The Cyber Security Readiness of Canadian Organizations

RESULTS OF THE 2018 SCALAR SECURITY STUDY

scalar

Contents

PART ONE

EXECUTIVE SUMMARY

The annual cost to recover from breaches averages

$3.7 MILLION in direct and indirect costs per organization.

PART ONE

EXECUTIVE SUMMARY

The fourth annual study of the cyber security readiness of Canadian organizations has found IT departments at a tipping point. The consequences of being unprepared for a breach now greatly outweigh the costs of a well-managed security program. Based on the findings, IT departments can expect that security breaches are the new normal. The average company finds itself under attack by hackers more than once a day. Eighty seven percent of responding organizations suffered at least one successful breach in the past 12 months. The cost to recover from these breaches averaged $3.7 million in direct and indirect costs per organization.

As attacks become more frequent and more costly, Canadian organizations are taking IT security increasingly seriously across critical areas like staffing, budget, and identification processes. However, key cyber security weaknesses still exist, including:

- Understanding exposure and vulnerabilities
- Security training for employees
- Speed of installing security updates and patches
- Security incident response planning

Firms also face organizational blind spots about risk areas, with the top concerns being:

- Exposure to insider threats from employees or contractors
- Getting the organization to conduct regular cyber security risk assessments and audits
- Inability to identify the threats that could jeopardize infrastructure and data

Segmenting the results of the survey by organization size and using the National Institute of Standards and Technology (NIST) cyber security framework to help analyze the results allowed several key lessons to emerge:

- Larger organizations are attacked and breached significantly more often than smaller organizations
- Smaller organizations suffer more high impact breaches than larger organizations
- Due to the difficulty in assessing business impacts, many small and medium/large organizations may not understand what security solutions to deploy for the greatest return on their security investment
- Exposure and vulnerabilities are often highly underestimated because security planning does not adequately account for external relationships such as those with suppliers or partners
- Security training for employees is deficient
- Speed of installing security updates and patches is inadequate and does not prioritize which updates or patches are most important if a comprehensive threat and risk assessment has not been conducted
- Response planning lacks documentation and regular updating

Canadian organizations are reporting an average of

455

attacks last year.
That's more than one attack each day.

PART TWO

INTRODUCTION AND METHODOLOGY

The average cost of a breach per employee is

$12,392*

*In smaller organizations.
The cost per employee in large organizations is $755.

PART TWO

INTRODUCTION AND METHODOLOGY

This report represents the findings of the 2018 Scalar Security Study. Independently conducted by IDC Canada, the data provided in this report was obtained through a Canada-wide cross-industry survey of 421 IT security and risk & compliance professionals. All survey participants were screened for direct involvement in improving or managing their organization's IT security. Sixty-two percent of the IT security respondents were at a supervisor level (Infosec Supervisor/IT Supervisor) or higher. Survey respondents were screened to represent organizations with a minimum of 15 full-time employees and at least 10% of their total employees located in Canada.

The survey is meant to provide insight into the big questions facing IT security departments:

- How large is the threat of attack facing Canadian organizations?
- How expensive are cyber security breaches getting?
- What weaknesses still need to be addressed?
- How prepared are organizations to respond to security breaches?
- What technologies or processes can organizations implement to improve their cyber defences?

The survey was conducted over the course of November-December 2017 by IDC Canada on behalf of Scalar. The Appendix shows a detailed description of the demographics and firmographics of the survey participants.

Organization Size Segmentation

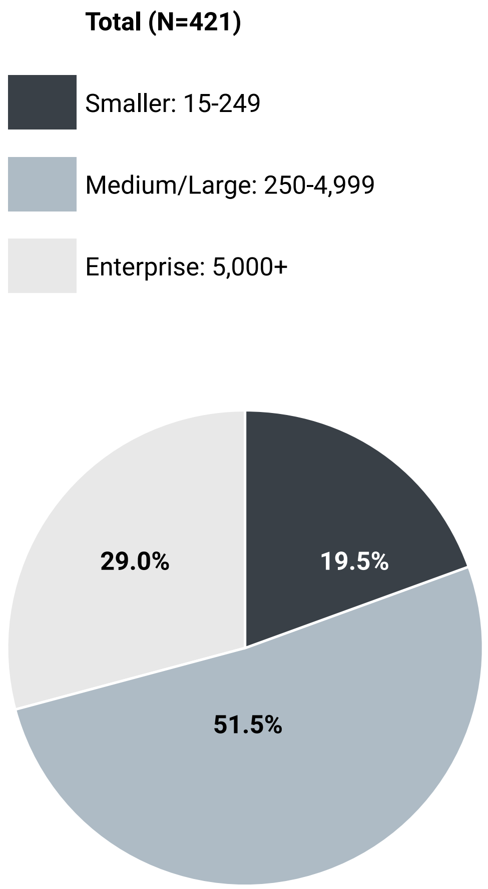
In this report, Scalar classifies responding organizations as Smaller, Medium/Large, and Enterprise class organizations. The definition for each is based on its number of employees:

- Smaller: 15-249 full-time employees located within Canada
- Medium/Large: 250-4,999 full-time employees located within Canada
- Enterprise: 5,000+ full-time employees located within Canada

The NIST cyber security framework is widely used as a base for developing organizational information security strategy. Survey respondents were asked several questions representing the core aspects of the NIST framework in order to help analyze the security maturity level of Canadian organizations:

- Identify
- Protect
- Detect
- Respond
- Recover

PIE CHART 1. *Classification based on Organization Size*



Only

26%

of respondents across organization sizes conduct formal training for employees

PART THREE
KEY FINDINGS

PART THREE
KEY FINDINGS

In this section, we analyze the key findings of the research. The complete audited findings are presented in the Appendix of this report. A summary of the key findings is as follows:

Cyber security threats are omnipresent and costly to the bottom line

- Many organizations face more than one attack per day and suffer multiple breaches per year
- Of the organizations that suffered a breach, 47% had sensitive customer or employee data stolen
- The recovery cost of a breach averages $3.7 million per organization in direct and indirect costs
- Organizations expect to be breached, but many are not fully confident in their ability to deal with it

Organizations face risk regardless of size

- Smaller organizations have more high impact security incidents and a much higher cost of breaches per employee ($12,392) than larger organizations ($755)
- Larger organizations are attacked and breached significantly more often than smaller organizations

Canadian organizations are beginning to take IT security more seriously

- Full-time staff devoted solely to IT security are being employed, even at Smaller organizations
- A strong majority are performing core NIST processes, but not enough are conducting them across their entire organization. This negatively impacts the comprehensiveness of Threat Risk Assessments (TRAs) and creates gaps in security effectiveness

Traditional key weaknesses still need to be addressed

- Exposure and vulnerabilities are often underestimated because planning does not adequately account for third-party relationships and connections to suppliers, partners, and external vendors
- Security training for employees is deficient
- Speed of installing security updates and patches is inadequate and will not prioritize which updates and patches are most important if a comprehensive TRA has not been conducted
- Response planning lacks documentation and regular updating

Many firms could benefit from external expertise

- Smaller organizations have a problem with security effectiveness: one-fifth rate their security resources as ineffective at protecting against attacks
- Addressing issues such as insider threat, cloud security, threat identification, establishing regular security assessment cycles, and preventing theft of customer data are the key priorities
- External security services with solution, technology, and process expertise can efficiently supplement in-house security departments
- New security technologies can help address many of the security effectiveness issues organizations have

FINDING ONE: THE OMNIPRESENT THREAT OF A CYBER ATTACK

On average, responding organizations were attacked more than 450 times per year, resulting in an average of 9.33 breaches per organization per year. Of those breaches, more than 20% were high impact incidents, such as a major breach where highly sensitive data has been exposed. Almost 80% were low impact incidents, such as non-targeted malware, drive-by downloads, or ransomware on only a few devices.

TABLE 1. *Number of attacks and breaches (high and low impact) organizations have been subject to over the past twelve months*

Means	TOTAL
Base: All Respondents	(421)
TOTAL number of attacks	454.75
TOTAL number of breaches	9.33
# of High Impact incidents (eg. major breach – highly sensitive data exposed, targeted attack, etc.)	1.9 = 20.4% of total breaches
# of Low Impact incidents (eg. minor incident - drive by download, ransomware on only a few devices, non-targeted malware, etc.)	7.43 = 79.6% of total breaches

Security breaches expose companies to big losses

Eighty-seven percent of respondents suffered at least one cyber security breach in the past 12-months. Respondents provided feedback on the direct and indirect costs of a security breach, including lost revenue.

Of the organizations that have suffered security breaches:

- The average cost per organization surveyed is $3.7 million. This cost includes:
  - $3.5 million in cost of lost revenue and profitability incorporating:
    - Network/infrastructure/end-user downtime (58% suffered network/infrastructure/end-user downtime – on average 3.75 days, or 90 hours, of cumulative downtime per organization)
    - Employee work days expended recovering from breaches (average 16 employee work days per organization)
    - Files and records compromised (83% had files/records affected - on average more than 1,900 files were affected per breached organization)
    - Sensitive data compromised (47% had sensitive data involved in their breaches – with almost one quarter involving customer or employee PII (personally identifiable information), and more than half involving sensitive/proprietary but non-PII business data)
  - $215,080 per organization in direct dollars expended addressing the breaches

TABLE 2. *Number of attacks and breaches (high and low impact) organizations have been subject to over the past twelve months*

		Organization Size		
	TOTAL	Smaller	Medium/Large	Enterprise
Base: All Organizations That Were Subject To Breaches Over The Past Twelve Months	(367) = 87.2%	(67) = 81.7%	(189) = 87.1%	(111) = 91.0%
Lost revenue	$3,299,057	$1,076,481	$4,223,908	$3,361,860
Lost profit	$164,952	$53,824	$211,195	$168,092
Direct dollars expended addressing breaches	$215,081	$53,600	$255,732	$243,334
TOTAL	**$3,679,090**	**$1,183,905**	**$4,690,836**	**$3,773,287**
Cost of breaches per employee	$1,733	$12,392	$3,690	$755
Cumulative hours of downtime for organizations that suffered downtime	90 hours	59 hours	101 hours	83 hours
Employee work days expended recovering from breaches	16 work days	10 work days	18 work days	16 work days
Average number of files or records compromised for organizations where files/records were affected	1,908	1,069	2,028	2,019
Percent of files that contained sensitive data	47%	61%	46%	41%

Organizations expect to be breached, but many are still not adequately prepared

When asked how confident they are in their organization's ability to prevent cyber security breaches from happening, only 5% of survey respondents had a "high" degree of confidence. 51% were confident, but not to the highest degree. Despite being subject to more cyber attacks than Smaller organizations, Medium/Large organizations and Enterprise are much more confident in their ability to prevent breaches from happening.

