The Cyber Security Readiness of Canadian Organizations

RESULTS OF THE 2016
SCALAR SECURITY STUDY

scalar

Contents

scalar | Ponemon INSTITUTE

PART ONE

INTRODUCTION

PART ONE
INTRODUCTION

The second annual Scalar Security Study examines the cyber security readiness of Canadian organizations and the trends in dealing with growing cyber threats. Specifically, we wanted to know:

- Do organizations feel more or less prepared to deal with attacks than last year?
- How have cyber attacks targeting Canadian organizations changed in the past year?
- What is the average cost of cyber attacks for Canadian organizations?
- What cyber security strategies, tactics, and technologies are most effective?

We surveyed 654 IT and IT security practitioners in Canada. The research was independently conducted by Ponemon Institute. To ensure a knowledgeable respondent, only those who play a role in directing the IT function, improving IT security in their organizations, setting IT priorities, and managing budgets participated in the study. Respondents came from a wide variety of industries, and almost two thirds work at organizations with between 251 and 5,000 employees in Canada (see Part 4: Methods for a detailed breakdown).

KEY FINDINGS OF OUR RESEARCH INCLUDE:

Respondents reported an average of 40 cyber attacks per year, which is a 17 percent increase from last year's figure of 34 attacks. With this in mind, it is not surprising that **over half (51 percent) of this year's respondents experienced an incident involving the loss or exposure of sensitive information** within the last twelve months. This is also an increase from our last study, when 46 percent of respondents had experienced such an incident.

The vast majority of respondents believe that cyber crimes are increasing in frequency, sophistication, and severity, which was also the case last year. It also appears that respondents are becoming more discouraged in their efforts to fight cyber crime. **Only 37 percent of respondents believe they are winning the cyber security war**, compared with 41 percent last year. Insufficient personnel and lack of in-house expertise are the primary challenges to achieving a strong cyber security posture and these were significant challenges identified in last year's study as well.

Seventy percent of respondents say their organizations experienced situations when exploits and malware have evaded their intrusion detection systems (IDS), and 82 percent of respondents say their organizations experienced situations when cyber attacks have evaded their anti-virus (AV) solutions.

Only 38 percent of respondents say their organizations have systems and controls in place to deal with advanced persistent threats (APTs), and **organizations have an average of almost one separate APT-related incident per month**. IT downtime, business disruption, and theft of personal information are the primary consequences of APTs or zero day threats experienced. On average, respondents say 25 percent of employees were targeted by phishing attacks.

In the past 12 months, **companies represented in this research experienced an average of 5 denial of service (DoS) attacks or about one every two months**. Further, 44 percent of respondents say their organization experienced a DoS attack that caused a disruption to business operations and/or system downtime. The cost of business disruptions and system downtimes averaged $1.2 million.

The greatest threats to organizations are web-borne attacks. Eighty percent of respondents say the most frequent compromises are web-borne malware attacks, followed by rootkits at 65 percent of respondents.

Mobile devices and applications are seen as the greatest IT security risk. Mobile devices, third party applications, and negligent third party risk are the top three concerns for 72 percent, 68 percent, and 45 percent of respondents, respectively. These risks all have in common the human factor, which requires both technology and governance to reduce the threat.

Cyber security compromises are costly, and intellectual property is a target. Thirty-three percent of respondents say their firm experienced a loss of intellectual property due to cyber attacks within the past 24 months, with 36 percent of them believing it caused a loss of competitive advantage. The average cost of the loss of this information was just under $6 million.

However, theft of intellectual property is not the only cost from a cyber attack. On average, over the last 12 months, **organizations spent approximately $7 million** each on the following: clean up or remediation ($766,667), lost user productivity ($950,625), disruption to normal operations ($1.1 million), damage or theft of IT assets and infrastructure ($1.6 million), and damage to reputation and marketplace image ($2.6 million). With organizations reporting an average of 40 attacks per year, this makes the average cost per attack approximately $175,000.

Cyber security spend has increased slightly. On average, respondents estimate their approximate annual budget for IT is $71 million and an average of 11 percent of this budget is dedicated to information security. This increased slightly from about 10 percent last year.

The majority of respondents believe **gathering and using threat intelligence is key to winning the cyber security war**. Sixty percent of respondents do either fully or partially participate in an initiative or program for exchanging threat intelligence with peers, government, and/or industry groups, believing it improves the security posture of their organization, in addition to improving situational awareness.

What can organizations do to improve their security posture? Once again we identified certain organizations represented in this study that self-report to have achieved a more effective cyber security posture and are better able to mitigate risks, vulnerabilities, and attacks. We refer to these as "high performing" organizations, and they represent 53 percent of the sample size. When compared with the remaining 47 percent of the sample, the "low performers", we see that high performers spend 43 percent more of their IT budget on information security, and are almost twice as likely to have a cyber security strategy that is fully aligned with their business objectives and mission. Interestingly, high performers actually report more attacks per year than low performers – this may be because they detect more attacks. This theory is further supported by the fact that high performers have a more realistic understanding of the threat landscape, and are more likely to believe attacks are increasing in frequency, sophistication, and severity than low performers. High performers also believe technologies such as network traffic surveillance, security information and event management (SIEM), and identity management and authentication yield the highest ROI.

As a result of these strategies, tactics, and investments, **high performers experienced less situations when cyber attacks evaded their AV or IDS controls, are 28 percent more confident they are winning the cyber security war, and are 19 percent less likely to have experienced an attack that led to the loss or exposure of sensitive information**.

Looking forward, the technologies that are expected to receive the most funding over the next 12 months across all respondents are: network traffic surveillance, SIEM, endpoint security solutions, big data analytics for cyber security, and identity management and authentication. Since high performers appear to be seeing ROI in leveraging some of these technologies, this is an encouraging trend.

Only

37%

of organizations believe they are winning the cyber security war

PART TWO

KEY FINDINGS

Organizations in Canada experience an average of

40

cyber attacks per year

PART TWO
KEY FINDINGS

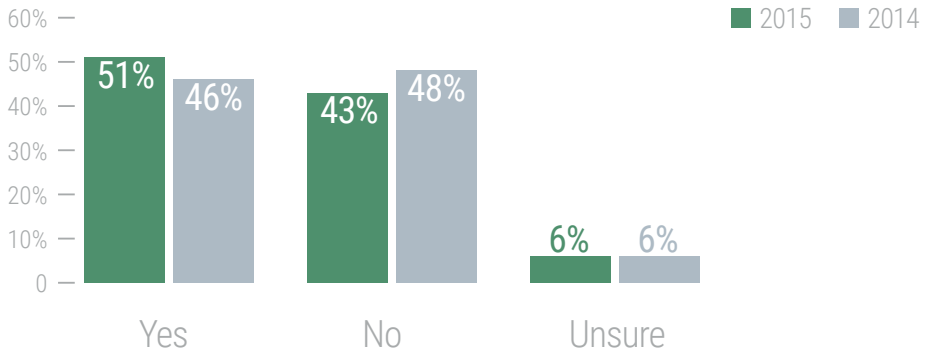
In this section, we analyze the key findings of the research. The complete audited findings are presented in Appendix A of this report. The report is organized according to the following themes:

- The security threat landscape
- The financial aspects of cyber crime and cyber security
- The importance of threat intelligence
- Characteristics of organizations with a strong cyber security posture

THE SECURITY THREAT LANDSCAPE

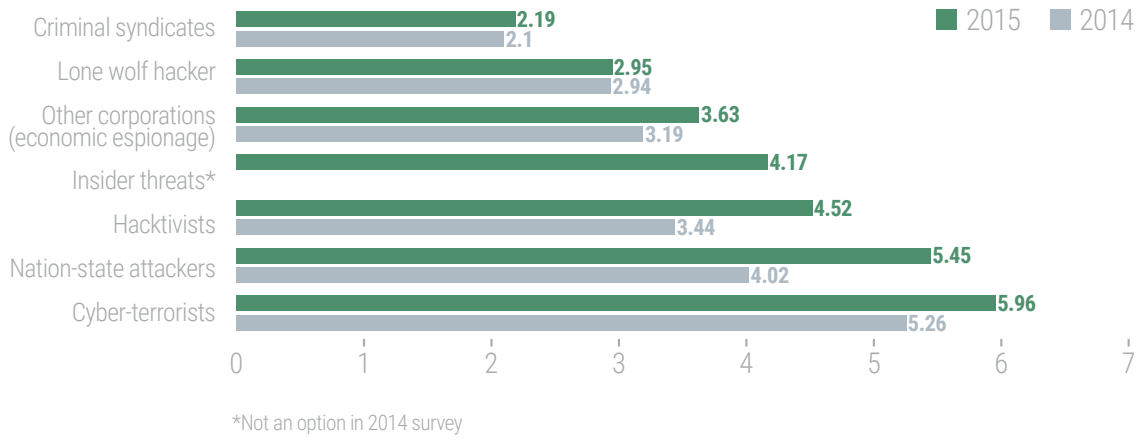
Cyber attacks are more frequent and more sensitive information has been lost or exposed since last year. On average, organizations in this study have had 40 cyber attacks in the past 12 months and this is an increase from 34 attacks in last year's study. As shown in Figure 1, 51 percent say they experienced an incident involving the loss or exposure of sensitive information, and this is an increase from 46 percent in 2014.

FIGURE 1. *Has your organization experienced an incident involving the loss or exposure of sensitive information in the past 12 months?*



According to Figure 2, the most likely attackers are considered to be criminal syndicates and lone wolf hackers. Least likely to attack organizations are cyber terrorists and nation state attackers. This year we introduced insider threats as one of the choices, and they were ranked more likely than hacktivists, nation-state attackers, and cyber terrorists to launch an attack.

FIGURE 2. *Which types of attackers are most likely to launch an attack against your company?*
1 = most likely to launch to 7 = least likely to launch

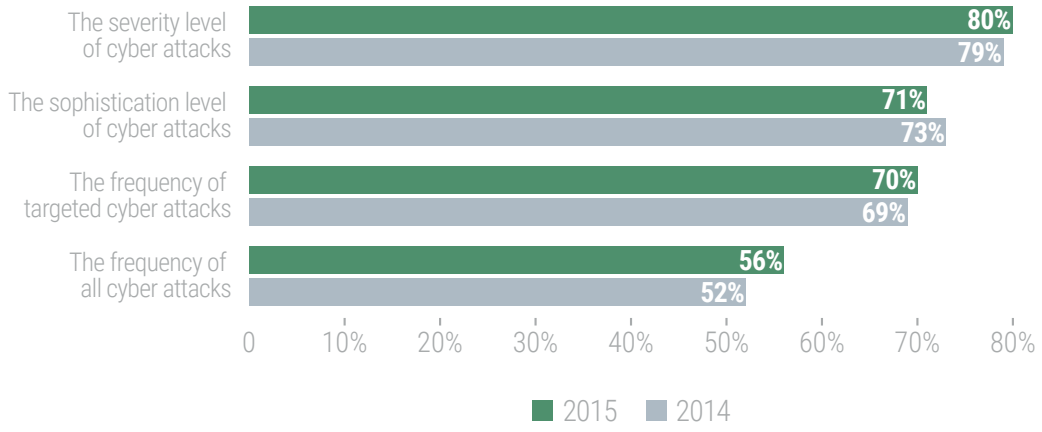


*Not an option in 2014 survey

The majority of respondents continue to say cyber attacks are increasing in frequency, sophistication, and severity. Only 37 percent of respondents believe their organization is winning the cyber security war.

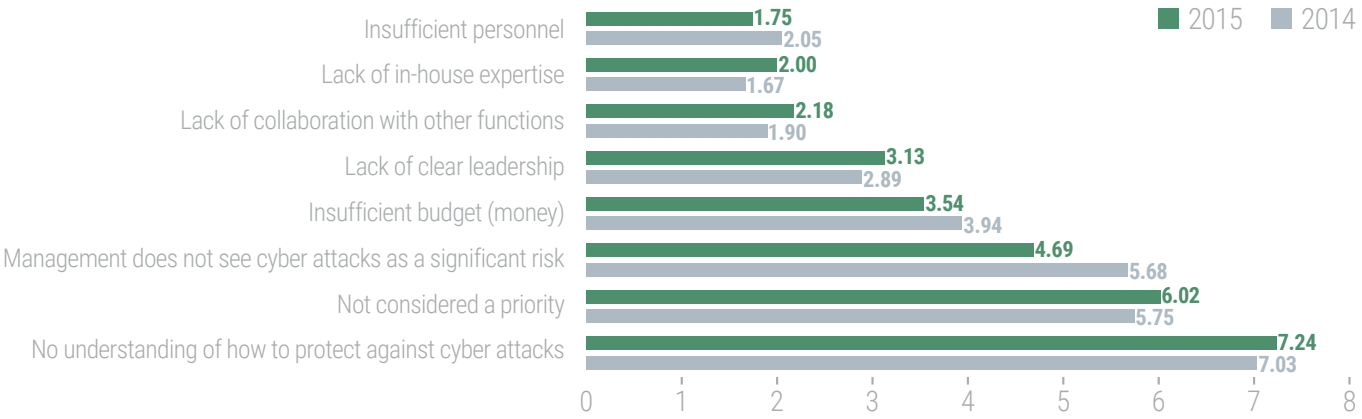
As presented in Figure 3, 56 percent of respondents say the frequency of all cyber attacks has increased (52 percent last year), 70 percent say the frequency of targeted cyber attacks has increased (69 percent last year), 71 percent of respondents say the sophistication level of cyber attacks has increased (73 percent last year), and 80 percent of respondents say the severity of cyber attacks has increased (79 percent last year).

