The Cyber Resilience of Canadian Organizations

Results of the 2019 Scalar Security Study

CONTENTS:

PART 1:
EXECUTIVE SUMMARY


On average, organizations experienced
440
attacks in the past year

PART 2: EXECUTIVE SUMMARY

Scalar's study of the cyber resilience of Canadian organizations finds there is a new normal across the threat landscape. Cyber security incidents – whether they be exfiltration, infiltration, or denial of service – are now occurring on a regular basis. To address this, the focus of cyber security efforts is shifting from an emphasis on protection against attacks, to improving the detection of malicious actors on the network, and responding to and recovering from incidents as quickly as possible. The findings of the 2019 Scalar Security Study reflect on these new trends and introduce cyber resilience as a security theme that emphasizes the importance of business continuity and the need for organizations to return to normal operations and a trusted state after an incident has occurred.

Over the past year, Canadian organizations have increased their focus on identifying assets on the network, prioritizing deployment of cyber security solutions, and patching on-premise infrastructure, but there are still key cyber resilience weaknesses including:

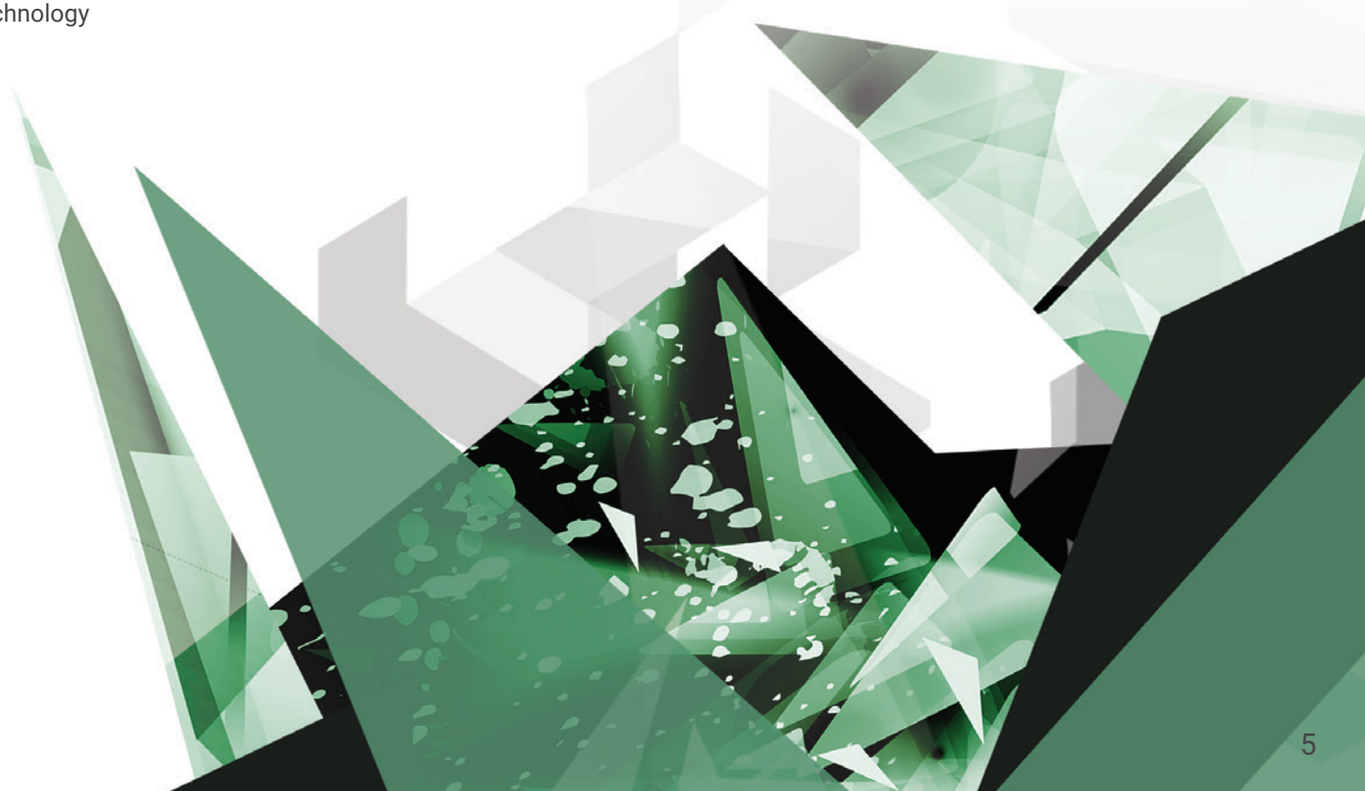
- Inability to prevent cyber security breaches
- Lack of comprehensive cyber resilience strategies including people, processes, and technology
- Slow detection and response times and adoption of monitoring solutions
- Lack of documented incident response