TABLE 3. *How confident are you in your organization's overall ability to prevent cyber security breaches from happening?*

		Organization Size		
	TOTAL	Smaller	Medium/Large	Enterprise
Base: All Respondents	(421)	(82)	(217)	(122)
Highly confident	5%	6%	3%	8%
Confident	51%	16%	61%	56%
Neutral	38%	66%	29%	34%
Not confident	6%	12%	6%	2%
Not at all confident	0%	0%	0%	0%

While larger organizations are more confident in their security measures, the sheer volume of attacks leaves them vulnerable to a breach. Smaller organizations have low confidence in their ability to prevent breaches, which may speak to the amount of resources they can allocate to cyber security preparedness.

Once breaches have happened, a significant percentage of respondents have a neutral or even negative level of confidence in their organization's ability to effectively respond. Smaller organizations are much less confident they can prevent a breach from occurring in the first place, but their confidence levels align more closely with larger organizations when it comes to detecting and responding to breaches once they have happened.

TABLE 4. *How confident are you in your organization's overall ability to detect and respond to cyber security breaches once they have happened?*

			Organization Size	
	TOTAL	Smaller	Medium/Large	Enterprise
Base: All Respondents	(421)	(82)	(217)	(122)
Highly confident	11%	9%	11%	12%
Confident	53%	48%	55%	54%
Neutral	31%	41%	25%	34%
Not confident	5%	2%	8%	0%
Not at all confident	0%	0%	0%	0%
Cost of breaches per employee	$1,733	$12,392	$3,690	$755

Scalar's experience is that Smaller organizations find it harder to implement tools and processes that prevent breaches than to implement tools and processes that detect and respond to them. This is primarily because of limited budget and resources, but it is important for Smaller organizations to find a means of reducing the amount of breaches they suffer, because per employee, they get very expensive. Meanwhile, Larger organizations have difficulty understanding the impact of breaches because of the amount of attacks and breaches they are subject to; negatively affecting their confidence in their ability to respond.

Survey respondents were asked about total number of attacks and total number of breaches.
ATTACK: An attempt to damage, disrupt, or gain unauthorized access to a computer, computer system, or electronic communications network.
BREACH: Successful attempts.

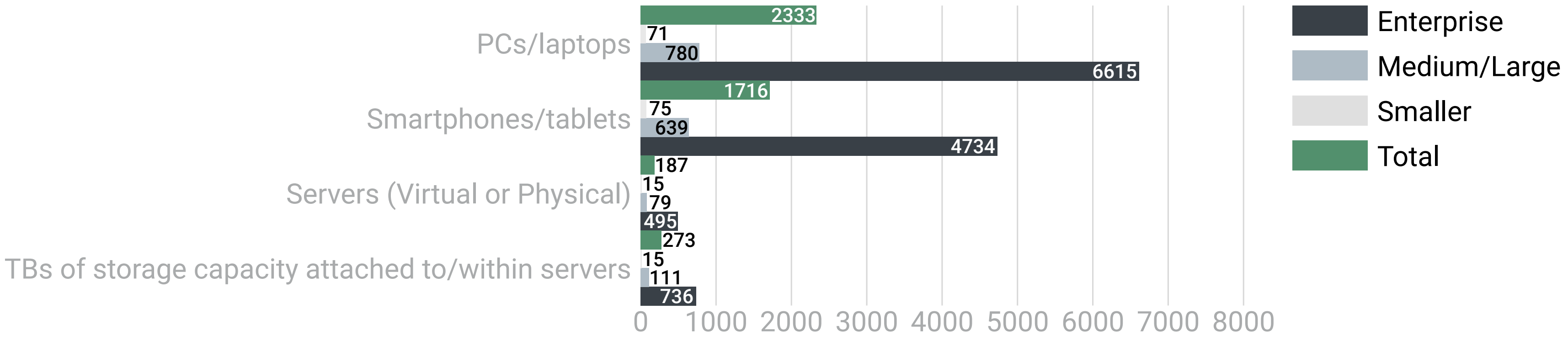
FINDING TWO: ORGANIZATIONS FACE RISK REGARDLESS OF SIZE

When it comes to cyber security threats, size doesn't matter. Larger organizations are attacked, and breached, significantly more often than their smaller counterparts. But smaller organizations experience more high-impact incidents, and it costs them. High impact incidents, such as breaches that result in stolen data, cost small organizations $12,392 per employee on average, compared to $755 per employee at larger organizations. Regardless of size, organizations face serious cyber threats from malicious actors.

Threat surface increases exponentially with an organization's size

Threat surface is the potential exposure of an organization's devices, data, and networks to security vulnerabilities. In this study, threat surface was estimated by asking respondents for their networked device and hardware counts; and for information on what percentage of their organization's business activity is conducted through the web.

FIGURE 1. *Threat/attack surface in terms of average number of networked devices/hardware increases exponentially as an organization's size increases. This is demonstrated consistently in the survey results across all device and hardware types:*

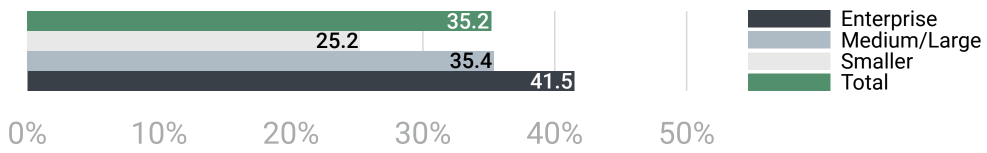


THREAT RISK ASSESSMENT

Assess your risk by conducting a comprehensive Threat Risk Assessment (TRA), and develop and implement a security plan based on the TRA – and your organization will have less data stolen and will suffer less downtime.

Large organizations are more likely to manage their own infrastructure to conduct online business (see Figure 2). Keeping infrastructure in-house, combined with the challenges of keeping patches up-to-date (which is explained in findings later in the study), puts larger organizations at more significant risk of being breached. This appears to be strongly supported by recent high profile breaches caused by inadequately patched, web-facing infrastructure being compromised.

FIGURE 2. *What percentage of your organizations' business activity is conducted via website maintained by your organization?*



INCIDENT RESPONSE PLAN

Make an Incident Response plan, you'll need it – and you'll need to update it. Even large organizations with sophisticated security plans can't be complacent. Recent headlines have proven the need for constant evaluation to ensure cyber security measures are up-to-date.

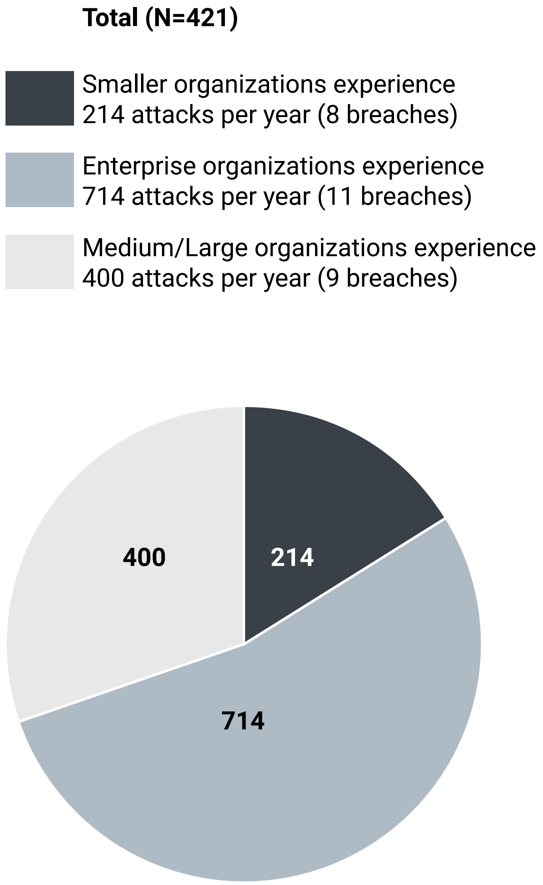
Larger organizations are attacked and breached significantly more often

The total number of attacks and breaches reported is significantly higher for Enterprise class organizations. The total number of attacks increases 234% from Smaller-to-Enterprise; and the total number of breaches increases by a third.

TABLE 5. *Please estimate how many attacks and breaches your organization has been subject to over the past twelve months:*

		Organization Size		
Means	TOTAL	Smaller	Medium/Large	Enterprise
Base: All Respondents	(421)	(82)	(217)	(122)
TOTAL number of attacks:	454.75	213.83	399.88 (87% increase from Smaller) 234% increase	714.26 (79% increase from Medium/Large; from Smaller)
TOTAL number of breaches:	9.33 = 2.1% of attacks	8.1 = 3.8% of attacks	8.98 = 2.2% of attacks and 11% increase from Smaller	10.77 = 1.5% of attacks and 20% increase from Medium/Large; 33% increase from Smaller

PIE CHART 2. *Classification based on Attacks per year*



Just because an organization is smaller in size doesn't mean it faces less risk

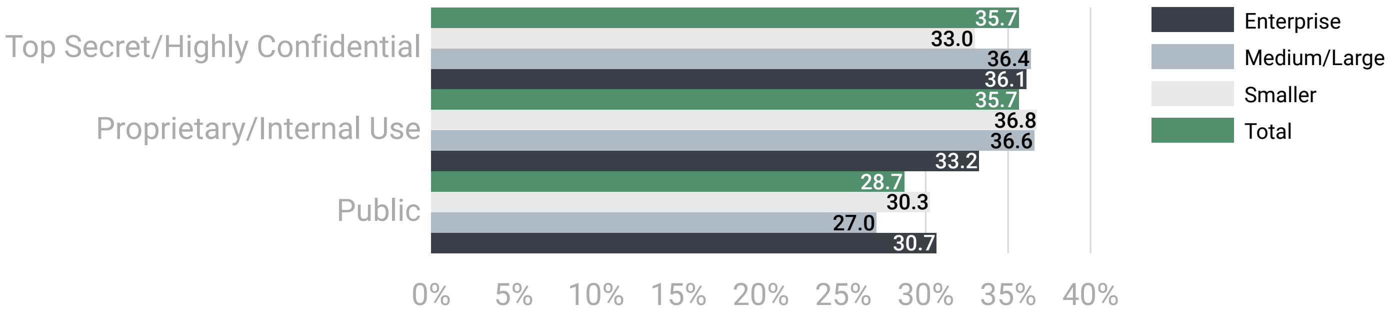
- Smaller organizations have more high impact security incidents even though their attack surface is smaller
- Smaller organizations' data is just as critical as larger organizations', and therefore equally as important to secure

Smaller organizations have more high-impact security incidents which drives their cost of breaches per employee higher
Being smaller in size doesn't mean an organization faces less risk. Despite being attacked and breached less often, Smaller organizations suffer more high impact security incidents than Larger organizations. Because attacks against Smaller organizations are more likely to result in a costly high impact breach, it is imperative that they invest in improving security defences to help reduce the total number of breaches they suffer.