FIGURE 3. *How have the frequency, sophistication, and severity of cyber attacks changed?*
Increased responses only



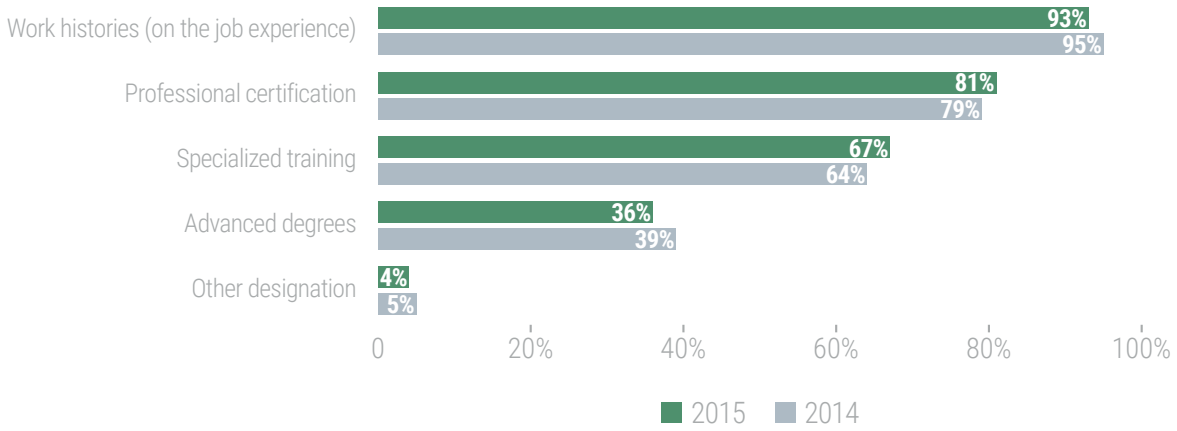
Sufficient and expert personnel are needed to achieve a strong cyber security posture. Insufficient personnel and lack of in-house expertise are the primary challenges to achieving a strong cyber security posture and these were significant barriers to cyber security readiness in last year's study as well, according to Figure 4.

FIGURE 4. *What challenges keep your organization's cyber security posture from being fully effective?*
1 = most challenging to 8 = least challenging



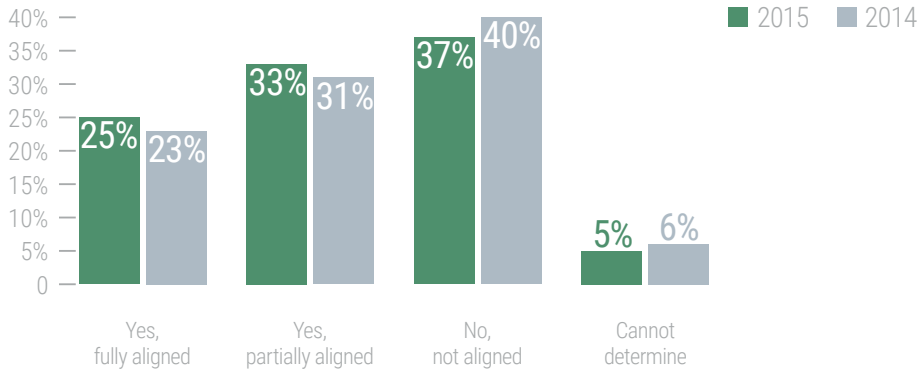
According to Figure 5, to determine if their personnel are qualified, organizations rely upon work histories and professional certification. Fifty percent of respondents say their organization does not have a sufficient number of in-house personnel who possess these qualifications or they are unsure.

FIGURE 5. *How does your organization determine the qualifications or expertise of personnel who manage cyber security risk?*
More than one response permitted



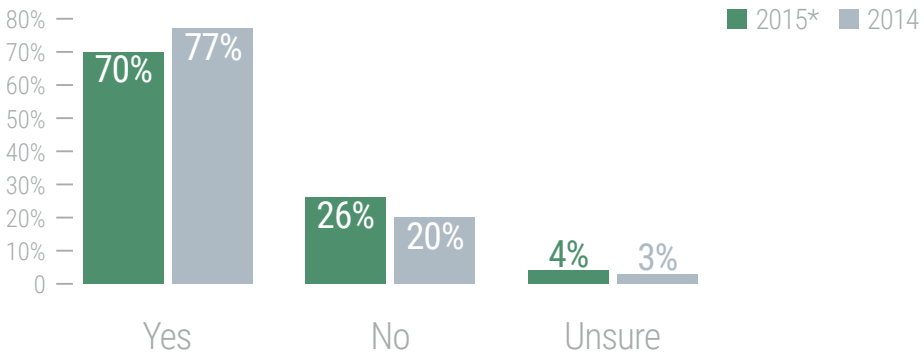
On a positive note, the majority of respondents (58 percent) believe their organization's cyber security strategy is fully or partially aligned with its business objectives and mission, as shown in Figure 6. This is an improvement from 54 percent last year.

FIGURE 6. *Is your organization's cyber security strategy aligned with its business objectives and mission?*



Organizations are getting better at preventing situations when cyber attacks evade intrusion detection systems (IDS) but advanced persistent threats (APTs) affect most organizations. This year, 70 percent of respondents say their organizations experienced situations when cyber attacks have evaded their IDS, and this declined from 77 percent of respondents last year, according to Figure 7.

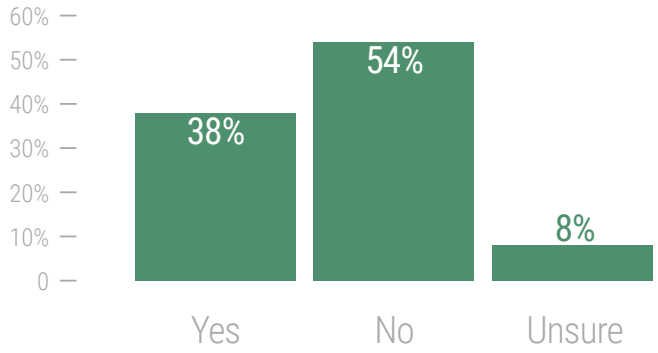
FIGURE 7. *Did you experience a cyber attack that evaded IDS or anti-virus (AV) solutions?*



*In this year's study, we asked respondents two separate questions: if their organization had ever experienced situations when cyber attacks have evaded their IDS, and if they had ever experienced situations where they have evaded their AV solutions and/or other traditional security controls. The 2015 responses indicated above reflect the responses to the first question (IDS) only. For a detailed breakdown of responses to both questions, please see the appendix.

As shown in Figure 8, only 38 percent of respondents say their organizations have systems and controls in place to detect and stop APTs.

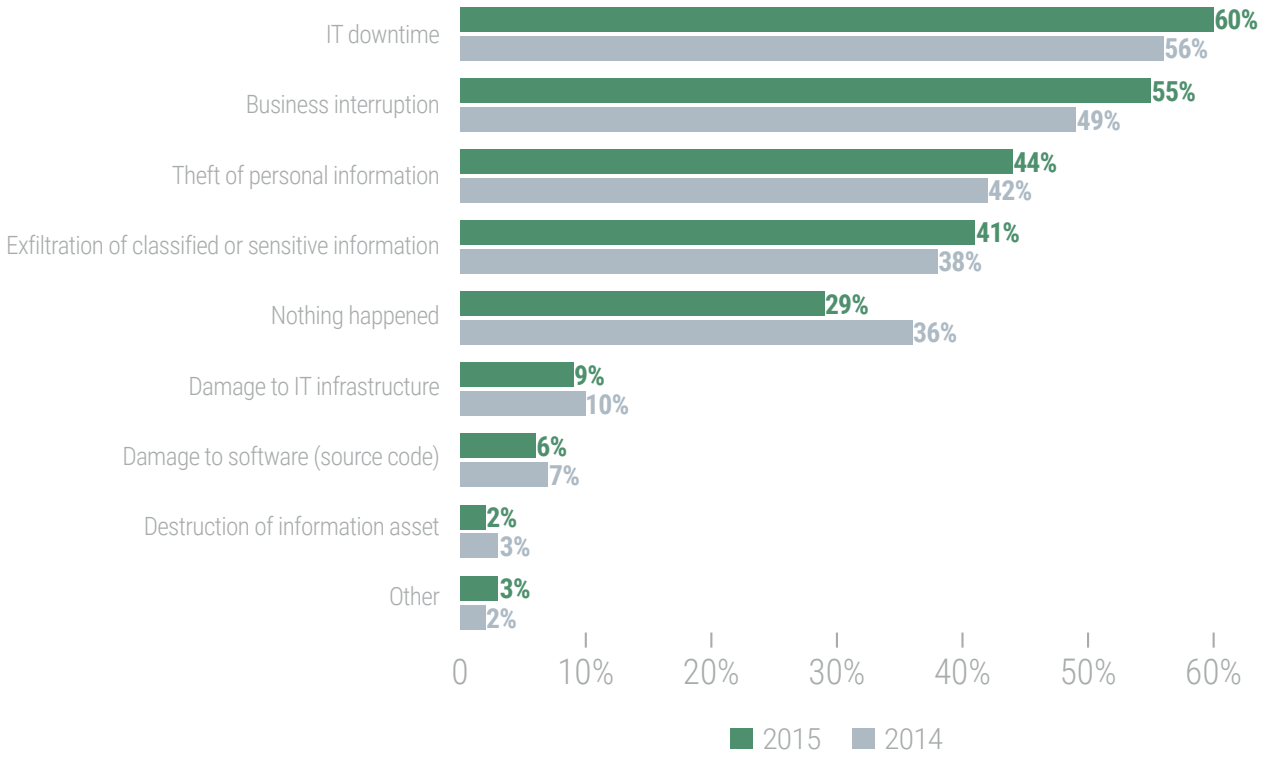
FIGURE 8. *Does your organization have systems and controls in place to detect and stop APTs?*



Organizations have an average of almost one separate APT-related incident per month. IT downtime, business disruption, and theft of personal information are the primary consequences of APTs or zero day threats experienced, according to Figure 9. On average, respondents say 25 percent of employees were targeted by phishing attacks.

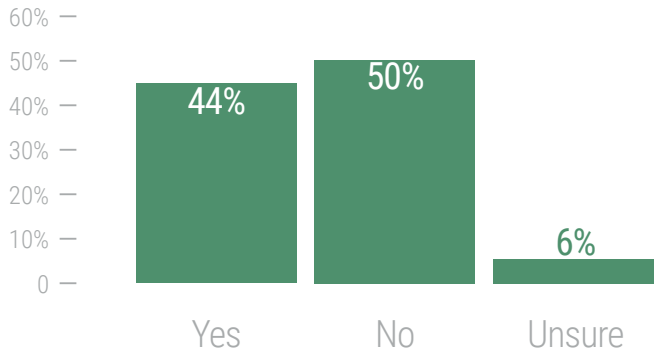
Interestingly, almost one third of respondents said nothing happened as a result of the APTs, but with 54 percent of respondents without systems and controls in place to detect APTs or zero day threats, it is possible that these threats are going unidentified or being misdiagnosed in the environment.

