreased	0%
Total	100%

Q11. Is your organization's cyber security strategy **aligned** with its business objectives and mission?	Pct%
Yes, fully aligned	23%
Yes, partially aligned	31%
No, not aligned	40%
Cannot determine	6%
Total	100%

Q12. What challenges keep your organization's cyber security posture from being fully effective? Please rank the following choices from 1 = most challenging to 8 = least challenging.	Avg Rank
Lack of in-house expertise	1.67
Lack of collaboration with other functions	1.90
Insufficient personnel	2.05
Lack of clear leadership	2.89
Insufficient budget (money)	3.94
Management does not see cyber attacks as a significant risk	5.68
Not regarded as a priority issue	5.75
No understanding how to protect against cyber attacks	7.03

Q13. Using the following 10-point scale, how difficult is it for your organization to achieve a fully effective cyber security posture?	Pct%
1 to 2	0%
3 to 4	7%
5 to 6	14%
7 to 8	24%
9 to 10	55%
Total	100%
Extrapolated value	8.04

Part 3. Cost estimation (over the past 12-month period)

Q14a. Approximately, how much did cyber security compromises cost your organization in terms of clean-up or remediation (including technical support costs)?	Pct%
Zero	0%
Less than $100,000	6%
100,001 to $250,000	44%
250,001 to $500,000	20%
500,001 to $1,000,000	13%
1,000,001 to $5,000,000	3%
5,000,001 to $10,000,000	1%
10,000,001 to $25,000,000	1%
25,000,001 to $50,000,000	0%
More than $50,000,000	0%
Cannot estimate	12%
Total	100%
Extrapolated value	676,023

Q14b. Approximately, how much did cyber security compromises cost your organization in terms of lost user productivity?	Pct%
Zero	0%
Less than $100,000	4%
100,001 to $250,000	20%
250,001 to $500,000	32%
500,001 to $1,000,000	18%
1,000,001 to $5,000,000	12%
5,000,001 to $10,000,000	3%
10,000,001 to $25,000,000	0%
25,000,001 to $50,000,000	0%
More than $50,000,000	0%
Cannot estimate	11%
Total	100%
Extrapolated value	987,191

Q14c. Approximately, how much did cyber security compromises cost your organization in terms of disruption to normal operations?	Pct%
Zero	0%
Less than $100,000	3%
100,001 to $250,000	21%
250,001 to $500,000	39%
500,001 to $1,000,000	15%
1,000,001 to $5,000,000	7%
5,000,001 to $10,000,000	1%
10,000,001 to $25,000,000	0%
25,000,001 to $50,000,000	1%
More than $50,000,000	0%
Cannot estimate	13%
Total	100%
Extrapolated value	1,101,379

Q14d. Approximately, how much did cyber security compromises cost your organization in terms of damage or theft of IT assets and infrastructure?	Pct%
Zero	5%
Less than $100,000	5%
100,001 to $250,000	14%
250,001 to $500,000	37%
500,001 to $1,000,000	11%
1,000,001 to $5,000,000	8%
5,000,001 to $10,000,000	7%
10,000,001 to $25,000,000	2%
25,000,001 to $50,000,000	0%
More than $50,000,000	0%
Cannot estimate	11%
Total	100%
Extrapolated value	1,533,989

Q14e. Approximately, how much did cyber security compromises cost your organization in terms of damage to reputation and marketplace image (brand value)?	Pct%
Zero	4%
Less than $100,000	1%
100,001 to $250,000	11%
250,001 to $500,000	29%
500,001 to $1,000,000	16%
1,000,001 to $5,000,000	10%
5,000,001 to $10,000,000	10%
10,000,001 to $25,000,000	3%
25,000,001 to $50,000,000	1%
More than $50,000,000	0%
Cannot estimate	15%
Total	100%
Extrapolated value	2,586,941

Combined extrapolated value	6,885,523

Q15a. Has your firm experienced a loss of intellectual property or other commercially sensitive business information due to cyber attacks within the past 12 months?	Pct%
Yes	35%
No (Go to Q16)	41%
Unsure (Go to Q16)	24%
Total	100%

Q15b. If yes, do you think the loss of **intellectual property**, has caused your firm to lose a competitive advantage? Or do you think that this isn't really the case (e.g. perhaps rivals can't use information in an effective manner or perhaps information will soon be out of date)?	Pct%
Yes, I believe it has caused a loss of competitive advantage	32%
No, it hasn't caused a loss of competitive advantage	30%
Unsure	38%
Total	100%