Despite facing fewer attacks and breaches, Smaller firms suffer more high impact security incidents, leading to a much higher cost per breach per employee. This indicates that their security risk is no less severe, and may be even greater, than for Medium/Large or Enterprise firms.

Smaller organizations can't be complacent. They face serious cyber risks if they haven't implemented a thorough and well-maintained security program.

FIGURE 3. *Large or small, an organization’s data is critically important*
The percentage of business data that is Top Secret/Highly Confidential and Proprietary/Internal Use is similar between all organization sizes.



Regardless of size, organizations can’t be complacent when it comes to cyber security. Large organizations face daily attacks, and small organizations face a greater risk of high impact breaches. Assess your exposure by conducting a comprehensive TRA, and use the findings to develop and implement a security plan. That will help to protect important data and prevent costly downtime. However, security breaches have become the new normal, so you’ll need to have an incident response plan. Even large organizations with sophisticated security programs need to have a plan in place for when breaches occurs, and that plan needs to be updated regularly. Recent headlines prove the importance of constantly evaluating and updating your cyber security measures.

Think beyond your walls. Consider not just how attackers can get into your organization, but how they can breach your suppliers, partners, and external vendors as well.

FINDING THREE: CANADIAN ORGANIZATIONS ARE BEGINNING TO TAKE SECURITY MORE SERIOUSLY

The rising costs related to cyber security breaches seem to be getting the attention of Canadian firms. Even smaller organizations are hiring full-time staff devoted to IT security, and a strong majority of organizations are performing core NIST processes. However, some organizations are failing to conduct Threat Risk Assessments across their entire operation, which creates gaps in the effectiveness of their security plans. When it comes to cyber security preparedness, organizations can't settle for half-measures.

Enterprise organizations employ ten full-time staff devoted solely to IT security; even Smaller organizations are employing fully dedicated IT security staff

Canadian organizations are beginning to take cyber security threats more seriously. Even Smaller organizations are employing, on average, one fully dedicated IT security headcount. At Medium/Large organizations, headcount fully dedicated to IT security expands to three security professionals, and further increases to ten full-time security professionals at Enterprise-class organizations.

TABLE 6. *Security accounts for approximately 10% of total IT budgets*

With more than 10% of total annual IT budget being devoted to security, it becomes more important to optimize expenditures within the framework of prepare, defend, and respond against threat. This can be done by investing in the right tools, threat and risk assessment, and roadmapping of security plans.

			Organization Size	
Means	TOTAL	Smaller	Medium/Large	Enterprise
Base: All Respondents	(421)	(82)	(217)	(122)
How many full-time employees does your company have located within Canada?	2122.86	95.54	1271.39	5000
How many IT security staff (fully devoted to IT security) are employed at your organization?	4.61	1.07	2.94	9.94
Estimated total annual IT budget (eg. staff, hardware, software, services) of your organization ($M):	$12.5M	$8.2M	$11.4M	$17.3M
Percentage of total annual IT budget devoted to security?	10.1%	9.5%	10.1%	10.5%

An analysis of the survey results using the National Institute of Standards and Technology (NIST) framework shows that a strong majority of organizations are performing core NIST processes

The "Identify" portion of the NIST framework deals with basic security identification processes that help identify exposure to vulnerabilities, the business impact of security incidents, and what solutions should be prioritized for deployment.

Survey respondents were asked how they conduct four basic security identification processes intended to represent the Identify portion of the NIST framework:

- Taking inventory of applications, devices, and systems
- Assessing security vulnerabilities across applications, devices, and systems
- Assessing the business impact of data loss and disruption of work
- Prioritizing deployment of specific security solutions to address key vulnerabilities

It's a positive sign that a strong majority of organizations are performing all four processes: but not enough organizations are conducting them across their entire operations. This erodes the comprehensiveness of their Threat Risk Assessments, and creates gaps in their security strategy and effectiveness.

TABLE 7. *Although high percentages of organizations conduct these processes, not enough conduct them across their entire organization which leads to gaps in security strategy and effectiveness:*
Percent of organizations that conduct the following processes

		Organization Size		
Percent of organizations who **DO NOT** conduct this process	TOTAL	Smaller	Medium/Large	Enterprise
Base: All Respondents	(421)	(82)	(217)	(122)
Taking inventory of applications, devices, and systems				
Conduct the process	96%	94%	98%	96%
Conduct it across their entire organization	43%	43%	40%	48%
Discovering/assessing security weaknesses/vulnerabilities across applications, devices, and systems				
Conduct the process	98%	95%	98%	100%
Conduct it across their entire organization	69%	48%	73%	77%
Assessing the business impact of data loss/corruption, disruption of work				
Conduct the process	87%	87%	83%	94%
Conduct it across their entire organization	31%	40%	27%	32%
Prioritizing deployment of specific security solutions (to address key weaknesses/vulnerabilities)				
Conduct the process	85%	89%	79%	92%
Conduct it across their entire organization	29%	35%	28%	27%

Canadian organizations are making strides in their cyber security preparedness. Spending is increasing, and even small organizations are employing full-time staff devoted solely to IT security. Firms are beginning to recognize the large costs that stem from ineffective security planning. However, it's not enough to simply implement measures. Many Smaller and Medium/Large organizations could benefit from further analysis of their current system and how to improve it. The best protection requires consistent auditing and updating.

FINDING FOUR: TRADITIONAL KEY CYBER SECURITY WEAKNESSES STILL NEED TO BE ADDRESSED

While no security system is completely impenetrable, many organizations still have key security weaknesses that leave them unnecessarily exposed. Firms often underestimate their true risk exposure and vulnerabilities, because they don't account for third-party relationships with suppliers, partners, and external vendors. They also fail to appreciate the risk from employees. Despite the fact that employees are often the easiest target for hackers, many organizations fail to provide sufficient training. Organizations also fail to install security patches in a timely manner, or fail to prioritize which updates are most important. Finally, many firms don't have processes in place to regularly update their incident response plans. While Canadian companies have made progress in their cyber security strategies, they still have work to do in planning, updating, and responding to threats. Organizations will feel more confident in their cyber security as they implement more comprehensive systems.

Vulnerabilities are often underestimated because security planning fails to account for third party relationships (suppliers, partners, and external vendors)

Continuing with the NIST framework, analyzing an organization's complete business - including external relationships with suppliers, partners, and third parties - is a crucial part of identifying its true exposure. Survey respondents were asked whether their security planning includes external sources of exposure. See table 10. Close to three quarters of the organizations surveyed do not consider external relationships in a comprehensive manner in their security planning. For example, there have been instances of massive breaches at Fortune 500-scale companies caused by hackers breaking into corporate networks using login credentials stolen from third parties, such as property or facilities management companies.

TABLE 8. *Does your security planning consider your key suppliers and third-party relationships, and the data flows between you and them?*

		Organization Size		
	TOTAL	Smaller	Medium/Large	Enterprise
Base: All Respondents	(421)	(82)	(217)	(122)
YES – in a comprehensive manner	26%	29%	25%	26%
YES – but we should look at this in more detail	60%	62%	56%	66%
NO	11%	9%	16%	4%
Not sure/don't know	3%	0%	3%	3%

Build employee security awareness. Employees are one of any organization's weakest security links, but too often organizations fail to sufficiently train and educate them on security risks and proper handling of sensitive data.

Security training for employees is deficient

Survey respondents were asked how they train employees in four basic security areas to represent the “Protect” portion of the NIST framework:

- Updating PC and smartphone OS and apps
- How to use security technology
- How to identify attacks such as phishing and other scams
- Proper care of sensitive data

A significant percentage of respondents conduct formalized training in only two of the four areas. This leaves organizations vulnerable, as employees are both a primary target and cause of security incidents (eg. improper handling of customer data), and organizational insiders are a major source of breaches:

- Training on how to identify attacks such as phishing and other scams is highly deficient. Employees are the primary target of attackers, and ensuring they are aware of threats should be an IT security priority. Only 26% of respondents across organization sizes conduct formal training for employees
- Training on proper care of sensitive data, such as customer or employee private information is deficient. Considering the business impact of breaches involving sensitive data, and that employees are a common target for attacks, proactive training regarding personal information should be a priority for IT security departments

TABLE 9. *Which of the following best describes how your organization trains employees on the following?*
Formalized security training is deficient in key areas of risk

			Organization Size	
Formal versus ad hoc or no training	TOTAL	Smaller	Medium/Large	Enterprise
To frequently update PC and smartphone OS and apps:				
Formal training with reminders as required by new threats	29%	48%	24%	25%
Ad hoc or no training	71%	52%	76%	75%
How to use security technology:				
Formal training with reminders as required by new threats	66%	51%	68%	72%
Ad hoc or no training	34%	49%	32%	28%
How to identify attacks such as phishing and other scams:				
Formal training with reminders as required by new threats	26%	40%	22%	25%
Ad hoc or no training	74%	60%	78%	74%
Proper care of sensitive data such as customer/other employee private data:				
Formal training with reminders as required by new threats	59%	43%	60%	70%
Ad hoc or no training	41%	57%	40%	30%

Speed of installing security updates and patches is inadequate and will not prioritize which updates and patches are most important if a comprehensive threat and risk assessment has not been conducted

Survey respondents were asked how long it takes them to implement security updates (including critical patches) across the following device, hardware, network, and infrastructure areas to represent the "Protect" portion of the NIST framework:

- PCs
- Smartphones
- On-premise databases, apps, servers
- Web applications
- Network equipment
- Public cloud (IaaS/PaaS)

Outside of PCs and smartphones, the majority of organizations surveyed install critical security updates within a month or even a year or longer. The lack of speed in updating web applications and IaaS and PaaS is especially concerning in terms of increasing security vulnerability because of the amount of threat exposure in these areas. With the delayed patching problem extending across all organization sizes and IT areas other than PCs and smartphones, it is a pervasive cyber security weakness.