FIGURE 9. *What happened as a result of the APTs or zero day threats your organization experienced?*
More than one response permitted



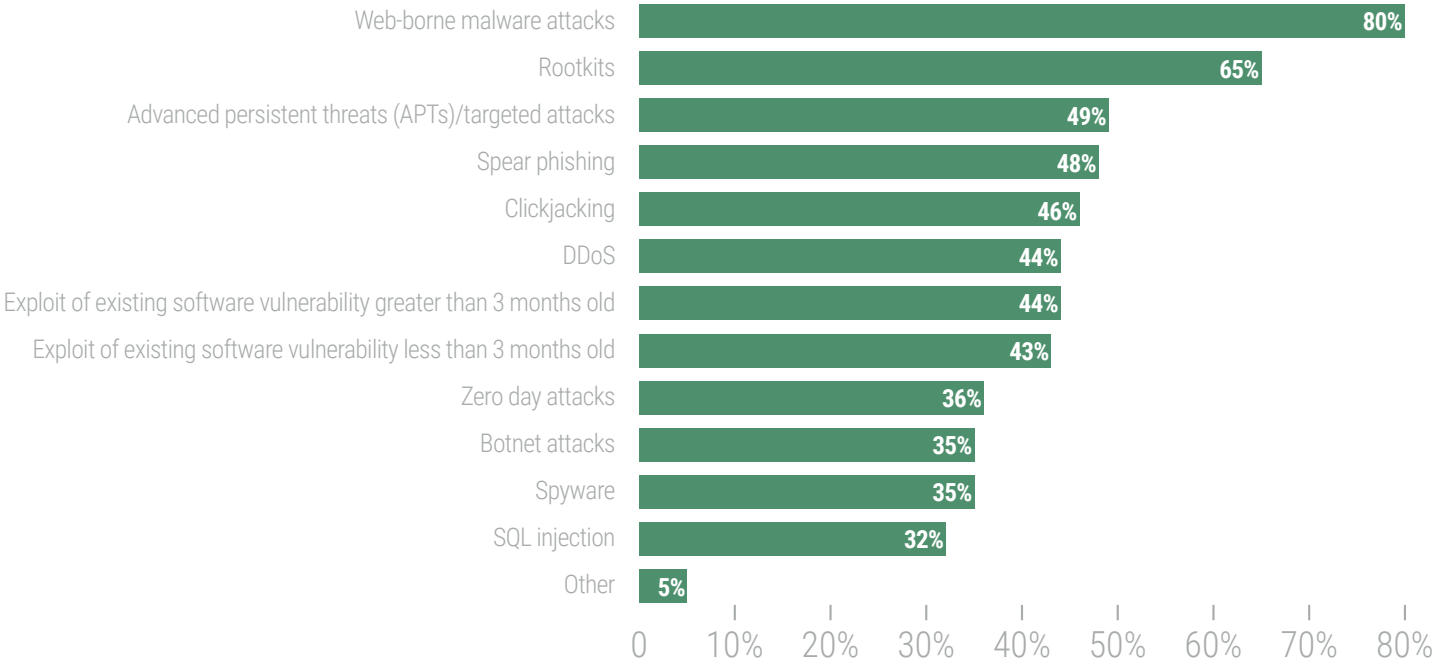
Denial of service (DoS) attacks are estimated to occur every other month. According to Figure 10, 44 percent of respondents say their organization experienced a DoS attack that caused a disruption to business operations and/or system downtime. Respondents estimate that the cost of business disruptions and system downtime due to DoS attacks averaged $1.2 million in the past 12 months.

FIGURE 10. *Did your organization experience a DoS attack that caused a disruption to business operations and/or system downtime?*



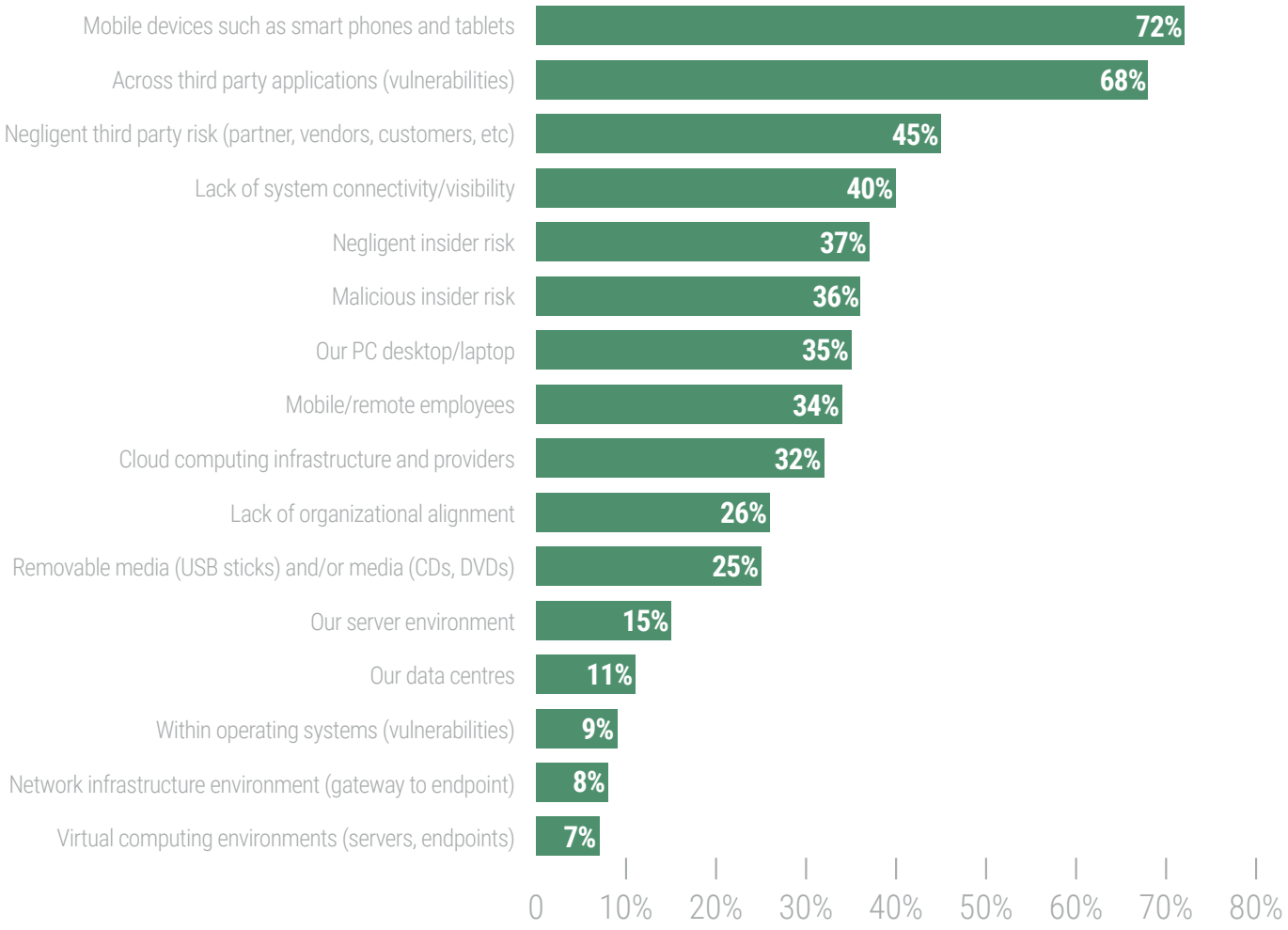
The greatest threats to organizations are web-borne attacks. As shown in Figure 11, 80 percent of respondents say the most frequent compromises are web-borne malware attacks, followed by rootkits at 65 percent of respondents.

FIGURE 11. *Incidents or compromises frequently seen in IT networks*
More than one response permitted



Respondents feel the greatest rise in potential IT security risks are from mobile devices and third party applications.

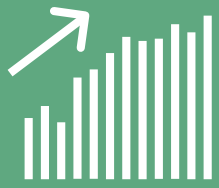
FIGURE 12. *Where are you seeing the greatest rise of potential IT security risk within your IT environment?*
Five responses permitted



On average,
respondents estimated that
cyber security compromise
cost their organization

$7 MILLION

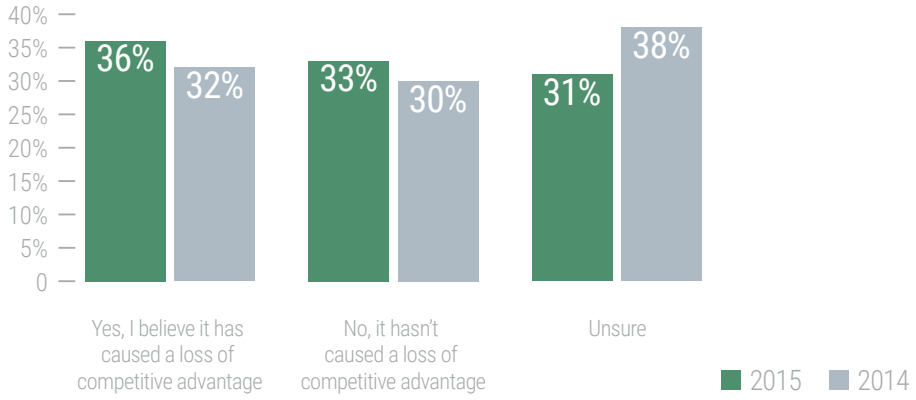
in the last 12 months



THE FINANCIAL ASPECTS OF CYBER CRIME AND CYBER SECURITY

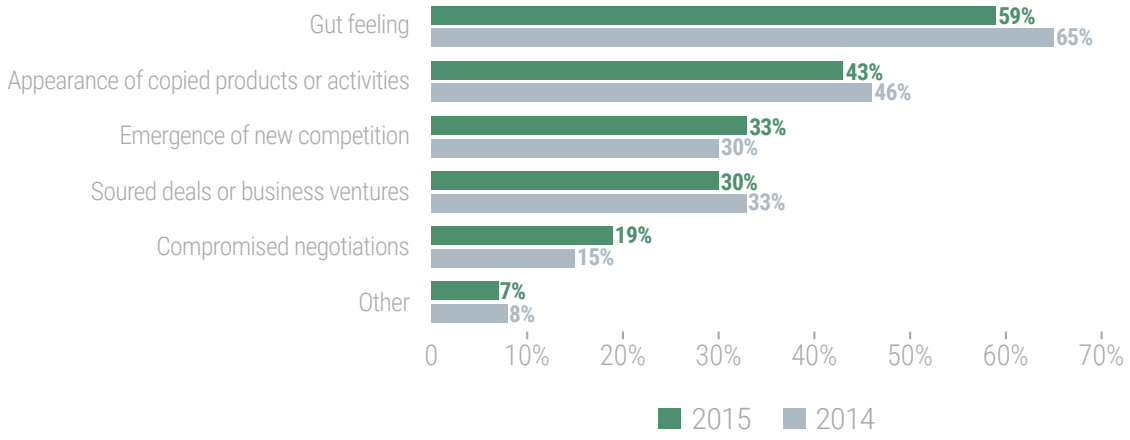
Intellectual property is targeted for cyber attacks. Thirty-three percent of respondents say their firm experienced a loss of intellectual property or other commercially sensitive business information due to cyber attacks within the past 24 months, and 36 percent of these respondents believe that it caused a loss of competitive advantage, as shown in Figure 13.

FIGURE 13. *Do you think the loss of intellectual property has caused your firm to lose its competitive advantage?*



Based on the findings in Figure 14, perceptions about the loss of competitive advantage are based primarily on a gut feeling (59 percent of respondents) and the appearance of copied products or activities (43 percent of respondents).

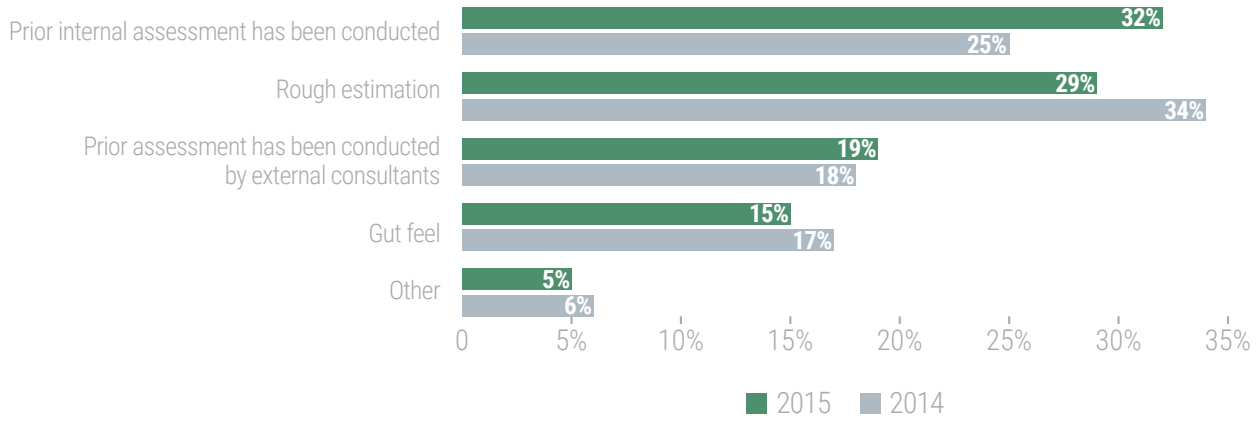
FIGURE 14. *How did your firm determine the loss of competitive advantage as a result of the cyber attack?*
More than one response permitted



Of those organizations that had their intellectual property stolen in the past 24 months (33 percent of respondents), the average estimated cost to the organization was about $6 million. These respondents also say their organizations lost an average of approximately $5.5 million due to the theft of commercially sensitive information.