Q15c. If yes, how did your firm determine the loss of competitive advantage as a result of the cyber attack?	Pct%
Emergence of new competition	30%
Appearance of copied products or activities	46%
Soured deals or business ventures	33%
Compromised negotiations	15%
Gut feeling	65%
Other (please specify)	8%
Totals	197%

Q15d. If yes, has the loss of intellectual property affected your firm's propensity to make investments in research and development?	Pct%
Yes	31%
No	48%
Unsure	21%
Totals	100%

Q15e. Approximately, how much did losses due to the theft of intellectual property cost your organization over the past 12 months?	Pct%
Zero	0%
Less than $100,000	0%
100,001 to $250,000	0%
250,001 to $500,000	4%
500,001 to $1,000,000	9%
1,000,001 to $5,000,000	27%
5,000,001 to $10,000,000	30%
10,000,001 to $25,000,000	6%
25,000,001 to $50,000,000	2%
More than $50,000,000	2%
Cannot estimate	20%
Total	100%
Extrapolated value	8,775,000

Q15f. Please explain how you arrived at the estimated cost ranges provided in Q15e.	Pct%
Internal assessment had been conducted	25%
Assessment conducted by external consultant (experts)	18%
Rough estimation	34%
Gut feel	17%
Other (please specify)	6%
Total	100%

Part 5. Security spending & investment	
Q16. What percentage of your organization's IT budget is dedicated to security?	Pct%
Less than 5%	38%
5 to 10%	30%
11 to 15%	13%
16 to 20%	7%
21 to 25%	7%
26 to 30%	3%
31 to 35%	2%
More than 35%	0%
Total	100%
Extrapolated value	9.8%

Q17a. Does your organization measure the ROI of investments in security technologies?	Pct%
Yes	47%
No	46%
Unsure	7%
Total	100%

Q17b. If Yes, which of the following security technologies that your organization procured has the highest ROI. Please select no more than **five top choices**.	Pct%
Security information and event management (SIEM)	50%
Network traffic surveillance	46%
Identity management & authentication	45%
Wireless security solutions	37%
Encryption for data at rest	35%
Next generation firewalls	33%
Endpoint security solutions	30%
Web application firewalls (WAF)	30%
Encryption for data in motion	29%
Test data anonymization solution	25%
Sandbox security solutions	24%
Code review and debugging systems	21%
Data loss prevention (DLP)	17%
Data tokenization technology	17%
Virtual private networks (VPN)	16%
Big data analytics for cyber security	15%
Intrusion detection and/or prevention systems	12%
Governance solutions (GRC)	10%
Anti-virus / anti-malware	8%
Total	500%

Q18. Following is a list of leading security technologies. Please choose the technologies that will most likely experience an increase in budget allocation over the next 12 months.	Pct%
Big data analytics for cyber security	47%
Security information and event management (SIEM)	42%
Network traffic surveillance	42%
Identity management & authentication	40%
Endpoint security solutions	33%
Code review and debugging systems	31%
Sandbox security solutions	20%
Encryption for data at rest	28%
Encryption for data in motion	26%
Wireless security solutions	26%
Web application firewalls (WAF)	22%
Next generation firewalls	20%
Data tokenization technology	18%
Data loss prevention (DLP)	15%
Governance solutions (GRC)	12%
Anti-virus / anti-malware	12%
Test data anonymization solution	8%
Intrusion detection and/or prevention systems	6%
Virtual private networks (VPN)	5%
Total	453%

Part 5. Role & Organizational Characteristics	
D1. What best describes your position or organizational level?	Pct%
Executive/VP	3%
Director	17%
Manager	21%
Supervisor	16%
Technician	34%
Associate/staff	6%
Consultant/contractor	3%
Other (please specify)	0%
Total	100%

D2. What best describes your company's primary industry classification?	Pct%
Financial services	17%
Pulbic sector	10%
Retail	9%
Services	7%
Technology & software	6%
Professional Services	6%
Conglomerates	6%
Energy & utilities	5%
Consumer products	5%
Education & research	4%
Health & life sciences	4%
Manufacturing & mining	4%
Aerospace & defense	3%
Agriculture & food services	3%
Entertainment & media	3%
Communications	3%
Industrial	2%
Transportation	2%
Other (please specify)	1%
Total	100%

D3. What is the worldwide headcount of your organization?	Pct%
< 250	15%
251 to 500	18%
501 to 1,000	21%
1,000 to 5,000	15%
5,001 to 10,000	13%
10,001 to 25,000	10%
> 25,000	8%
Total	100%
Extrapolated value	5,830