Given the difficulties IT departments can have with patching because of the sheer number of patches, legacy infrastructure that can't be patched, or low tolerance for downtime, it is a key area where outside expertise can help. External security firms can help in-house teams identify and prioritize updates from a comprehensive threat and risk assessment perspective. Outside expertise can also help alleviate problems with the patching process itself, and significantly increase the speed of installing critical updates.

Patch and update quickly.
One of the easiest and most effective security protections is simply updating your software.

Patching is a key area of cyber security weakness that extends across all organization sizes and almost all devices, hardware, and infrastructure areas. Delays in installing critical security updates for a month - or year, or even longer – significantly increase security vulnerabilities.

TABLE 10. *How long does it take your organization to install security updates/patches (including critical updates/patches)?*

		Organization Size		
Percent	TOTAL	Smaller	Medium/Large	Enterprise
Base: All Respondents	(421)	(82)	(217)	(122)
PCs:				
Within a week	70	49	82	63
Within a month	26	40	15	36
Within a year or longer	4	11	3	1
Smartphones:				
Within a week	87	72	89	92
Within a month	11	27	9	5
Within a year or longer	2	1	2	3
On-premise databases, apps, servers:				
Within a week	13	24	11	8
Within a month	71	54	74	80
Within a year or longer	15	22	15	12
Web applications:				
Within a week	11	18	13	5
Within a month	30	38	29	27
Within a year or longer	59	44	58	68
Network equipment:				
Within a week	12	20	11	9
Within a month	59	47	62	63
Within a year or longer	29	33	27	28
Public cloud (IaaS/PaaS):				
Within a week	12	29	10	6
Within a month	22	32	19	19
Within a year or longer	66	39	71	75

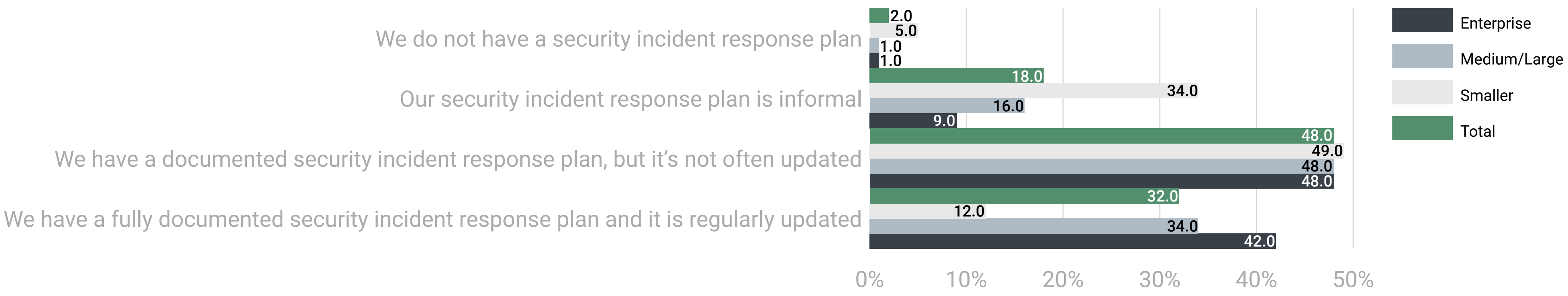
Response planning lacks documentation and regular updating

Survey respondents were asked how they would best describe their organization’s security incident response plan to represent the “Respond and Recover” portion of the NIST framework. Four responses representing low maturity (no/informal plan), mid-level maturity (documented but not often updated) and high maturity (fully documented and regularly updated) were allowed:

- We do not have a security incident response plan
- Our security incident response plan is informal
- We have a documented security incident response plan, but it’s not often updated
- We have a fully documented security incident response plan and it is regularly updated

An organization’s security incident response plan represents its blueprint for recovering from security breaches and incidents. As the basis for recovering from potentially high impact breaches, only a fully documented plan that is regularly updated is truly adequate. While the survey results suggest organizations are aware that an incident response plan is required (only two percent do not have a plan), the effectiveness of plans that are not fully documented and regularly updated will be sub-optimal and create unnecessary business risk.

FIGURE 4. *The majority of organizations, even Enterprise-scale, do not have a fully documented, regularly updated security incident response plan in place.*



Canadian organizations are taking the threat of cyber security breaches more seriously, but there is still work to be done. Firms need to think beyond their walls, and consider the risks posed by suppliers, partners, and external vendors. Employees need to be adequately trained to spot security risks and properly handle sensitive data. Security updates need to be consistently applied as an easy and effective line of defence. No system can be completely secure, but there is a large opportunity for Canadian firms to reduce the gaps in their cyber security program.

FINDING FIVE: MANY FIRMS COULD BENEFIT FROM EXTERNAL EXPERTISE

Cyber security threats are becoming more sophisticated, and organizations need to keep up. One-fifth of Smaller firms say their resources are ineffective at protecting against attacks. Organizations are concerned about insider threats, cloud security, and theft of customer data. Tapping external expertise may be the most efficient way to close these gaps. Bringing in outside security services with solution, technology, and process experience can supplement in-house security departments.

Smaller organizations have a problem with security effectiveness: one-fifth rate their security resources as ineffective at protecting against attacks
When asked to rate the effectiveness of their security resources (people, technology, and process), there was a clear, statistically significant gap in the effectiveness ratings of smaller versus larger organizations. The gap was across all three resource areas:

- Smaller organizations clearly lag larger organizations in perceived effectiveness of their security resources.
- Compared to Medium/Large and Enterprise, Smaller organizations face a resource gap in areas such as tools, IT security staffing levels, expertise in threat and risk assessment, and specialized security solution knowledge. External support can be an efficient way for Smaller organizations to close the security gap.
- Smaller organizations are much more likely to rate their security resources as ineffective.

TABLE 11. *How effective are each of the following at protecting your organization from security attacks?*
Respondents who rate the following security resources as ineffective

			Organization Size	
	TOTAL	Smaller	Medium/Large	Enterprise
Base: All Respondents	(421)	(82)	(217)	(122)
Internal IT/security staff	8%	23%	5%	3%
Security technology we have currently deployed	7%	18%	6%	2%
Our security risk and incident response process	9%	22%	8%	1%

Be wary of new and old threats alike. Old attacks don't go away. All threats, no matter how old they are grow in sophistication and their ability to adapt to existing defences. They can always return to attack you.

Addressing issues such as insider threat, cloud security, threat identification, establishing regular security assessment cycles, and preventing theft of customer data are the key priorities
The top overall security concerns and top concerns in implementing a security plan of organizations responding to the survey are consistent across organization size indicating they are key security priorities throughout the Canadian market.

TABLE 12. *The top overall security concerns are consistent across organization size, and are the key security priorities throughout Canada.*

- Insider threat
- Cloud security
- Public exposure of customer data

Please rate how concerned you believe your organization is with each of the following:

			Organization Size	
	TOTAL	Smaller	Medium/Large	Enterprise
Base: All Respondents	(421)	(82)	(217)	(122)
Insider/malicious employee threat	63%	73%	60%	61%
Cloud security	63%	72%	62%	59%
Public exposure of customer data	62%	72%	62%	57%
Data not being backed up	40%	30%	38%	48%
IoT security	37%	12%	45%	39%
Security related downtime of business-critical IT resources	34%	23%	35%	40%
Mobile threats	28%	29%	27%	29%
Hacktivism	21%	24%	19%	22%
State Sponsored Attacks	19%	12%	23%	18%
Ransomware	15%	12%	14%	19%

Think of newer technologies that can increase your security effectiveness
like Breach Detection, Response and Recovery tools, and Threat Intelligence services.

The top concerns in implementing a security plan are also shared across organization size:

- Exposure to insider threats from employees or contractors
- Getting the organization to conduct regular cyber security risk assessments and audits
- Not being able to identify threats that could jeopardize infrastructure and data

Finding and recruiting qualified staff and obtaining adequate budget rank last among security concerns.
This is consistent with the survey findings that Canadian organizations are taking IT security seriously from a staffing and budget perspective.

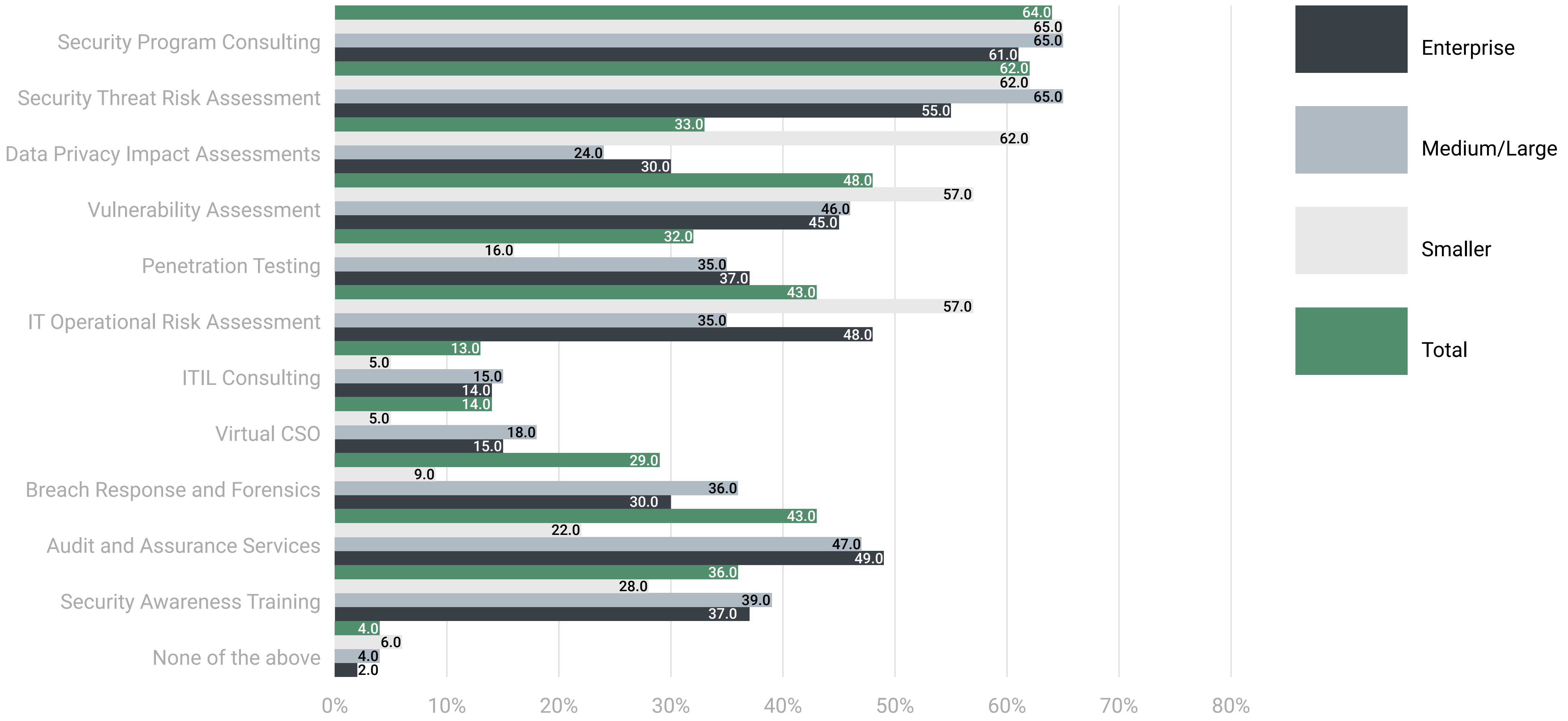
TABLE 13. *Do you have concerns in any of the following areas regarding implementing a security plan for your organization?*