According to Figure 15, these assessments were based upon a prior internal assessment (32 percent of respondents), rough estimation (29 percent of respondents), assessment conducted by consultants (19 percent of respondents), and gut feel (15 percent of respondents).

FIGURE 15. *How did you estimate the cost of lost competitive advantage due to a cyber attack?*



Theft of intellectual property is not the only cost from a cyber attack. On average, over the last 12 months, organizations represented in this study spent approximately $7 million each on the following: clean up or remediation ($766,667), lost user productivity ($950,625), disruption to normal operations ($1.1 million), damage or theft of IT assets and infrastructure ($1.6 million), and damage to reputation and marketplace image ($2.6 million). Table 1 shows how this amount increased since last year. Disruption and lost user productivity declined slightly. All other categories increased.

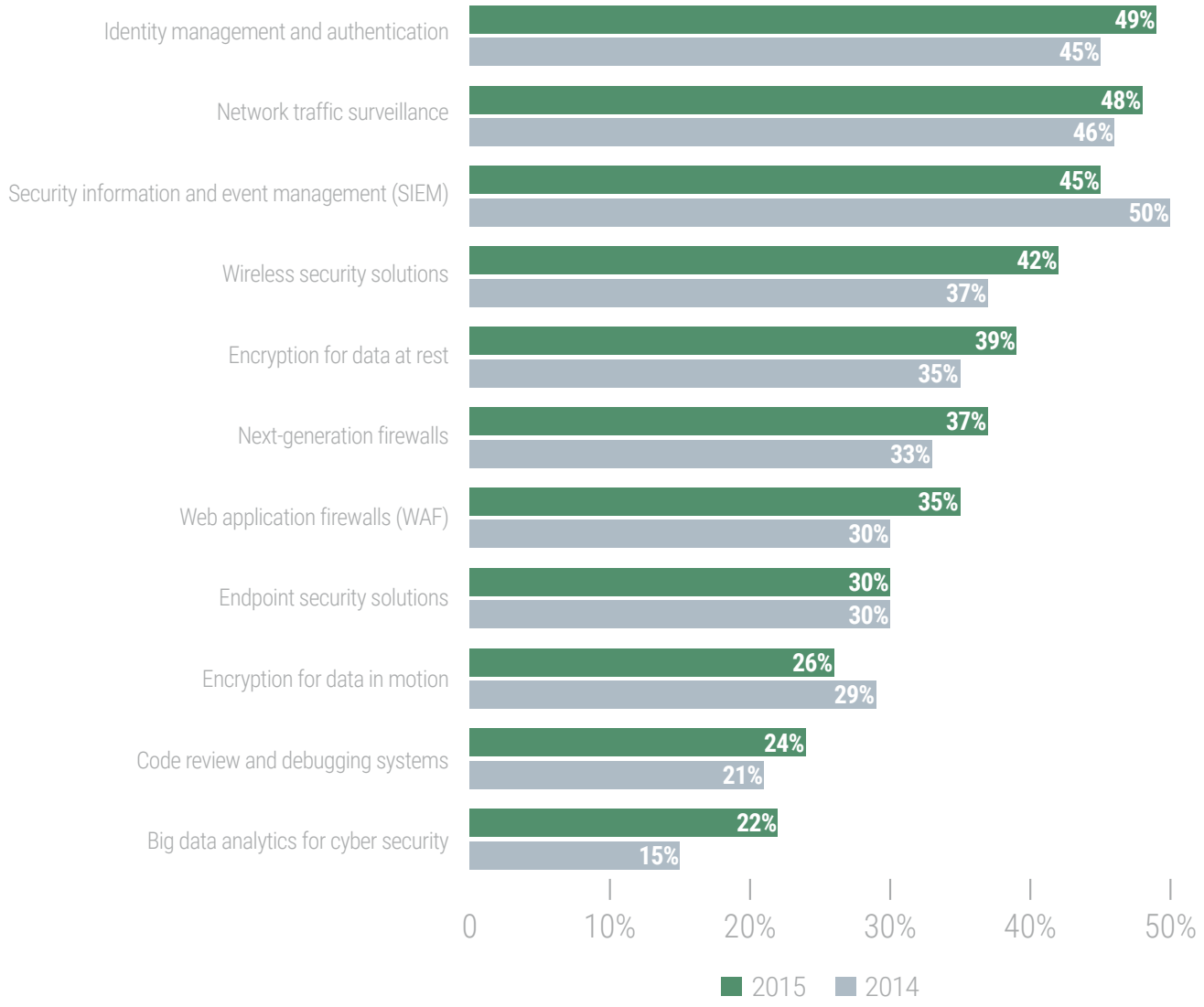
TABLE 1. *How much did cyber security compromise cost your organization?*
Extrapolated value

	2015	2014
Cleanup or remediation	$766,667	$676,023
Lost user productivity	$950,625	$987,191
Disruption to normal operations	$1,061,818	$1,101,379
Damage or theft of IT assets and infrastructure	$1,638,663	$1,533,989
Damage to reputation	$2,647,560	$2,586,941
Total	**$7,065,332**	**$6,885,523**

Are organizations spending enough on security? On average, respondents estimate their approximate annual budget for IT is $71 million and an average of 11 percent of this budget is dedicated to information security. This increased slightly from about 10 percent last year.

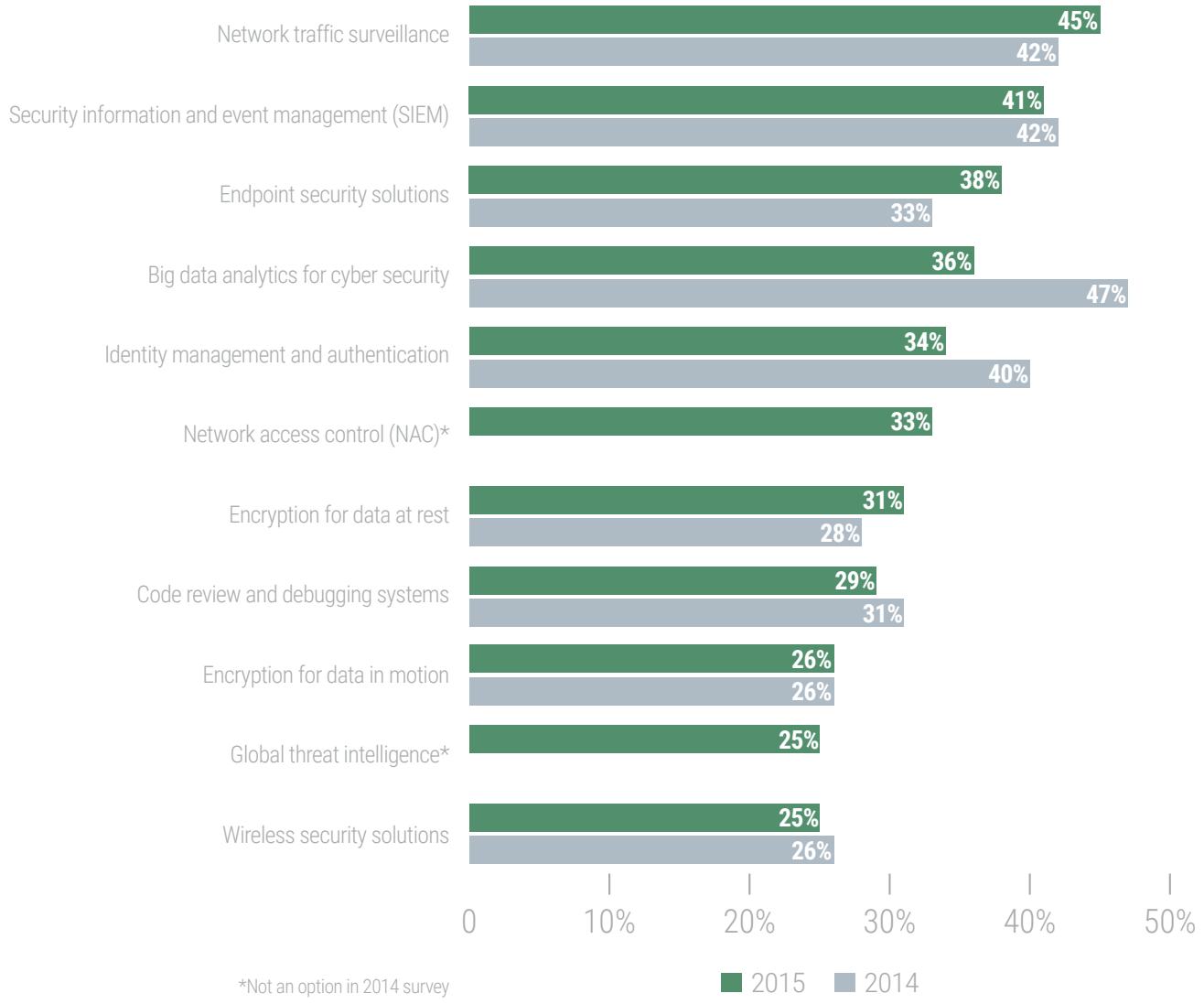
The majority of respondents (51 percent) measure the effectiveness of investment in security technologies to achieve security objectives. As shown in Figure 16, the top five most effective technologies are: identity management and authentication, network traffic surveillance, SIEM, wireless security solutions, and encryption for data at rest.

FIGURE 16. *Which security technologies have been the most effective in helping your organization achieve its security objectives?*
Five responses permitted



According to Figure 17, technologies that are expected to receive the most funding in the next 12 months are: network traffic surveillance, SIEM, endpoint security solutions, big data analytics for cyber security, and identity management and authentication.

FIGURE 17. *The top technologies that will receive more spending*
More than one response permitted

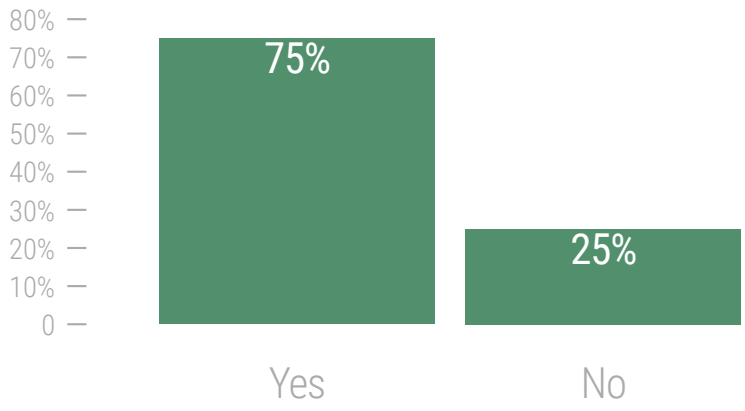


*Not an option in 2014 survey

THE IMPORTANCE OF THREAT INTELLIGENCE

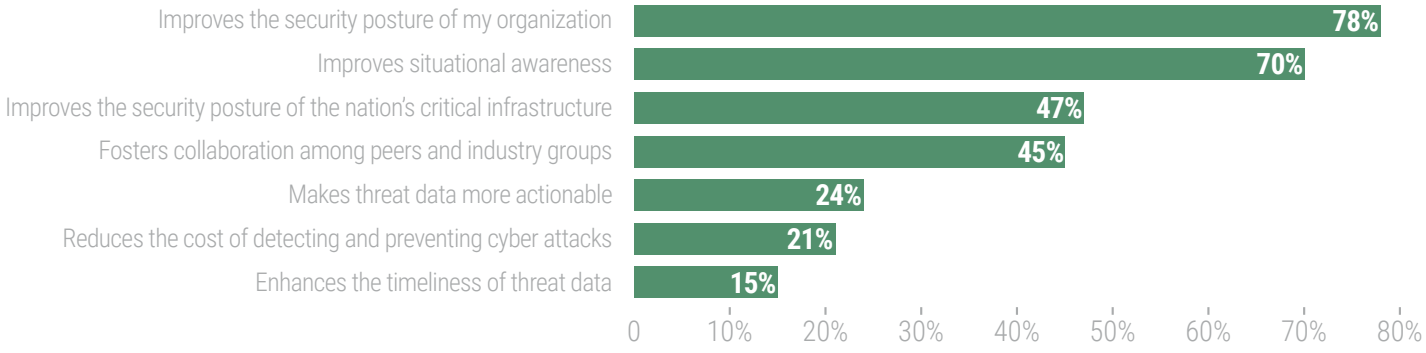
A strong security posture is dependent upon threat intelligence. As shown in Figure 18, the majority of respondents believe in gathering and using threat intelligence to win the cyber security war. Sixty percent of respondents do either fully or partially participate in an initiative or program for exchanging threat intelligence with peers, government, and/or industry groups.