D4. What percentage of employees are located in Canada?	Pct%
< 10%	0%
10% to 25%	13%
26 to 50%	16%
51 to 75%	21%
75 to 100%	50%
Total	100%
Extrapolated value	65%

D5. What is the worldwide revenue of your organization for the last fiscal year? If you're unsure, please provide a rough estimate.	Pct%
Under $20 million	15%
20 million to $49.9 million	22%
50 million to $299.9 million	22%
300 million to $999.9 million	18%
1 billion to $2.99 billion	11%
3 billion to $6.99 billion	7%
$7 billion and above	5%
Total	100%
Extrapolated value ($billions)	1.08

Analysis of high and low performing companies	Overall	Low	High
Sub-samples	623	324	299
Q1. How would you rate your organization's cyber security posture (in terms of its effectiveness at mitigating risks, vulnerabilities and attacks across the enterprise)?	Pct%	Low	High
1 or 2	9%	9%	
3 or 4	20%	20%	
5 or 6	23%	23%	
7 or 8	29%		29%
9 or 10	19%		19%
Total	100%	52%	48%

Q2b. Does your organization have a sufficient number of in-house personnel who possess these qualifications?	Pct%	Low	High
Yes	46%	40%	53%
No	49%	56%	41%
Unsure	5%	4%	6%
Total	100%	100%	100%

Part 2: Cyber attack experience

Q3. How many cyber attacks has your organization experienced over the past 12 months?	Pct%	Low	High
Extrapolated average	34.30	30.50	38.42

Q4. Has your organization experienced an incident involving the loss or exposure of sensitive information in the past 12 months?	Pct%	Low	High
Yes	46%	53%	38%
No	48%	42%	55%
Unsure	6%	5%	7%
Total	100%	100%	100%

Q5. Do you believe your organization is winning the cyber security war?	Pct%	Low	High
Yes	41%	36%	46%
No	50%	56%	44%
Unsure	9%	8%	10%
Total	100%	100%	100%

Q6a. Has your organization ever experienced situations when cyber attacks have evaded intrusion detection systems (IDS) and/or anti-virus (AV) solutions?	Pct%	Low	High
Yes	77%	81%	73%
No	20%	17%	23%
Unsure	3%	2%	4%
Total	100%	100%	100%

Q6b. Do you consider these any of these exploits an APT?	Pct%	Low	High
Yes	61%	50%	73%
No	34%	44%	23%
Unsure	5%	6%	4%
Total	100%	100%	100%

	Increased	Increased	Increased
Please rate the following statements using one of the three choices provided below each item. Note that the time period for estimating the net change is the previous **12 months** (relative to the prior years).	Overall	Low	High
Q10a. Within your organization, how has the **frequency of** cyber attacks changed?	52%	48%	56%
Q10b. Within your organization, how has the **frequency of targeted** cyber attacks changed?	69%	60%	79%
Q10c. Within your organization, how has the **sophistication level** of cyber attacks changed?	73%	63%	84%
Q10d. Within your organization, how has the **severity level** of cyber attacks changed?	79%	70%	89%

Q11. Is your organization's cyber security strategy **aligned** with its business objectives and mission?	Overall	Low	High
Yes, fully aligned	23%	16%	31%
Yes, partially aligned	31%	28%	34%
No, not aligned	40%	48%	31%
Cannot determine	6%	8%	4%
Total	100%	100%	100%

Security spending as a percent of total IT spending	Overall	Low	High
Q16. What percentage of your organization's IT budget is dedicated to security?	9.8%	8.0%	11.8%

Q17a. Does your organization measure the ROI of investments in security technologies?	Pct%	Low	High
Yes	47%	41%	54%
No	46%	50%	42%
Unsure	7%	9%	5%
Total	100%	100%	100%

Q17b. If Yes, which of the following security technologies that your organization procured has the highest ROI.	Pct%	Low	High
Security information and event management (SIEM)	50%	43%	58%
Network traffic surveillance	46%	44%	48%
Identity management & authentication	45%	38%	53%
Encryption for data at rest	35%	29%	42%
Next generation firewalls	33%	26%	41%
Endpoint security solutions	30%	25%	35%
Web application firewalls (WAF)	30%	31%	29%
Encryption for data in motion	29%	29%	29%
Sandbox security solutions	24%	19%	29%

Organizational size	Pct%	Low	High
Headcount	5,830	5,657	6,017
Revenues ($billions)	$1.08	$0.99	$1.18

Ponemon Institute
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.