		Organization Size		
	TOTAL	Smaller	Medium/Large	Enterprise
Base: All Respondents	(421)	(82)	(217)	(122)
Exposure to insider threats from employee or contractors	71%	80%	70%	69%
Getting the organization to conduct regular cyber security risk assessments and audits	71%	78%	71%	68%
Not being able to identify the threats that could jeopardize infrastructure and data	67%	80%	65%	64%
Business executives and managers taking responsibility for cyber security and sponsoring appropriate action to protect the organization	51%	56%	52%	45%
Obtaining cooperation between business and IT on security planning	49%	55%	48%	45%
Not having enough operational personnel to meet security objectives	48%	71%	45%	37%
Achieving organization-wide implementation and compliance with your security plan	46%	62%	40%	46%
Not being able to protect against sophisticated Advanced Persistent Threats even if they are identified	26%	24%	24%	30%
Finding and recruiting qualified security staff	17%	17%	18%	16%
Obtaining adequate budget	9%	6%	8%	11%

External security services with solution, technology, and process expertise can efficiently supplement in-house security departments in many of these areas
Programs, services, and expertise are available from external security service providers that can help organizations' in-house security departments address key priorities and concerns such as:

- Insider threat
- Cloud security strategy planning and deployment
- Threat identification
- Best practices for getting the buy-in to drive regular security assessment and audit cycles and experts to help conduct assessments and audits
- Experts at establishing data handling protocols and processes to help prevent public exposure of customer data (remembering that poor internal/employee data practices/hygiene are often to blame)

FIGURE 5. *Examples of the external security services used by the organizations surveyed*



New security technologies can help address many of the security effectiveness issues organizations have

When asked to select the security tactics that were most effective, survey respondents focused on traditional methods. See Table 15. The five most effective security technologies as selected by survey respondents were:

- Data Security (encryption, etc.)
- Network Security (NGFW)
- Email Security
- Security Monitoring (SIEM, log management)
- Traditional Endpoint Protection

The study did not ask respondents to explain why these specific technologies were most effective for them, but the focus on traditional technologies indicates a need to be more progressive and look at new technologies such as Threat Intelligence that can significantly increase security effectiveness, especially in Smaller organizations who lack confidence in their ability to prevent breaches from happening in the first place.

Security Awareness Training's selection close to the top 5 is important to note, as it emphasizes the need to address employee-based security risk and insider breach threat.

Breach Response and Forensics Tools also come in near the top 5 for Enterprise. Enterprise-scale firms are also much more likely than Smaller and Medium/Large organizations to have a fully documented and regularly updated incident response plan. These tools help provide detailed information that allows response plans to be kept up-to-date with current threats.

Good leadership enables effective cyber security. By creating an environment that prioritizes IT security, good leadership makes it easier to implement and enforce security processes, and invest in newer security technologies and tools such as Threat Intelligence.

The five security tactics selected as most effective at protecting against threats were the same across all organization sizes.
However, Smaller organizations' perception of security technology effectiveness outside of their top five is significantly lower than that of Medium/Large and Enterprise.

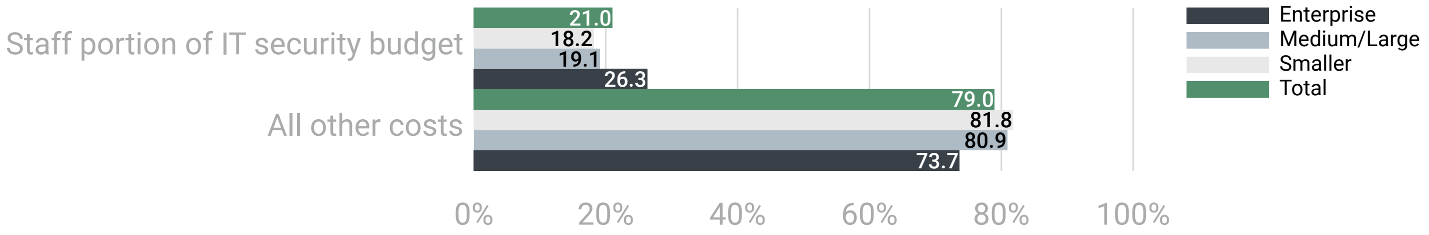
TABLE 14. *From the list below, please select the five technologies or tactics you feel have been the most effective at protecting your organization from cyber security threats over the past year:*

			Organization Size	
	TOTAL	Smaller	Medium/Large	Enterprise
Base: All Respondents	(421)	(82)	(217)	(122)
Data Security (encryption, etc.)	62%	68%	60%	59%
Network Security (NGFW)	61%	83%	58%	51%
Email Security	58%	80%	53%	52%
Security Monitoring (SIEM, log management)	54%	79%	50%	43%
Traditional Endpoint Protection	49%	73%	43%	43%
Security Awareness Training	33%	18%	38%	34%
Vulnerability Management	28%	16%	29%	34%
Breach Response and Forensics Tools	27%	10%	29%	36%
Web Content Filtering	24%	17%	29%	20%
Risk and Compliance Automation	23%	5%	27%	27%
Threat Intelligence	21%	11%	20%	30%
DNS Security	20%	15%	22%	21%
Identity and Access Management	18%	7%	18%	25%
Next-gen Endpoint Protection	17%	12%	19%	16%
DDoS Protection (appliance or service)	6%	5%	4%	11%
Other	-	-	-	-

Expertise in evaluating which managed services can be adopted for the greatest improvement in IT security staff efficiency can significantly improve the effectiveness of IT security spending

Since a large portion of IT security spending is staff related, improving staff efficiency will significantly improve response. But organizations' focus on traditional security methods and technologies and the large percentage of organizations who have not yet adopted many external managed security services indicates a lack of in-depth knowledge in the area. Externally provided expertise in evaluating which managed services could be adopted to generate IT security staff efficiencies could be very beneficial for many organizations.

FIGURE 6. *IT staff accounts for a significant portion of IT security budgets – improving IT staff efficiency through selective managed security services adoption could increase the effectiveness of IT security spending*



Only security device management has been adopted by 50% or more of the organizations surveyed. A lack of in-depth knowledge of managed security services offerings and capabilities indicates external expertise could be extremely useful in evaluating which managed services an organization can adopt to generate the most efficiency benefits for IT security staff.

TABLE 15. *Percent of organizations that use the following externally managed security services:*

			Organization Size	
	TOTAL	Smaller	Medium/Large	Enterprise
Base: Respondents Who Use Externally Managed Security Services	(409)	(79)	(209)	(121)
Security Device Management	52%	37%	59%	51%
Managed Threat Intelligence	48%	39%	49%	50%
Managed Data Loss Prevention	46%	35%	53%	43%
Managed Web Application Firewall	45%	41%	44%	49%
Managed Zero-day Endpoint Protection	38%	27%	40%	41%
Vulnerability Management Service	35%	27%	30%	48%
Managed DDoS Prevention	34%	41%	31%	36%
Managed NGFW	32%	32%	31%	34%
Managed SIEM on-premise	31%	27%	33%	31%
Managed SIEM (IaaS) - Cloud	27%	25%	27%	27%

Organizations need to remain vigilant. Old threats can evolve and grow in sophistication. New threats are being created all the time. Firms need to be consistently evaluating new technologies – like Breach Detection, Response and Recovery tools, and Threat Intelligence services – to see how they can fit into an overall cyber security framework. Organizational leadership needs to prioritize IT security and invest in consistent updates. In a constantly changing threat landscape, external expertise can be an efficient way to bridge any gaps in your defences.

PART FOUR
CONCLUSIONS

PART FOUR CONCLUSIONS

The landscape of cyber security in Canada continues to evolve. Attacks are becoming more frequent, sophisticated, and severe. Canadian organizations need to fend off more than an attack per day. Attackers need sensitive data to sell to earn their livelihood. They are getting better at their craft all the time, and able to find a way in through any weak point in a PC, smartphone, cloud service email, web application, network, server, sensor or through lack of employee knowledge. As a consequence, the amount of data being compromised – across all businesses in all industries – is growing. Large mega-breaches, where millions of records are exposed, make the headlines continually. But attackers will settle for dozens of records, too, from breaching smaller organizations.

In Canada, the average cost of a breaches per organization is $3.7 million per year. With mandatory breach notification taking effect this year in Canada – including steep fines for failure to notify customers – these costs are on the rise. Moreover, organizations doing business with EU countries need to be aware of the dramatic fines set out in the General Data Protection Regulation (GDPR). The cost of simply treading water in cyber security is no longer acceptable. Every organization, whether small or large, needs to take action.

Organizations that comply with regulations such as PCI, information security management standards such as ISO 27001, or legislation such as the Digital Privacy Act are far more secure than their peers. Organizations that don't concern themselves with external compliance requirements are two times more likely to have attacks turn into actual breaches and loss. The most likely reason for this is that compliance requirements span a range of security controls from network protection to breach detection to employee training. Although not a compliance regulation itself, the National Institute of Standards and Technology (NIST) Cyber security Framework (CSF) covers the essential elements an organization should follow in developing a security strategy. Another great resource is the SANS Institute Top 20 Critical Controls for Cyber Defense, typically used by organizations seeking compliance.