FIGURE 18. *Do you believe gathering and using threat intelligence is essential to a strong security posture?*



Why do organizations participate in threat intelligence sharing? According to Figure 19, those organizations participating in threat intelligence sharing do so because it improves the security posture of their organization, in addition to improving situational awareness.

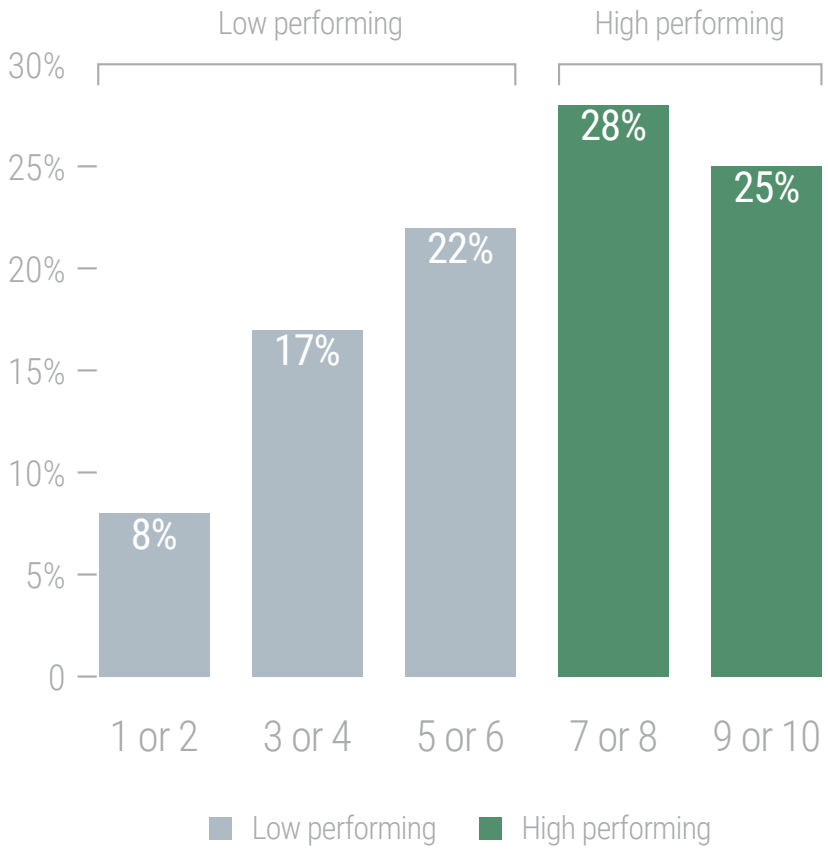
FIGURE 19. *If your organization participates, what are the main reasons?*
Three responses permitted



CHARACTERISTICS OF ORGANIZATIONS WITH A STRONG CYBER SECURITY POSTURE

As part of the research, we identified certain organizations represented in this study that self-reported to have achieved a more effective cyber security posture. As shown in Figure 20, high performing organizations represent 53 percent of the organizations in this study (a self-reported effectiveness rating of 7 or higher on a scale of 1 = not effective to 10 = very effective).

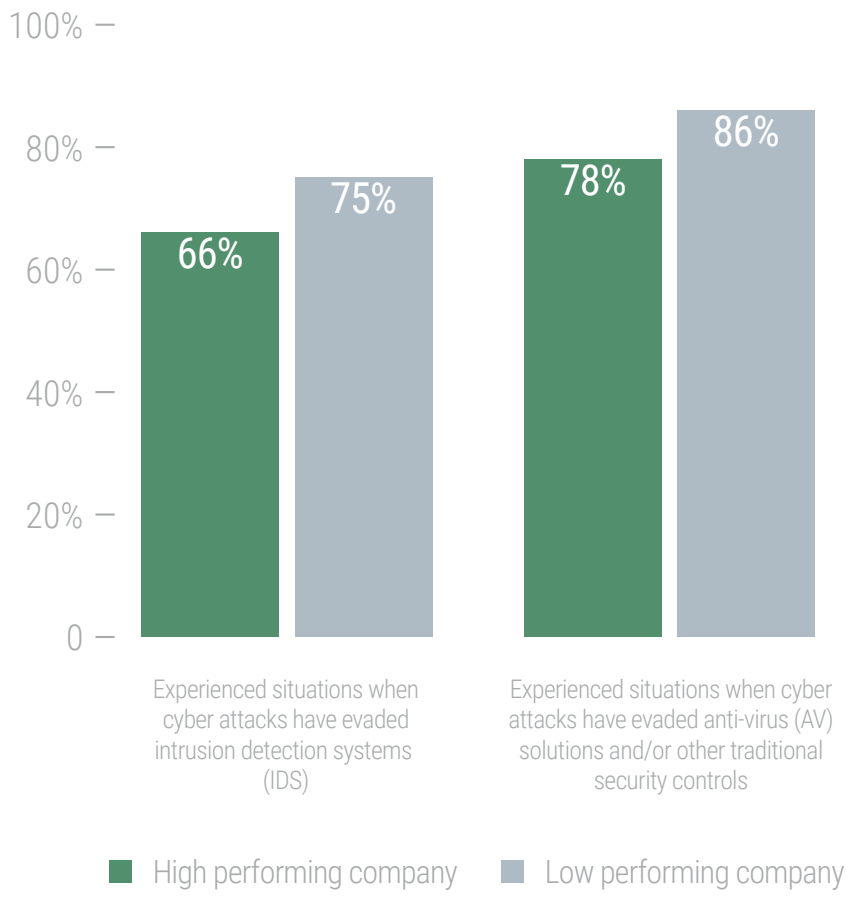
FIGURE 20. *How do you rate the effectiveness of your organization's cyber security posture and its ability to mitigate risks, vulnerabilities, and attacks across the enterprise?*
1= Not effective to 10 = Very effective
Extrapolated value = 6.4



What are the characteristics of a high performing organization? We cross-tabulated the responses from high performing organizations to understand if they were fundamentally different to the low performers. 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 secure additional funding is the fact that their cyber security strategy is supportive of their organization's business goals and mission.

In the past 12 months, high performing organizations actually reported more cyber attacks (an average of 45 attacks vs. 35 attacks on low performing organizations). However, high performing organizations have fewer successful cyber attacks. While both types of organizations have experienced situations when cyber attacks have evaded their IDS, fewer respondents in high performing organizations say they have had such a situation (66 percent of respondents vs. 75 percent of respondents in low performing organizations), as shown in Figure 21. Respondents in high performing organizations also say their organizations have fewer situations when cyber attacks evaded anti-virus solutions and other traditional security controls.

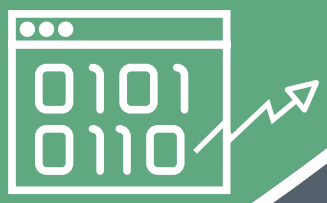
FIGURE 21. *Have cyber attacks evaded IDS and AV solutions?*
Yes responses only



High performing organizations are

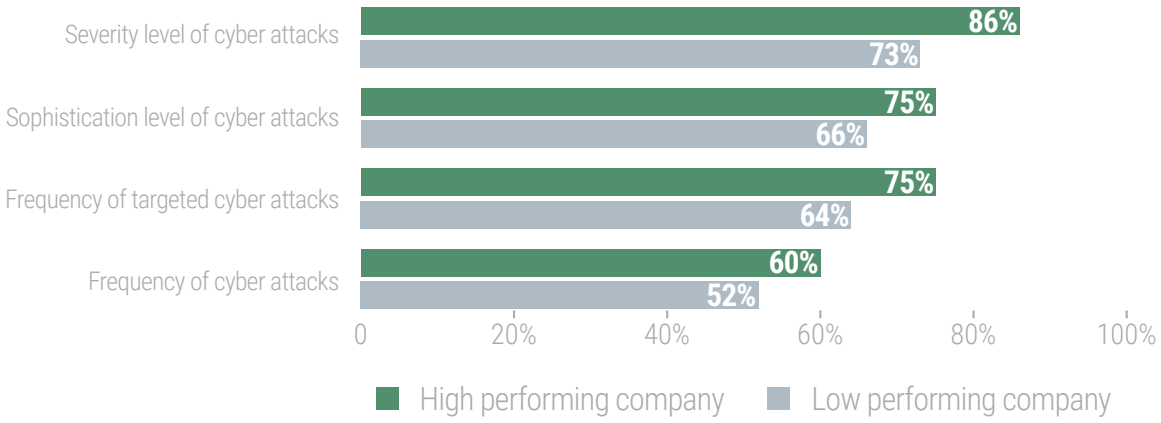
19%

LESS likely than low performers to have experienced an incident in the last 12 months that led to the loss or exposure of sensitive information



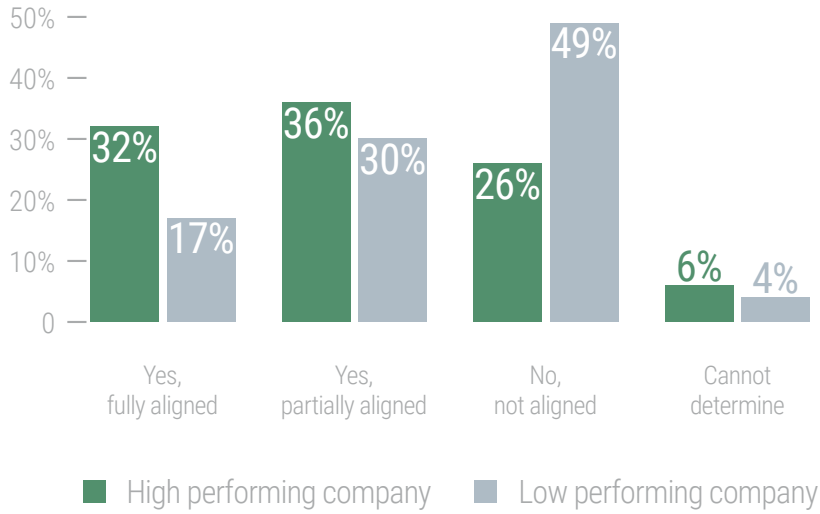
High performing organizations are more aware of the threat landscape. As shown in Figure 22, respondents in high performing organizations are more likely to believe the threat landscape is getting worse. They believe cyber attacks are becoming more severe, sophisticated, and frequent. It is very possible that this awareness is one of the reasons they detect more attacks per year.

FIGURE 22. *Changes in cyber attacks over the previous 12 months*
Increased responses only



Cyber security strategies are more often aligned with business objectives. According to Figure 23, high performing organizations are more likely to have their organization's cyber security strategy aligned with its business objectives and mission. High performers are almost twice as likely as low performers to have a cyber security strategy that is fully aligned to the business goals and mission.

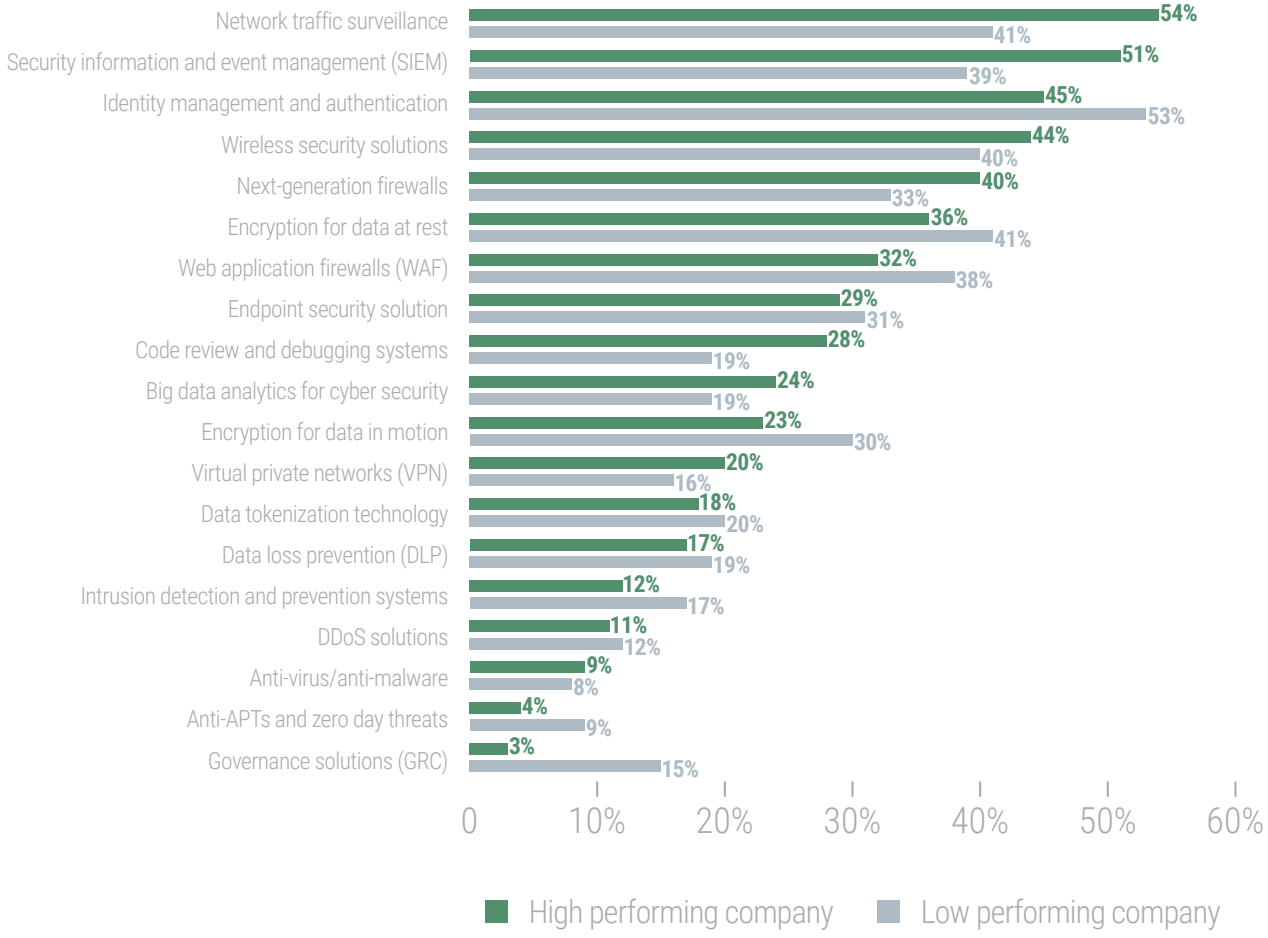
FIGURE 23. *Is your organization's cyber security strategy aligned with its business objectives and mission?*



High performing organizations have more resources to fight the cyber security war. High performing organizations dedicate 43 percent more of their total IT budget to security than the low performing organizations (an average of 12.3 percent of the IT budget vs. 8.6 percent). They are also more likely to have a sufficient number of in-house personnel who possess the necessary skills and experience required to manage cyber security risk (56 percent of high performers believe they have a sufficient number of in-house personnel with these skills and experience, versus 43 percent of low performers).

According to Figure 24, high performing and low performing organizations have different perceptions about which technologies are most effective in achieving their security objectives. By far, high performing organizations consider network traffic surveillance and SIEM as most effective. Low performing organizations consider identity management and authentication as most effective. Given that high performers report more attacks but less successful breaches, it would appear that monitoring and visibility tools yield effective results.

FIGURE 24. *Security technologies that are considered most effective*
More than one response permitted



Do these characteristics yield results? High performers do see marked improvements versus low performers. They are 28 percent more likely to believe they are winning the cyber security war, and 19 percent less likely to have experienced an incident in the last 12 months that led to the loss or exposure of sensitive information. While this is an encouraging outlook, it is interesting to note that their increased spend (43 percent more than low performers) does not yield a 1:1 improvement in these statistics.

PART THREE

CONCLUSIONS

High performing organizations invest in

VISIBILITY

of their network,

DETECT

more attacks, and suffer less successful

BREACHES

PART THREE
CONCLUSIONS

While it appears that the overall threat landscape has become more severe in the last 12 months, high performing organizations continue to illustrate that it is possible to improve an organization's cyber security posture. The practices of these high performers provide guidance on how organizations can improve their cyber security effectiveness. High performing organizations invest in visibility of their network, detect more attacks, and suffer less successful breaches. They also ensure enterprise-wide adoption of a cyber security strategy by aligning it with the overall mission of the organization. This alignment enables them to allocate a greater portion of their IT budget to security-specific initiatives. Some specific strategies and tactics organizations should consider to increase their security posture are:

- Conduct assessments to understand areas where the organization is most vulnerable to an attack. If necessary, enlist the help of trusted risk advisory consultants who will work directly with your organization to efficiently identify and manage risk in your environment.

- Secure adequate resources for investment in practices and technologies determined to be critical to achieving a strong cyber security posture. Align your security strategy to the overall business goals and mission to help secure sufficient budget and ensure your spend is being allocated wisely. If you don't know where to start, look to trusted advisory firms who can provide virtual CISO programs and help you to build an end-to-end security program.

- Invest in technologies such as SIEM, network intelligence, and identity management and authentication to identify and understand normal versus abnormal behaviour in your environment.

- Proactively recruit experts with the necessary skillset to help lead the organization's cyber security team. Ensure the in-house expertise exists and encourage all IT and IT security practitioners on staff to obtain specialized training and maintain their credentials. If you do not have sufficient in-house expertise, consider outsourcing to a managed security services provider.

If you have any questions on any of the findings of this study, or would like to better understand where your organization is on the high/low performing scale, reach out to your local Scalar office.

56%

of respondents report their position is at or above the supervisory level

PART FOUR

METHODS

PART FOUR
METHODS

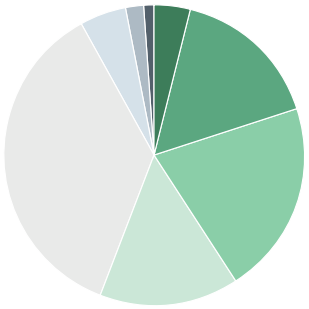
A sampling frame of 16,470 IT and IT security practitioners in Canada who play a role in directing the IT function, improving IT security in their organizations, setting IT priorities, and managing budgets were selected as participants to this survey. Table 2 shows 699 total returns. Screening and reliability checks required the removal of 45 surveys. Our final sample consisted of 654 surveys or a 4.0 percent response.

TABLE 2. Sample response

	2015	2014
Total sampling frame	16,470	15,816
Total returns	699	701
Rejected or screened surveys	45	78
Final sample	654	623
Response rate	**4.0%**	**3.9%**

PIE CHART 1.
Current position within the organization

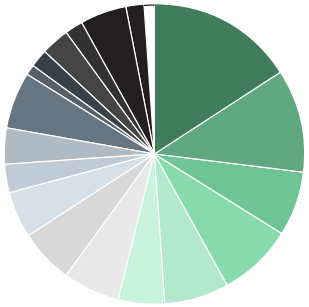
Pie Chart 1 reports the respondent's organizational level within participating organizations. By design, more than half of respondents (56 percent) are at or above the supervisory levels.



Executive/VP	4%
Director	16%
Manager	21%
Supervisor	15%
Technician	36%
Associate/staff	5%
Consultant/contractor	2%
Other	1%

PIE CHART 2.
Primary industry focus

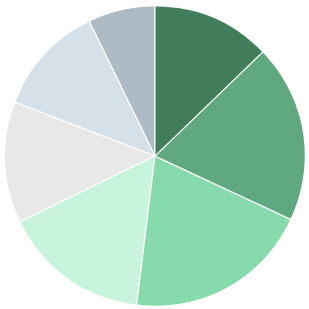
Pie Chart 2 reports the industry classification of respondents' organizations. This chart identifies financial services (16 percent) as the largest segment, followed by public sector (11 percent), and services (8 percent).



Financial services	16%
Public sector	11%
Retail	7%
Services	8%
Technology & software	7%
Professional Services	5%
Conglomerates	6%
Energy & utilities	6%
Consumer products	5%
Education & research	3%
Health & life sciences	4%
Manufacturing & mining	6%
Aerospace & defence	1%
Agriculture & food services	2%
Entertainment & media	3%
Communications	2%
Industrial	5%
Transportation	2%
Other	1%

PIE CHART 3.
Global employee headcount

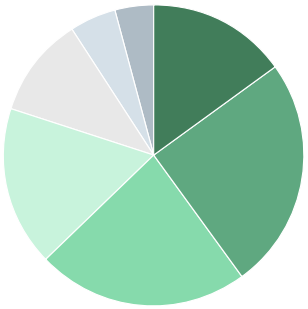
As shown in Pie Chart 3, almost half (48 percent) of respondents are from organizations with a global headcount of more than 1,000 employees.



≤ 250	13%
251 to 500	19%
501 to 1,000	20%
1,001 to 5,000	16%
5,001 to 10,000	13%
10,001 to 25,000	12%
> 25,000	7%

PIE CHART 4.
Canadian employee headcount

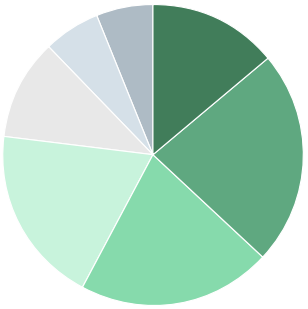
As shown in Pie Chart 4, 65 percent of respondents are from organizations with a Canadian headcount of between 251 and 5,000 employees.



≤ 250	15%
251 to 500	25%
501 to 1,000	23%
1,001 to 5,000	17%
5,001 to 10,000	11%
10,001 to 25,000	5%
> 25,000	4%

PIE CHART 5.
Global revenue for the last fiscal year

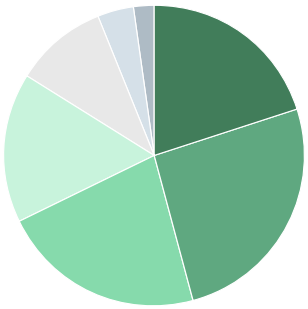
Sixty-three percent of respondents reported their organization's global revenue for the last fiscal year to be at or above $50 million, as shown in Pie Chart 5.



Under $20 million	14%
$20 million to $49.9 million	23%
$50 million to $299.9 million	21%
$300 million to $999.9 million	19%
$1 billion to $2.99 billion	11%
$3 billion to $6.99 billion	6%
$7 billion and above	6%

PIE CHART 6.
Canadian revenue for the last fiscal year

More than half (54 percent) of the respondents reported their organization's Canadian revenue for the last fiscal year to be at or above $50 million, as shown in Pie Chart 6.



Under $20 million	20%
$20 million to $49.9 million	26%
$50 million to $299.9 million	22%
$300 million to $999.9 million	16%
$1 billion to $2.99 billion	10%
$3 billion to $6.99 billion	4%
$7 billion and above	2%

PART FIVE
CAVEATS

PART FIVE

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 Canada. We also acknowledge that the results may be biased by external events such as media coverage. 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 accurate responses.

PART SIX

APPENDICES

APPENDIX A: 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 October 2015.

Survey response	2015	2014
Total sampling frame	16,470	15,816
Total returns	699	701
Rejected or screened surveys	45	78
Final sample	654	623
Response rate	4.0%	3.9%

S1. *Which of the following best describes your role in managing the IT function within your organization? Check all that apply.*

	2015	2014
Setting IT priorities	55%	53%
Managing IT budgets	50%	51%
Selecting vendors and contractors	49%	46%
Determining IT strategy	31%	33%
Evaluating program performance	47%	48%
Bolstering IT security	70%	67%
None of the above [STOP]	0%	0%
Total	302%	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)? 1 = not effective to 10 = very effective.*

	2015	2014
1 or 2	8%	9%
3 or 4	17%	20%
5 or 6	22%	23%
7 or 8	28%	29%
9 or 10	25%	19%
Total	100%	100%
Extrapolated value	6.40	6.08

Q2. *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.*

	2015	2014
Insufficient personnel	1.75	2.05
Lack of in-house expertise	2.00	1.67
Lack of collaboration with other functions	2.18	1.90
Lack of clear leadership	3.13	2.89
Insufficient budget (money)	3.54	3.94
Management does not see cyber attacks as a significant risk	4.69	5.68
Not considered a priority	6.02	5.75
No understanding of how to protect against cyber attacks	7.24	7.03
Average	3.82	3.86

Q3a. *How does your organization determine the qualifications or expertise of personnel who manage cyber security risk? Please select all that apply.*

	2015	2014
Professional certification	81%	79%
Work histories (on the job experience)	93%	95%
Specialized training	67%	64%
Advanced degrees	36%	39%
Other designation (please specify)	4%	5%
Total	281%	282%

Q3b. *Does your organization have a sufficient number of in-house personnel who possess these qualifications?*

	2015	2014
Yes	50%	46%
No	46%	49%
Unsure	4%	5%
Total	100%	100%

PART 2: Cyber Attack Experience

Q4. *Approximately, how many cyber attacks has your organization experienced over the past 12 months?*

	2015	2014
None	12%	15%
1 to 5	10%	12%
6 to 10	18%	23%
11 to 25	19%	14%
26 to 50	10%	11%
51 to 100	13%	10%
More than 100	18%	15%
Total	100%	100%
Extrapolated value	40.2	34.3

Q5. *Has your organization experienced an incident involving the loss or exposure of sensitive information in the past 12 months?*