KEY CALLS-TO-ACTION FOR CANADIAN ORGANIZATIONS

Assess your risk by conducting a comprehensive Threat Risk Assessment (TRA), and develop and implement a security plan based on the results.
Because security budgets are finite, directing dollars proportionally to the most vulnerable spots of the organization is a key to reducing breaches. Without a plan – even a relatively informal one – it's unlikely your budget will be spent in the right places. There are different kinds of security plans. The most important starting point is a risk plan, and it's best to start by assessing risk through a Threat Risk Assessment. Organizations with a security risk plan suffer far fewer breaches than their less prepared peers – up to a 32% lower breach count. It may sound daunting setting up a risk plan, but it's not.

Think beyond your walls.
Organizations need to consider the security of their PCs, smartphones, servers, network, web applications, cloud services, databases and applications. Not just how attackers can get into the organization, but how they can breach your suppliers, partner, and external vendors as well. Any weak point needs to be identified across all attack surfaces. Only 1 in 4 organizations consider the security of their third-party relationships and the data flows between them. This leaves a majority of organizations exposed to additional points of attack.

Be wary of new and old threats alike.
Old attacks don't go away. Surprisingly, organizations are not too concerned with ransomware. This is likely because organizations feel the threat has been dealt with. Not so. Just like the flu and its variations, all threats, including ransomware, grow in sophistication and their ability to adapt to existing defences. They can always return to attack you.

Put the right technologies in place.
Organizations tend to rely on traditional and mostly passive security technologies such as firewalls and signature-based endpoint protection. Put the right technologies in place and have them configured correctly and optimized. Utilizing technologies such as NGFWs, next generation endpoint, and SIEM is important, but they must be deployed in an efficient way. From email to network monitoring, many security solutions are available as through the cloud as a service (SaaS), reducing the on-premise infrastructure and security staff required to secure your business. Not only can you reduce your on-premise footprint, many SaaS based security solutions use the power of the cloud to offer advanced anomaly detection, user behaviour analytics, and machine learning.

Build employee security awareness.
Train staff and remind them of why good security practices are so important. Employees are one of any organization's weakest security links, but organizations fail to sufficiently train and educate them on security risks and proper handling of sensitive data. Here is how organizations across Canada stack up on 4 key areas of employee cyber security training.

Employee training actions	Well trained	Not well trained
How to use basic security tools (eg. password managers)	66%	34%
Proper care of sensitive data (eg. customer/other employee private data)	59%	41%
To frequently update PC and smartphone software	29%	71%
How to identify attacks (eg. phishing and other scams)	26%	74%

Patch and update quickly.
One of the easiest and most effective security protections is simply updating software. Yet too many devices and backend systems are left exposed for much longer than they should be. The good news is that there are tools available to automate the process, to both highlight when software is out of date and then automatically update it.

	Left exposed without critical updates for weeks
PCs	30%
Smartphones	13%
Server and backend systems	86%
Web app	89%
Network	88%
IaaS/PaaS	88%

Defending against attacks is important, but speed of detection and rapid recovery is critical.
Taking the right steps to identify risks is an efficient way to protect your business. But breach detection, response, and recovery are also key aspects of a complete cyber security process that will reduce costs and effort.

The speed at which your organization detects a breach is critical. For example, despite storing 50x more data than small organizations, large organizations only have 1.4x more files exposed during a breach. That's because large organizations detect breaches 40% faster than small organizations. Threat intelligence is critical for preventing breaches. Organizations that don't have a threat intelligence service in place experience 168% more breaches than organizations that utilize one.

Make an incident response plan, you'll need it – and you'll need to update it.
Nearly 9 out of 10 Canadian organizations reported a cyber security breach last year. Those that had an incident response plan spent less than half the money and 20% less staff time on responding to and recovering from breaches than those with less planning. Make sure to revisit your incident response plan at least once a year and update it as necessary. Many changes can occur across an organization in that timeframe, including new technologies, business objectives, costs, and staff accountabilities, that could require changes to your plan.

Great leadership enables effective cyber security.
By creating an environment that prioritizes IT security, good leadership makes it easier to implement and enforce security processes, obtain adequate IT security staffing and budget, gain organizational certifications (eg. ISO 27001), and invest in newer security technologies and tools such as Threat Intelligence. Our study indicates that proper leadership can result in a greater than 25% reduction in the number of breaches suffered per year.

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 nonresponse 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.

PART SIX
APPENDIX

PART SIX

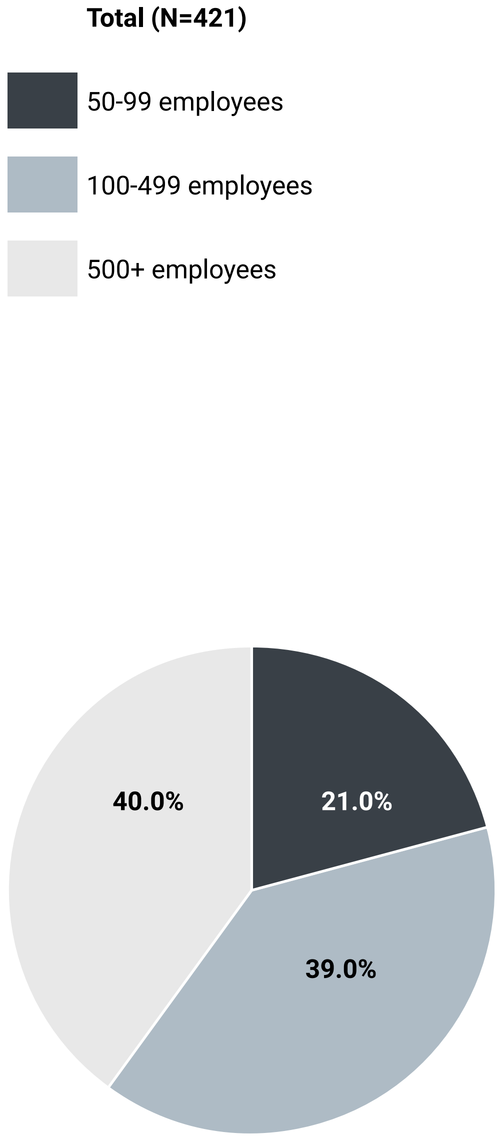
APPENDIX

Demographics

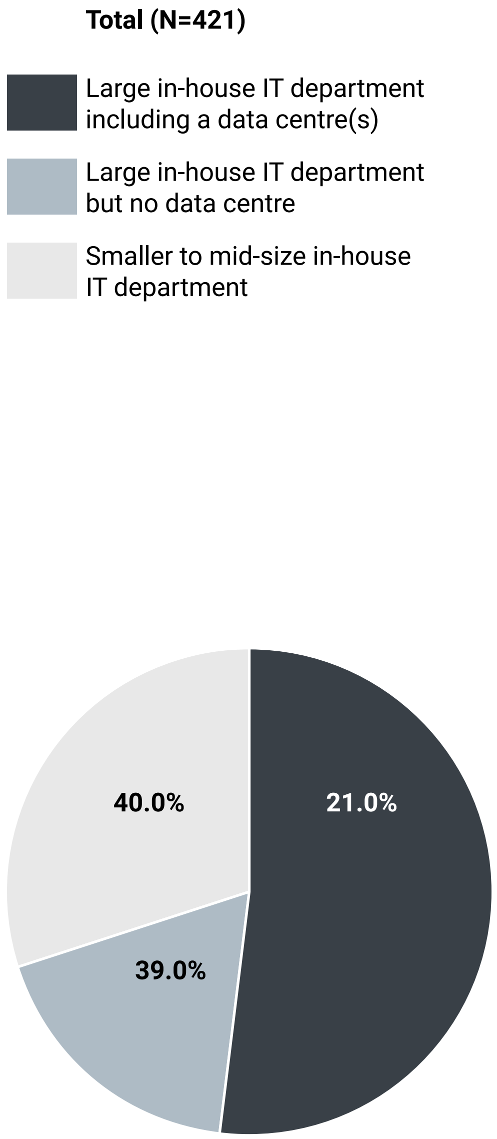
A sampling frame of 8,062 Canadian IT security and risk & compliance professionals were selected to receive invitations to participate in this survey. All survey participants were screened for direct involvement in improving or managing their organization's IT security. The following table shows the returns including the removal of certain participants based on screening and reliability checks. Our final sample consisted of 421 surveys, or a 5.2% response rate.

The survey firmographics and demographics are as follows:

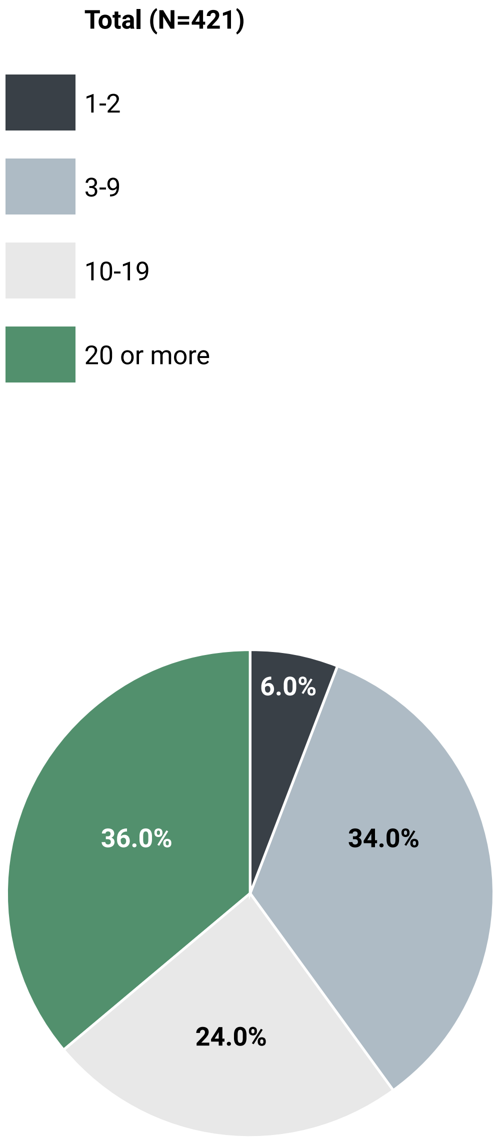
PIE CHART 3. *Employee size range*



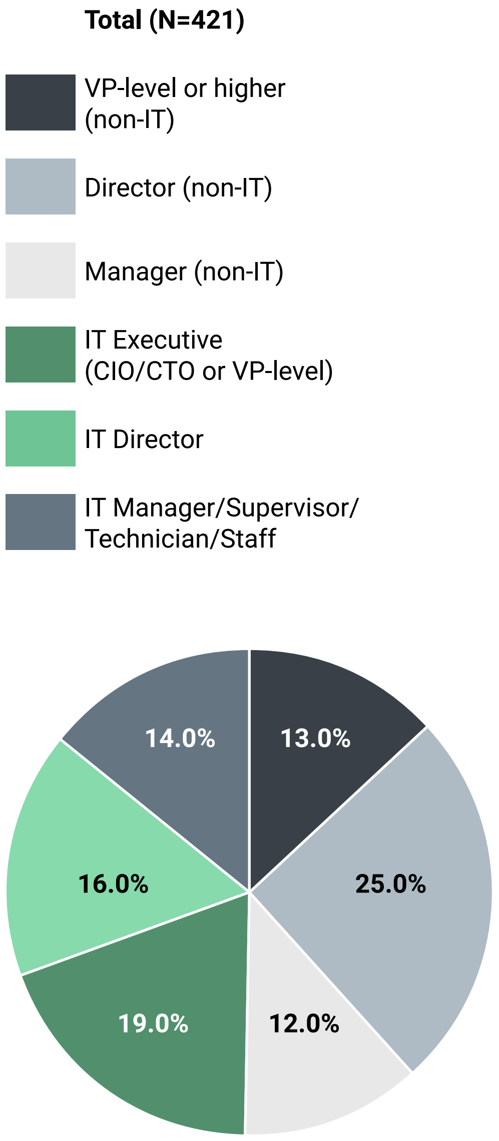
PIE CHART 4. *IT department characteristics*