	2015	2014
Yes	51%	46%
No	43%	48%
Unsure	6%	6%
Total	100%	100%

Q6. *Do you believe your organization is winning the cyber security war?*

	2015	2014
Yes	37%	41%
No	53%	50%
Unsure	10%	9%
Total	100%	100%

Q7a. *Has your organization ever experienced situations when cyber attacks have evaded your intrusion detection systems (IDS)?*

	2015	2014*
Yes	70%	77%
No	26%	20%
Unsure	4%	3%
Total	100%	100%

*IDS and AV responses were combined in 2014

Q7b. *Has your organization ever experienced situations when cyber attacks have evaded your anti-virus (AV) solutions and/or other traditional security controls?*

	2015
Yes	82%
No	15%
Unsure	3%
Total	100%

Q8. *Does your organization have systems and controls in place to detect and stop advanced persistent threats (APTs)?*

	2015
Yes	38%
No	54%
Unsure	8%
Total	100%

Q9. *How many separate APT-related incidents did your organization experience over the past 12 months?*

	2015
None	4%
1 to 2	3%
3 to 4	5%
5 to 6	7%
7 to 8	9%
9 to 10	12%
More than 10	14%
Unsure how to identify incidents as APTs	46%
Total	100%
Extrapolated value	8.91

Q10. *What happened to your organization as a result of the APTs or zero day threats it experienced? Please select all that apply.*

	2015	2014
Nothing happened	29%	36%
IT downtime	60%	56%
Business interruption	55%	49%
Exfiltration of classified or sensitive information	41%	38%
Theft of personal information	44%	42%
Damage to IT infrastructure	9%	10%
Damage to software (source code)	6%	7%
Destruction of information asset	2%	3%
Other (please specify)	3%	2%
Total	249%	243%

Q11. *Please rank order the following types of attackers from 1 = most likely to launch to 7 = least likely to launch an attack against your company.*

	2015	2014
Nation-state attackers	5.45	4.02
Criminal syndicates	2.19	2.1
Lone wolf hacker	2.95	2.94
Hacktivists	4.52	3.44
Cyber-terrorists	5.96	5.26
Insider threats*	4.17	
Other corporations (economic espionage)	3.63	3.19
Average	4.12	3.49

*Not a response in 2014

Q12. *What percentage of employees were targeted by a phishing attack?*	2015	2014*
None	27%	
1% to 20%	33%	
21% to 40%	14%	
41% to 60%	11%	
61% to 80%	9%	
81% to 100%	6%	
Total	100%	
Extrapolated value	25%	

Q13a. *Did your organization experience a denial of service (DoS) attack that caused a disruption to business operations and/or system downtime?*	2015	2014*
Yes	44%	
No	50%	
Do not know	6%	
Total	100%	

Q13b. *If yes, how many such attacks occurred in the past 12 months?*	2015	2014*
None	6%	
1 to 2	12%	
3 to 4	34%	
5 to 6	19%	
7 to 8	15%	
9 to 10	9%	
More than 10	5%	
Total	100%	
Extrapolated value	5.00	

Q13c. *If yes, how much did business disruptions and system downtimes cost your organization in the past 12 months?*	2015	2014*
Zero	18%	
Less than $100,000	29%	
$100,000 to $250,000	16%	
$250,001 to $500,000	19%	
$500,001 to $1,000,000	10%	
$1,000,001 to $5,000,000	3%	
$5,000,001 to $10,000,000	2%	
$10,000,001 to $25,000,000	2%	
$25,000,001 to $50,000,000	1%	
$50,000,001 to $100,000,000	0%	
More than $100,000,000	0%	
Total	100%	
Extrapolated value	$1,165,350	

*Not a question in 2014

Please rate the following statements using one of the four choices provided below each item.
Note that the time period for estimating the net change is the previous 24 months (relative to the prior years).

Q14a. *Within your organization, how has the frequency of all cyber attacks changed?*	2015	2014
Increased	56%	52%
Stayed the same	39%	44%
Decreased	5%	4%
Total	100%	100%

Q14b. *Within your organization, how has the frequency of targeted cyber attacks changed?*	2015	2014
Increased	70%	69%
Stayed the same	24%	26%
Decreased	6%	5%
Total	100%	100%

Q14c. *Within your organization, how has the sophistication level of cyber attacks changed?*	2015	2014
Increased	71%	73%
Stayed the same	24%	23%
Decreased	5%	4%
Total	100%	100%

Q14d. *Within your organization, how has the severity level of cyber attacks changed?*	2015	2014
Increased	80%	79%
Stayed the same	18%	21%
Decreased	2%	0%
Total	100%	100%

Q15. *Is your organization's cyber security strategy aligned with its business objectives and mission?*	2015	2014
Yes, fully aligned	25%	23%
Yes, partially aligned	33%	31%
No, not aligned	37%	40%
Cannot determine	5%	6%
Total	100%	100%

PART 3. Cost Estimation

Q16a. *Approximately, how much did cyber security compromise cost your organization in terms of cleanup or remediation (including technical support costs)?*	2015	2014
Zero	2%	0%
Less than $100,000	5%	6%
$100,000 to $250,000	45%	44%
$250,001 to $500,000	19%	20%
$500,001 to $1,000,000	11%	13%
$1,000,001 to $5,000,000	1%	3%
$5,000,001 to $10,000,000	3%	1%
$10,000,001 to $25,000,000	1%	1%
$25,000,001 to $50,000,000	0%	0%
$50,000,001 to $100,000,000	0%	0%
More than $100,000,000	0%	0%
Cannot estimate	13%	12%
Total	100%	100%
Extrapolated value	$766,667	$676,023

Q16b. *Approximately, how much did cyber security compromise cost your organization in terms of lost user productivity?*

	2015	2014
Zero	2%	0%
Less than $100,000	7%	4%
$100,000 to $250,000	18%	20%
$250,001 to $500,000	29%	32%
$500,001 to $1,000,000	16%	18%
$1,000,001 to $5,000,000	14%	12%
$5,000,001 to $10,000,000	2%	3%
$10,000,001 to $25,000,000	0%	0%
$25,000,001 to $50,000,000	0%	0%
$50,000,001 to $100,000,000	0%	0%
More than $100,000,000	0%	0%
Cannot estimate	12%	11%
Total	100%	100%
Extrapolated value	$950,625	$987,191

Q16c. *Approximately, how much did cyber security compromise cost your organization in terms of disruption to normal operations?*

	2015	2014
Zero	1%	0%
Less than $100,000	6%	3%
$100,000 to $250,000	18%	21%
$250,001 to $500,000	36%	39%
$500,001 to $1,000,000	17%	15%
$1,000,001 to $5,000,000	7%	7%
$5,000,001 to $10,000,000	1%	1%
$10,000,001 to $25,000,000	2%	0%
$25,000,001 to $50,000,000	0%	1%
$50,000,001 to $100,000,000	0%	0%
More than $100,000,000	0%	0%
Cannot estimate	12%	13%
Total	100%	100%
	$1,061,818	$1,101,379

Q16d. *Approximately, how much did cyber security compromise cost your organization in terms of damage or theft of IT assets and infrastructure?*

	2015	2014
Zero	6%	5%
Less than $100,000	5%	5%
$100,000 to $250,000	12%	14%
$250,001 to $500,000	35%	37%
$500,001 to $1,000,000	13%	11%
$1,000,001 to $5,000,000	6%	8%
$5,000,001 to $10,000,000	6%	7%
$10,000,001 to $25,000,000	3%	2%
$25,000,001 to $50,000,000	0%	0%
$50,000,001 to $100,000,000	0%	0%
More than $100,000,000	0%	0%
Cannot estimate	14%	11%
Total	100%	100%
Extrapolated value	$1,638,663	$1,533,989

Q16e. *Approximately, how much did cyber security compromise cost your organization in terms of damage to reputation and marketplace image (brand value)?*	2015	2014
Zero	3%	4%
Less than $100,000	3%	1%
$100,000 to $250,000	10%	11%
$250,001 to $500,000	23%	29%
$500,001 to $1,000,000	21%	16%
$1,000,001 to $5,000,000	12%	10%
$5,000,001 to $10,000,000	9%	10%
$10,000,001 to $25,000,000	1%	3%
$25,000,001 to $50,000,000	2%	1%
$50,000,001 to $100,000,000	0%	0%
More than $100,000,000	0%	0%
Cannot estimate	16%	15%
Total	100%	100%
Extrapolated value	$2,647,560	$2,586,941
Combined extrapolated value	$7,065,332	$6,885,523

Q17a. *Has your firm experienced a loss of intellectual property or other commercially sensitive business information due to cyber attacks within the past 24 months?*	2015	2014*
Yes	33%	35%
No or Unsure (Go to Q20)	67%	65%
Total	100%	100%

*In 2014, respondents were asked to consider the previous 12 months

Q17b. *If yes, do you think the loss of intellectual property, in particular, 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)?*	2015	2014
Yes, I believe it has caused a loss of competitive advantage	36%	32%
No, it hasn't caused a loss of competitive advantage	33%	30%
Unsure	31%	38%
Total	100%	100%

Q17c. *If yes, how did your firm determine the loss of competitive advantage as a result of the cyber attack?*	2015	2014
Gut feeling	59%	65%
Appearance of copied products or activities	43%	46%
Emergence of new competition	33%	30%
Soured deals or business ventures	30%	33%
Compromised negotiations	19%	15%
Other (please specify)	7%	8%
Total	191%	197%

Q18a. *Approximately, how much did losses due to the theft of intellectual property cost your organization over the past 24 months?*

	2015	2014*
Zero	0%	
Less than $100,000	8%	
$100,000 to $250,000	17%	
$250,001 to $500,000	24%	
$500,001 to $1,000,000	17%	
$1,000,001 to $5,000,000	3%	
$5,000,001 to $10,000,000	2%	
$10,000,001 to $25,000,000	4%	
$25,000,001 to $50,000,000	2%	
$50,000,001 to $100,000,000	2%	
More than $100,000,000	1%	
Cannot estimate	20%	
Total	100%	
Extrapolated value	$5,805,563	

Q18b. *Approximately, how much did losses due to theft of commercially sensitive information cost your organization over the past 24 months?*

	2015	2014*
Zero	0%	
Less than $100,000	0%	
$100,000 to $250,000	2%	
$250,001 to $500,000	3%	
$500,001 to $1,000,000	16%	
$1,000,001 to $5,000,000	28%	
$5,000,001 to $10,000,000	21%	
$10,000,001 to $25,000,000	8%	
$25,000,001 to $50,000,000	2%	
$50,000,001 to $100,000,000	1%	
More than $100,000,000	0%	
Cannot estimate	19%	
Total	100%	
Extrapolated value	$5,449,750	

*In 2014, the cost estimation was asked over the past 12 months, and is therefore not comparable to 2015 figures

Q18c. *Please explain how you arrived at the estimated cost ranges provided in Q18a and Q18b.*

	2015	2014
Prior internal assessment has been conducted	32%	25%
Prior assessment has been conducted by external consultants	19%	18%
Rough estimation	29%	34%
Gut feel	15%	17%
Other (please specify)	5%	6%
Total	100%	100%

PART 4. Security Spending & Investment

Q19. *What is your organization's approximate annual budget for IT?*	2015	2014*
Less than $1,000,000	1%	
$1,000,000 to $5,000,000	2%	
$5,000,001 to $10,000,000	2%	
$10,000,001 to $25,000,000	7%	
$25,000,001 to $50,000,000	12%	
$50,000,001 to $100,000,000	28%	
$100,000,001 to $250,000,000	23%	
$250,000,001 to $500,000,000	1%	
More than $500,000,000	0%	
Cannot estimate	24%	
Total	100%	
Extrapolated value	$70,944,000	

*Not a question in 2014

Q20. *What percentage of your organization's IT budget is dedicated to information security?*	2015	2014
Less than 3%*	4%	
3 to 6%	20%	38%
7 to 10%	23%	30%
11 to 15%	38%	13%
More than 15%	15%	19%
Total	100%	100%
Extrapolated value	10.9%	9.8%

*Not a response in 2014

Q21a. *Does your organization measure how effective investments in security technology are in achieving your security objectives?*	2015	2014
Yes	51%	47%
No	43%	46%
Unsure	6%	7%
Total	100%	100%

Q21b. *If yes, which of the following security technologies have been the most effective in helping your organization achieve its security objectives? Please select your top five choices.*

	2015	2014
Identity management and authentication	49%	45%
Network traffic surveillance	48%	46%
Security information and event management (SIEM)	45%	50%
Wireless security solutions	42%	37%
Encryption for data at rest	39%	35%
Next-generation firewalls	37%	33%
Web application firewalls (WAF)	35%	30%
Endpoint security solution	30%	30%
Encryption for data in motion	26%	29%
Code review and debugging systems	24%	21%
Big data analytics for cyber security	22%	15%
Data tokenization technology	19%	17%
Data loss prevention (DLP)	18%	17%
Virtual private networks (VPN)	18%	16%
Intrusion detection & prevention systems	14%	12%
DDoS solutions*	11%	
Governance solutions (GRC)	8%	10%
Anti-virus/anti-malware	8%	8%
Anti-APTs and zero day threats*	7%	
Total	500%	451%

Q22. *For each one of the following security technologies, please indicate whether your organization spending level will increase over the next 12 months.*

	2015	2014
Network traffic surveillance	45%	42%
Security information and event management (SIEM)	41%	42%
Endpoint security solutions	38%	33%
Big data analytics for cyber security	36%	47%
Identity management and authentication	34%	40%
Network access control (NAC)*	33%	
Encryption for data at rest	31%	28%
Code review and debugging systems	29%	31%
Encryption for data in motion	26%	26%
Wireless security solutions	25%	26%
Global threat intelligence*	25%	
Next-generation firewalls	22%	20%
Web application firewalls (WAF)	20%	22%
Data tokenization technology	19%	18%
Anti-virus/anti-malware	17%	12%
Data loss prevention (DLP)	16%	15%
Access governance*	11%	
Governance solutions (GRC)	10%	12%
Intrusion detection and prevention systems	9%	6%
Virtual private networks (VPN)	9%	5%
Anti-APTs and zero day threats*	8%	
Total	504%	425%

*Not a response in 2014

PART 5. Role & Organizational Characteristics

D1. *What best describes your position or organizational level?*	2015	2014
Executive/VP	4%	3%
Director	16%	17%
Manager	21%	21%
Supervisor	15%	16%
Technician	36%	34%
Associate/staff	5%	6%
Consultant/contractor	2%	3%
Other (please specify)	1%	0%
Total	100%	100%

D2. *What best describes your company's primary industry classification?*	2015	2014
Financial services	16%	17%
Public sector	11%	10%
Retail	7%	9%
Services	8%	7%
Technology & software	7%	6%
Professional Services	5%	6%
Conglomerates	6%	6%
Energy & utilities	6%	5%
Consumer products	5%	5%
Education & research	3%	4%
Health & life sciences	4%	4%
Manufacturing & mining	6%	4%
Aerospace & defence	1%	3%
Agriculture & food services	2%	3%
Entertainment & media	3%	3%
Communications	2%	3%
Industrial	5%	2%
Transportation	2%	2%
Other (please specify)	1%	1%
Total	100%	100%

D3. *What is the worldwide headcount of your organization?*	2015	2014
≤ 250	13%	15%
251 to 500	19%	18%
501 to 1,000	20%	21%
1,001 to 5,000	16%	15%
5,001 to 10,000	13%	13%
10,001 to 25,000	12%	10%
> 25,000	7%	8%
Total	100%	100%

D4. *What is the Canadian headcount of your organization?*	2015	2014*
≤ 250	15%	
251 to 500	25%	
501 to 1,000	23%	
1,001 to 5,000	17%	
5,001 to 10,000	11%	
10,001 to 25,000	5%	
> 25,000	4%	
Total	100%	

D5. *What is the worldwide revenue of your organization for the last fiscal year? If you are unsure, please provide a rough estimate.*	2015	2014
Under $20 million	14%	15%
$20 million to $49.9 million	23%	22%
$50 million to $299.9 million	21%	22%
$300 million to $999.9 million	19%	18%
$1 billion to $2.99 billion	11%	11%
$3 billion to $6.99 billion	6%	7%
$7 billion and above	6%	5%
Total	100%	100%

D6. *What is the Canadian revenue of your organization for the last fiscal year? If you are unsure, please provide a rough estimate.*	2015	2014*
Under $20 million	20%	
$20 million to $49.9 million	26%	
$50 million to $299.9 million	22%	
$300 million to $999.9 million	16%	
$1 billion to $2.99 billion	10%	
$3 billion to $6.99 billion	4%	
$7 billion and above	2%	
Total	100%	

*Not a question in 2014

Bonus Questions

BQ1. *Following are 5 areas of IT security risks. Please allocate the amount of spending earmarked for each risk listed in the table below. Use all 100 points in the table to allocate your responses.*	2015
Network	39
Application	16
Data	20
Endpoint	14
Human	11
Total points	100

BQ2. *Which of these types of incidents or compromises are you seeing frequently in your organization's IT networks? Please check all that apply.*

	2015
Web-borne malware attacks	80%
Rootkits	65%
Advanced persistent threats (APTs)/targeted attacks	49%
Spear phishing	48%
Clickjacking	46%
Exploit of existing software vulnerability greater than 3 months old	44%
DDoS	44%
Exploit of existing software vulnerability less than 3 months old	43%
Zero day attacks	36%
Spyware	35%
Botnet attacks	35%
SQL injection	32%
Other (please specify)	5%
Total	562%

BQ3. *Do you believe mobile endpoints have been the target of malware over the past 12 months?*

	2015
Yes	64%
No	20%
Unsure	16%
Total	100%

BQ4. *Where are you seeing the greatest rise of potential IT security risk within your IT environment? Please choose only your top five choices.*

	2015
Mobile devices such as smart phones and tablets	72%
Across third party applications (vulnerabilities)	68%
Negligent third party risk (partner, vendors, customers, etc)	45%
Lack of system connectivity/visibility	40%
Negligent insider risk	37%
Malicious insider risk	36%
Our PC desktop/laptop	35%
Mobile/remote employees	34%
Cloud computing infrastructure and providers	32%
Lack of organizational alignment	26%
Removable media (USB sticks) and/or media (CDs, DVDs)	25%
Our server environment	15%
Our data centres	11%
Within operating systems (vulnerabilities)	9%
Network infrastructure environment (gateway to endpoint)	8%
Virtual computing environments (servers, endpoints)	7%
Total	500%

BQ5a. *Does your organization participate in an initiative or program for exchanging threat intelligence with peers, government, and/or industry groups?*

	2015
Yes, fully participate	34%
Yes, partially participate	26%
Do not participate	40%
Total	100%

BQ5b. *If your organization participates, what are the main reasons? Please select only three choices.*

	2015
Improves the security posture of my organization	78%
Improves situational awareness	70%
Improves the security posture of the nation's critical infrastructure	47%
Fosters collaboration among peers and industry groups	45%
Makes threat data more actionable	24%
Reduces the cost of detecting and preventing cyber attacks	21%
Enhances the timeliness of threat data	15%
Other (please specify)	0%
Total	300%

BQ5c. *If your organization does not participate, what are the main reasons? Please select only three choices.*

	2015
No perceived benefit to my organization	76%
Lack of trust in the sources of intelligence	63%
Lack of resources	47%
Cost	45%
Slow, manual sharing processes	33%
Lack of incentives	17%
Potential liability of sharing	9%
Anti-competitive concerns	9%
Other (please specify)	1%
Total	300%

BQ6. *[If your organization shares] How does your organization exchange threat intelligence? Please select all that apply.*

	2015
Through an industry group	26%
Through a government entity	17%
Through a vendor threat exchange service	63%
Informal peer-to-peer exchange of information	70%
Total	176%

BQ7. *Do you believe gathering and using threat intelligence is essential to a strong security posture?*

	2015
Yes	75%
No	25%
Total	100%

APPENDIX B: Comparative Analysis of High vs. Low Performing Organizations

	Overall	Low	High
Sub-samples	654	307	347

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)? 1 = not effective to 10 = very effective.*

	Overall	Low	High
1 or 2	8%	8%	
3 or 4	17%	17%	
5 or 6	22%	22%	
7 or 8	28%		28%
9 or 10	25%		25%
Total	100%	47%	53%

Q3b. *Does your organization have a sufficient number of in-house personnel who possess these qualifications?*

	Overall	Low	High
Yes	50%	43%	56%
No	46%	52%	41%
Unsure	4%	5%	3%
Total	100%	100%	100%

Q4. *Approximately, how many cyber attacks has your organization experienced over the past 12 months?*

	Overall	Low	High
Extrapolated value	40.2	35.4	45.2

Q5. *Has your organization experienced an incident involving the loss or exposure of sensitive information in the past 12 months?*

	Overall	Low	High
Yes	51%	57%	46%
No	43%	38%	47%
Unsure	6%	5%	7%
Total	100%	100%	100%

Q6. *Do you believe your organization is winning the cyber security war?*

	Overall	Low	High
Yes	37%	32%	41%
No	53%	59%	48%
Unsure	10%	9%	11%
Total	100%	100%	100%

Q7a. *Has your organization ever experienced situations when cyber attacks have evaded your intrusion detection systems (IDS)?*

	Overall	Low	High
Yes	70%	75%	66%
No	26%	22%	29%
Unsure	4%	3%	5%
Total	100%	100%	100%

Q7b. *Has your organization ever experienced situations when cyber attacks have evaded your anti-virus (AV) solutions and/or other traditional security controls?*

	Overall	Low	High
Yes	82%	86%	78%
No	15%	11%	19%
Unsure	3%	3%	3%
Total	100%	100%	100%

Please rate the following statements using one of the four choices provided below each item.
Note that the time period for estimating the net change is the previous 24 months (relative to the prior years).

Q14a. *Within your organization, how has the frequency of all cyber attacks changed?*

	Overall	Low	High
Increased	56%	52%	60%
Stayed the same	39%	41%	37%
Decreased	5%	7%	3%
Total	100%	100%	100%

Q14b. *Within your organization, how has the frequency of targeted cyber attacks changed?*

	Overall	Low	High
Increased	70%	64%	75%
Stayed the same	24%	31%	18%
Decreased	6%	5%	7%
Total	100%	100%	100%

Q14c. *Within your organization, how has the sophistication level of cyber attacks changed?*

	Overall	Low	High
Increased	71%	66%	75%
Stayed the same	24%	30%	19%
Decreased	5%	4%	6%
Total	100%	100%	100%

Q14d. *Within your organization, how has the severity level of cyber attacks changed?*

	Overall	Low	High
Increased	80%	73%	86%
Stayed the same	18%	24%	13%
Decreased	2%	3%	1%
Total	100%	100%	100%

Q15. *Is your organization's cyber security strategy aligned with its business objectives and mission?*

	Overall	Low	High
Yes, fully aligned	25%	17%	32%
Yes, partially aligned	33%	30%	36%
No, not aligned	37%	49%	26%
Cannot determine	5%	4%	6%
Total	100%	100%	100%

Q20. *What percentage of your organization's IT budget is dedicated to information security?*

	Overall	Low	High
Extrapolated value	10.9%	8.6%	12.3%

Q21a. *Does your organization measure how effective investments in security technology are in achieving your security objectives?*

	Overall	Low	High
Yes	51%	41%	60%
No	43%	54%	33%
Unsure	6%	5%	7%
Total	100%	100%	100%

Q21b. *If yes, which of the following security technologies have been the most effective in helping your organization achieve its security objectives? Please select your top five choices.*

	Overall	Low	High
Identity management and authentication	49%	53%	45%
Network traffic surveillance	48%	41%	54%
Security information and event management (SIEM)	45%	39%	51%
Wireless security solutions	42%	40%	44%
Encryption for data at rest	39%	41%	36%
Next-generation firewalls	37%	33%	40%
Web application firewalls (WAF)	35%	38%	32%
Endpoint security solutions	30%	31%	29%
Encryption for data in motion	26%	30%	23%
Code review and debugging systems	24%	19%	28%
Big data analytics for cyber security	22%	19%	24%
Data tokenization technology	19%	20%	18%
Data loss prevention (DLP)	18%	19%	17%
Virtual private networks (VPN)	18%	16%	20%
Intrusion detection & prevention systems	14%	17%	12%
DDoS solutions	11%	12%	11%
Governance solutions (GRC)	8%	15%	3%
Anti-virus/anti-malware	8%	8%	9%
Anti-APTs and zero day threats	7%	9%	4%
Total	500%	500%	500%

About Scalar

Scalar is Canada's leading IT solutions integrator, focused on security, infrastructure, and cloud. Founded in 2004, Scalar is headquartered in Toronto, with offices in Montreal, Ottawa, London, Winnipeg, Calgary, Edmonton, and Vancouver. Scalar was recently named to the CRN Fast Growth Top 150 List and listed on the PROFIT 500 for the sixth year running. In addition, Scalar was deemed a Major Player in the IDC MarketScape for Canadian Managed Security Service Providers and ranked the #1 ICT security company on the 2014 and 2015 editions of the Branham 300.

For further details, visit www.scalar.ca or follow Scalar on Twitter, @scalardecisions.

About Ponemon Institute

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Their 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), Ponemon uphold strict data confidentiality, privacy and ethical research standards. They do not collect any personally identifiable information from individuals (or company identifiable information in their business research). Furthermore, they have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.

Research independently conducted by Ponemon Institute LLC | Published February 2016