PIE CHART 5. *Number of full-time IT staff*



PIE CHART 6. *Level of respondent*



Detailed Survey Results

S1. *Which of the following industry categories best represents the principal business activity of your organization?*

	TOTAL
Base: All Respondents	(421)
Business/Professional Services (eg. Legal, Accounting, Engineering, Architecture, etc.)	7%
Personal/Consumer Services (eg. Travel, Beauty, Personal Training, Dry Cleaning etc.)	3%
Construction	3%
Hospitality	3%
IT industry	6%
Not for profit	-
Manufacturing	8%
Crown Corporation or other publicly funded organization	-
Education K-12	-
Education College/University	5%
Financial Services	10%
Government	4%
Healthcare	8%
Primary (eg. Agriculture, Mining, Forestry, etc.)	4%
Oil & Gas or Field Services related	5%
Retail	8%
Communications (eg. Cable and Telecommunications Services, etc.)	5%
Media (eg. Radio/TV Broadcasting)	4%
Printing, Publishing, etc.	2%
Transportation and Warehousing	6%
Utilities	5%
Wholesale and Distribution	6%
Other	*
Don’t know	-

S1a. *Which level of government best describes your organization?*

	TOTAL
Base: All Respondents Select Government at S1	(18)
Federal	44%
Provincial	33%
Municipal	22%

S2. *How many full-time employees does your company have located within Canada?*

	TOTAL
Base: All Respondents	(421)
1-14	-
15-24	5%
25-99	7%
100-249	8%
250-499	21%
500-999	15%
1,000-4,999	15%
5,000+	29%
Don't know	-
Mean	2122.86

S3. *What percentage of your total employees are located within Canada?*

	TOTAL
Base: All Respondents	(421)
1%-9%	-
10%-25%	10%
26%-50%	16%
51%-75%	20%
76%-100%	54%
Don't know	-
Mean	67.85

S4. *Is your company headquartered in Canada, and if so which of the following areas is it headquartered in?*

	TOTAL
Base: All Respondents	(421)
Not headquartered in Canada	*
Western and Central Canada (BC, AB, SK, MB)	26%
Ontario	25%
Quebec	25%
Atlantic Canada (NB, NS, NFLD, PEI)	24%

S6. *How many full-time IT staff does your organization have?*

	TOTAL
Base: All Respondents	(421)
None	-
1-2	3%
3-5	6%
6-15	13%
16-40	29%
41-99	15%
100 or more	34%
Mean	54.26

S7. *Which of the following best describes the department you work for?*

	TOTAL
Base: All Respondents	(421)
Administration	-
Customer Support	-
C-level Executive Management excluding IT	-
Line of Business Management excluding IT	-
CIO/CTO/CSO/CISO, etc.	6%
Finance/Accounting	-
Human Resources	-
IT/IS/MIS/Data Centre/IT Security	87%
Legal/compliance/risk	7%
Logistics	-
Manufacturing/Production	-
Sales/Marketing	-
Purchasing/Procurement	-
Research & Development/Engineering excluding IT	-
Other	-

S8. *At your organization, do you play a role in or are you part of? (please select all that apply)*

	TOTAL
Base: All Respondents	(421)
Directing the IT function	26%
Improving/managing IT security	100%
Setting IT priorities	36%
Managing IT budgets	23%

S9. *Which of the following best describes your Job title?*

	TOTAL
Base: All Respondents	(421)
IT Executive – eg. CIO/CTO/VP, CSO/CISO	7%
IT Director	10%
Infosec Director	4%
IT Manager	17%
Infosec Manager	5%
IT Supervisor	10%
Infosec Supervisor	5%
IT Staff/Associate/Technician	17%
IT Associate/Staff	13%
IT Consultant/Contractor	5%
Legal/compliance/risk executive, manager or staff	7%
Don’t know	-

S10. *How many IT security staff are employed at your organization?*
You can enter fractions such as 0.75 if a person only devotes a part of their working time towards IT security.

	TOTAL
Base: All Respondents	(421)
Less than one	9%
1<3	40%
3<5	19%
5<9	14%
9<15	16%
15<21	3%
21+	1%
Mean	4.61

S11. *Which of the following ranges would your organization's annual revenue (or budget for government) fall under?*

	TOTAL
Base: All Respondents	(421)
Less than $10 million	10%
$10 million-$25 million	12%
$26 million-$99 million	15%
$100 million-$499 million	27%
$500 million-$999 million	21%
$1 billion or more	14%
Mean	394.37

Q1. *Q1. Which of the following government or industry regulations does your organization need to be compliant with? (please select all that apply)*

	TOTAL
Base: All Respondents	(421)
PCI	41
PIPEDA/Digital Privacy Act	69
GDPR	18
FFIEC, ITAR, OSFI, FedRAMP, FISMA	15
SOX, C-SOX	59
HIPAA, PHIPA	8
NERC/FERC	12
Other	3

Q2. *How many of each of the following does your organization have in Canada?*

SUMMARY : Mean	TOTAL
Base: All Respondents	(421)
PCs/laptops	2332.77
Smartphones/tablets	1715.82
Servers (Virtual or Physical)	187.09
TBs of storage capacity attached to/within servers	273.23

Q3. *Please estimate what percentage of your organization's customer, employee, and partner activity is conducted through a website maintained by your organization?*

	TOTAL
Base: All Respondents	(421)
Mean	35.19%

Q4. *What percentage of the data at your organization would be classified into each of the following levels of sensitivity?*

SUMMARY : Mean	TOTAL
Base: All Respondents	(421)
Top Secret/Highly Confidential	35.65%
Proprietary/Internal Use	35.65%
Public	28.7%

Q5. *Estimated total annual IT budget (eg. staff, hardware, software, services) of your organization:*

	TOTAL
Base: All Respondents	(421)
Mean	12488.58

Q6. *Percentage of total annual IT budget devoted to security?*

	TOTAL
Base: All Respondents	(421)
Mean	10.12%

Q7. *What percentage of your IT security budget is spent on staff versus all other costs?*

SUMMARY : Mean	TOTAL
Base: All Respondents	(421)
Staff portion of IT security budget	21.03%
All other costs	78.97%

Q8. *Which of the following best describes how your organization approaches the following:*

Taking inventory of applications, devices and systems	TOTAL
Base: All Respondents	(421)
Conducted across the entire organization	43%
Conducted across select areas/departments of the organization	54%
Not conducted	4%

Q8. *Which of the following best describes how your organization approaches the following:*

Discovering/assessing security weaknesses/vulnerabilities across applications, devices, and systems	TOTAL
Base: All Respondents	(421)
Conducted across the entire organization	69%
Conducted across select areas/departments of the organization	29%
Not conducted	2%

Q8. *Which of the following best describes how your organization approaches the following:*

Assessing the business impact of data loss/corruption, disruption of work	TOTAL
Base: All Respondents	(421)
Conducted across the entire organization	31%
Conducted across select areas/departments of the organization	56%
Not conducted	13%

Q8. *Which of the following best describes how your organization approaches the following:*

Prioritizing deployment of specific security solutions	TOTAL
Base: All Respondents	(421)
Conducted across the entire organization	29%
Conducted across select areas/departments of the organization	56%
Not conducted	15%

Q9. *Does your security planning consider your key suppliers and third-party relationships, and the data flows between you and them?*

	TOTAL
Base: All Respondents	(421)
YES – in a comprehensive manner	26%
YES – but we should look at this in more detail	60%
NO	11%
Not sure/don't know	3%

Q10. *From the list below, please select the five technologies or tactics you feel have been the most effective at protecting your organization from cyber security threats over the past year:*

	TOTAL
Base: All Respondents	(421)
Data Security (encryption, etc.)	62%
DDoS Protection (appliance or service)	6%
DNS Security	20%
Identity and Access Management	18%
Network Security (NGFW)	61%
Risk and Compliance Automation	23%
Security Monitoring (SIEM, log management)	54%
Threat Intelligence	21%
Vulnerability Management	28%
Web Content Filtering	24%
Next-gen Endpoint Protection	17%
Traditional Endpoint Protection	49%
Email Security	58%
Breach Response and Forensics Tools	27%
Security Awareness Training	33%
Other	*

Q11. *Which of the following best describes how your organization trains employees on the following?*

To frequently update PC and smartphone OS and apps	TOTAL
Base: All Respondents	(421)
Formal training with reminders as required by new threats, etc.	29%
Ad hoc training and reminders	65%
No training	6%

Q11. *Which of the following best describes how your organization trains employees on the following?*

How to use security technology	TOTAL
Base: All Respondents	(421)
Formal training with reminders as required by new threats, etc.	66%
Ad hoc training and reminders	28%
No training	6%

Q11. *Which of the following best describes how your organization trains employees on the following?*

How to identify attacks such as phishing and other scams	TOTAL
Base: All Respondents	(421)
Formal training with reminders as required by new threats, etc.	26%
Ad hoc training and reminders	64%
No training	10%

Q11. *Which of the following best describes how your organization trains employees on the following?*

Proper care of sensitive data such as customer/other employee private data	TOTAL
Base: All Respondents	(421)
Formal training with reminders as required by new threats, etc.	59%
Ad hoc training and reminders	27%
No training	14%

Q12. *How long does it take your organization to install security updates/patches (including critical updates/patches) or upgrade to the most secure version of operating systems and applications for the following?*

PCs	TOTAL
Base: All Respondents	(421)
Immediately when released	18%
Within a week	52%
Within a month	26%
Within a year	4%
A year or more	-

Q12. *How long does it take your organization to install security updates/patches (including critical updates/patches) or upgrade to the most secure version of operating systems and applications for the following?*

Smartphones	TOTAL
Base: All Respondents	(421)
Immediately when released	59%
Within a week	27%
Within a month	11%
Within a year	2%
A year or more	*

Q12.*How long does it take your organization to install security updates/patches (including critical updates/patches) or upgrade to the most secure version of operating systems and applications for the following?*

On-premise databases, apps, servers	TOTAL
Base: All Respondents	(421)
Immediately when released	6%
Within a week	7%
Within a month	71%
Within a year	15%
A year or more	*

Q12.*How long does it take your organization to install security updates/patches (including critical updates/patches) or upgrade to the most secure version of operating systems and applications for the following?*

Web applications	TOTAL
Base: All Respondents	(421)
Immediately when released	4%
Within a week	7%
Within a month	30%
Within a year	56%
A year or more	2%

Q12. *How long does it take your organization to install security updates/patches (including critical updates/patches) or upgrade to the most secure version of operating systems and applications for the following?*

Network equipment	TOTAL
Base: All Respondents	(421)
Immediately when released	4%
Within a week	8%
Within a month	59%
Within a year	27%
A year or more	2%

Q12. *How long does it take your organization to install security updates/patches (including critical updates/patches) or upgrade to the most secure version of operating systems and applications for the following?*

Public cloud (IaaS/PaaS)	TOTAL
Base: All Respondents	(421)
Immediately when released	6%
Within a week	6%
Within a month	22%
Within a year	61%
A year or more	5%

Q13. *How effective are each of the following at protecting your organization from security attacks?*
(% of respondents with top 2 box responses on a 1-7 scale; 7 being "Highly effective")

SUMMARY : TOP 2 BOX	TOTAL
Base: All Respondents	(421)
Internal IT/security staff	34%
Security technology we have currently deployed	35%
Our security risk and incidence response process	38%

Q13. *How effective are each of the following at protecting your organization from security attacks?*
(% of respondents with bottom 2 box responses on a 1-7 scale; 1 being "Not effective at all")

SUMMARY : BOTTOM 2 BOX	TOTAL
Base: All Respondents	(421)
Internal IT/security staff	8%
Security technology we have currently deployed	7%
Our security risk and incidence response process	9%

Q14. *Please estimate how many attacks and breaches your organization has been subject to over the past twelve months:*

TOTAL number of attacks	TOTAL
Base: All Respondents	(421)
0	4%
1-10	6%
11-50	25%
51-100	11%
101-500	24%
501-1000	14%
1001-5000	15%
Mean	454.75

Q14. *Please estimate how many attacks and breaches your organization has been subject to over the past twelve months:*

TOTAL number of breaches	TOTAL
Base: All Respondents	(421)
0	13%
1-10	56%
11-20	26%
21-30	4%
Mean	9.33

Q14. *Please estimate how many attacks and breaches your organization has been subject to over the past twelve months:*

Low impact incidents	TOTAL
Base: All Organizations Subject To Breaches Over The Past Twelve Months	(367)
0	14%
1-10	67%
11-20	16%
21-30	3%
Mean	7.43

Q14. *Please estimate how many attacks and breaches your organization has been subject to over the past twelve months:*

High impact incidents	TOTAL
Base: All Organizations Subject To Breaches Over The Past Twelve Months	(367)
0	26%
1-10	74%
Mean	1.9

Q15. *Which of the following apply to your organization’s security breaches?*

Estimated hours of cumulative downtime	TOTAL
Base: All Respondents Select Yes at Q15 (Downtime)	(213)
Mean	90

Q15. *Which of the following apply to your organization's security breaches?*

Files/records were affected	TOTAL
Base: All Organizations Subject To Breaches Over The Past Twelve Months	(367)
Yes	83%
No	17%

Q15. *Which of the following apply to your organization's security breaches?*

Sensitive data was involved	TOTAL
Base: All Organizations Subject To Breaches Over The Past Twelve Months	(367)
Yes	47%
No	53%

Q15. *Which of the following apply to your organization's security breaches?*

Downtime	TOTAL
Base: All Organizations Subject To Breaches Over The Past Twelve Months	(367)
Yes	58%
No	42%

Q15. *Which of the following apply to your organization's security breaches?*

Estimated number of files/records	TOTAL
Base: All Respondents Who Selected Yes at Q15 for (Files/records were affected)	(303)
Mean	1907.69

Q15. *Which of the following apply to your organization's security breaches?*

Sensitive but non-personal business data	TOTAL
Base: All Respondents Who Selected Yes at Q15 for (Sensitive data was involved)	(174)
Mean	56.12%

Q15. *Which of the following apply to your organization's security breaches?*

Customer or employee personal data	TOTAL
Base: All Respondents Select Yes at Q15 (Sensitive data was involved)	(174)
Mean	23.71%

Q16. *How long would you estimate it takes your organization to detect the following types of attacks?*

Low impact incident (eg. minor incident - drive by download, ransomware on only a few devices, non-targeted malware, etc.)	TOTAL
Base: All Respondents	(421)
Within hours	76%
Within a week	19%
Within a month	5%
Within a year	*
A year or more	-

Q16. *How long would you estimate it takes your organization to detect the following types of attacks?*

High impact incidents (eg. major breach – highly sensitive data exposed, targeted attack, etc.)	TOTAL
Base: All Respondents	(421)
Within hours	35%
Within a week	50%
Within a month	14%
Within a year	1%
A year or more	-

Q17. *Earlier in this survey you reported that your organization experienced breaches (major and minor) over the past twelve months. How much do you estimate it cost your organization to fully recover and respond to these breaches in terms of direct dollars expended with relation to?*

Hard costs (eg. legal, customer outreach, software, services, etc.)	TOTAL
Base: All Organization Has Been Subject To Breaches Over The Past Twelve Months	(367)
Mean	$131,975.13

Q17. *Earlier in this survey you reported that your organization experienced breaches (major and minor) over the past twelve months. How much do you estimate it cost your organization to fully recover and respond to these breaches in terms of direct dollars expended with relation to?*

Soft costs (eg. brand image, competitive standing, employee morale, etc.)	TOTAL
Base: All Organization Has Been Subject To Breaches Over The Past Twelve Months	(367)
Mean	$83,105.72

Q18. *How many work days do you estimate your organization's security/IT/legal and any other relevant staff spent recovering from breaches over the past year?*

	TOTAL
Base: All Respondents	(421)
Mean	16.1

Q19. *How many staff at your organization are responsible for monitoring security technologies for potential harmful activity? (please only include staff that watch for security events and do not include staff that only deploy or provide technical support for these security technologies/solutions)?*

	TOTAL
Base: All Respondents	(421)
Mean	3.06

Q20. *What percentage of your total security budget is spent on external third party provided managed security services (eg. firewall monitoring, threat intelligence, Web app monitoring, etc.)?*

	TOTAL
Base: All Respondents	(421)
Mean	30.28%

Q21. *Which of the following external managed security services does your organization use?*

	TOTAL
Base: All Respondents Using External Security Services	(409)
Managed DDoS Prevention	34%
Managed NGFW	32%
Managed SIEM (aaS) - Cloud	27%
Managed SIEM on-premise	31%
Managed Threat Intelligence	48%
Managed Zero-day Endpoint Protection	38%
Managed Web Application Firewall	45%
Security Device Management	52%
Vulnerability Management Service	35%
Managed Data Loss Prevention	46%
None of the above	1%

Q22. *Which of the following external security services does your organization use?*

	TOTAL
Base: All Respondents	(421)
Security Program Consulting	64%
Security Threat Risk Assessment	62%
Data Privacy Impact Assessments	33%
Vulnerability Assessment	48%
Penetration Testing	32%
IT Operational Risk Assessment	43%
ITIL Consulting	13%
Virtual CSO	14%
Breach Response and Forensics	29%
Audit and Assurance Services	43%
Security Awareness Training	36%
None of the above	4%

Q23. *Which of the following best describes your organization's security incident response plan?*

	TOTAL
Base: All Respondents	(421)
We do not have a security incident response plan	2%
Our security incident response plan is informal	18%
We have a documented security incident response plan, but it's not often updated	48%
We have a fully documented security incident response plan and it is regularly updated	32%

Q24. *How much do you feel executive (outside of IT) leadership at your organization is involved in leading a culture where security best practices must be followed? (average response on a 1-5 scale where 1 equals "Uninvolved leadership" and 5 equals "Highly involved leadership")*

	TOTAL
Base: All Respondents	(421)
Mean	3.51

Q28. *Please rate how concerned you believe your organization is with each of the following?*
(% of respondents with top 2 box responses on a 1-5 scale; 5 being "Highly concerned")

SUMMARY : TOP 2 BOX	TOTAL
Base: All Respondents	(421)
Insider/malicious employee threat	63%
Ransomware	15%
Mobile threats	28%
IoT security	37%
Data not being backed up	40%
Cloud security	63%
Public exposure of customer data	62%
State Sponsored Attacks	19%
Hacktivism	21%
Security related downtime of business-critical IT resources	34%

Q29. *How confident are you in your organization's overall ability to prevent cyber security breaches from happening?*

	TOTAL
Base: All Respondents	(421)
Highly confident (5)	5%
4 (4)	51%
3 (3)	38%
2 (2)	6%
Not at all confident (1)	*

Q30. *How confident are you in your organization's overall ability to detect and respond to cyber security breaches once they have happened?*

	TOTAL
Base: All Respondents	(421)
Highly confident (5)	11%
4 (4)	53%
3 (3)	31%
2 (2)	5%
Not at all confident (1)	*

About Scalar

Scalar is Canada's leading IT services provider, focused on security, infrastructure, cloud, and digital transformation. Founded in 2004, Scalar is headquartered in Toronto, with offices in Montreal, Ottawa, London, Winnipeg, Calgary, Edmonton, Victoria, and Vancouver. Scalar was recently named to the CRN Fast Growth Top 150 List and listed on the PROFIT 500 for the seventh 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 -2016 editions of the Branham 300.

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

About IDC Canada

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. IDC Canada is part of a network of over 1100 analysts providing global, regional, and local expertise on technology, industry opportunities and trends with more analysts dedicated to understanding the Canadian market than any other global research firm.

Research independently conducted by IDC Canada | Published February 2018