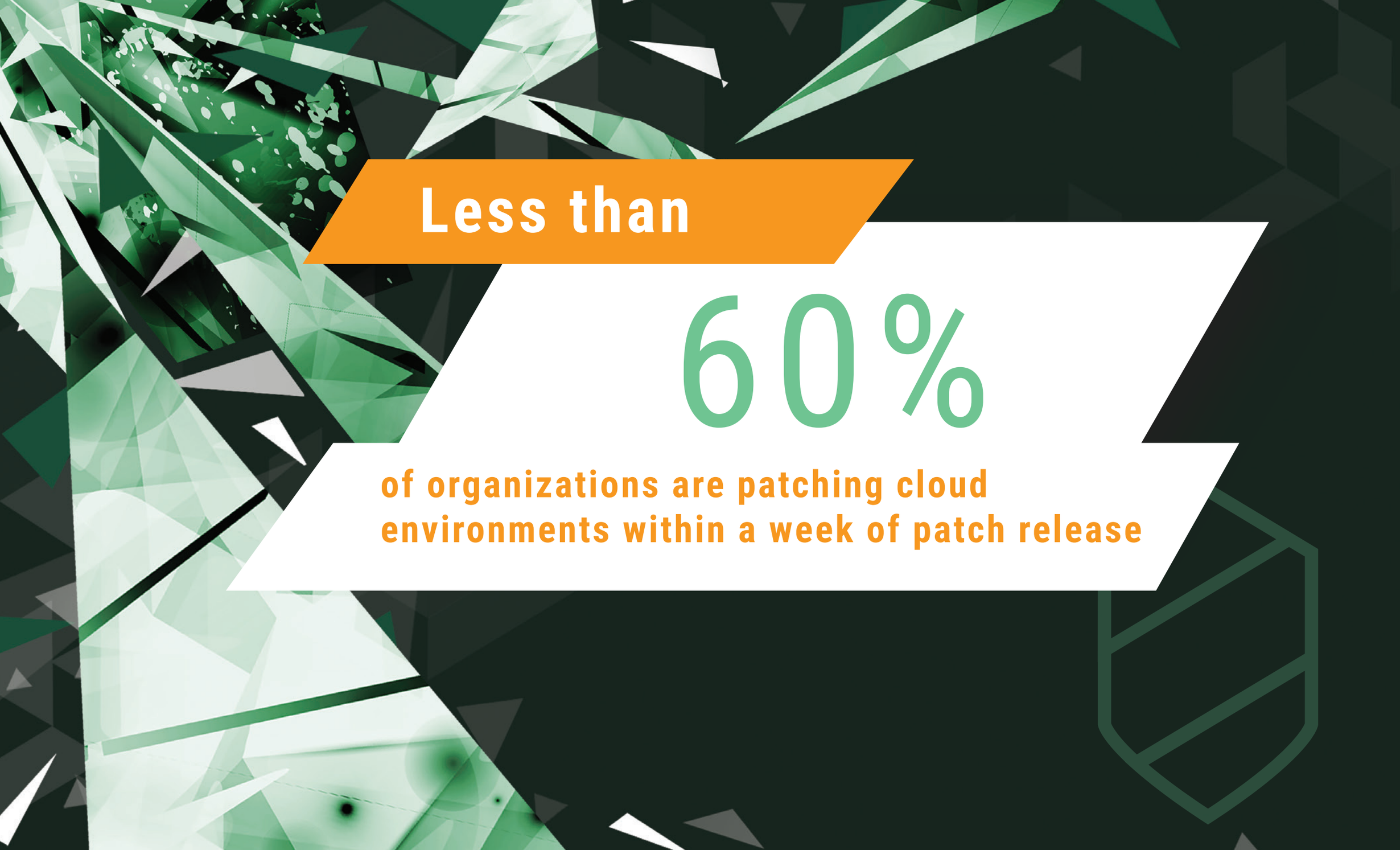
Firms also have organizational blind spots to risk areas, including:

- Understanding the data-flows between an organization and its third-party partners, suppliers, and vendors
- Knowledge of government privacy legislation
- Cyber security responsibilities in cloud environments including patching and updating software
- Exposure to insider threats from employees or contractors

Using the National Institute of Standards and Technology (NIST) cyber security framework and statistical segmentation, the survey results were analyzed to produce the following key lessons:

- Practicing a fundamental level of cyber resilience reduces the number of security incidents an organization experiences by more than 50%, and in the case of breaches, reduces its file and data exposure, downtime, and recovery costs
- Moving beyond a fundamental level of cyber resilience is difficult for Canadian organizations due to deficiencies in security planning, training, documentation, and the ability to assess risks and prioritize updates, patches, and security solution investment according to a comprehensive threat and risk assessment




Less than
60%
of organizations are patching cloud environments within a week of patch release

PART 2:

INTRODUCTION AND METHODOLOGY


The average cost of cyber compromise per organization
$4.8-$5.8
million

PART 2: INTRODUCTION AND METHODOLOGY

This report represents the findings of the 2019 Scalar Security Study, the Cyber Resilience of Canadian Organizations. Independently conducted by IDC Canada, the data provided in this report was obtained through a Canada-wide cross-industry survey of 407 IT security and risk & compliance professionals. All survey participants were screened for direct involvement in improving or managing their organization's IT security. Eighty-seven 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 serious is the threat of attack facing Canadian organizations?
- How expensive are security breaches getting?
- What is the total cost of compromise across the different types of cyber security breaches?
- What weaknesses still need to be addressed?
- How prepared are organizations to respond to and recover from security incidents?
- What technologies or processes can organizations implement to improve their cyber defences?

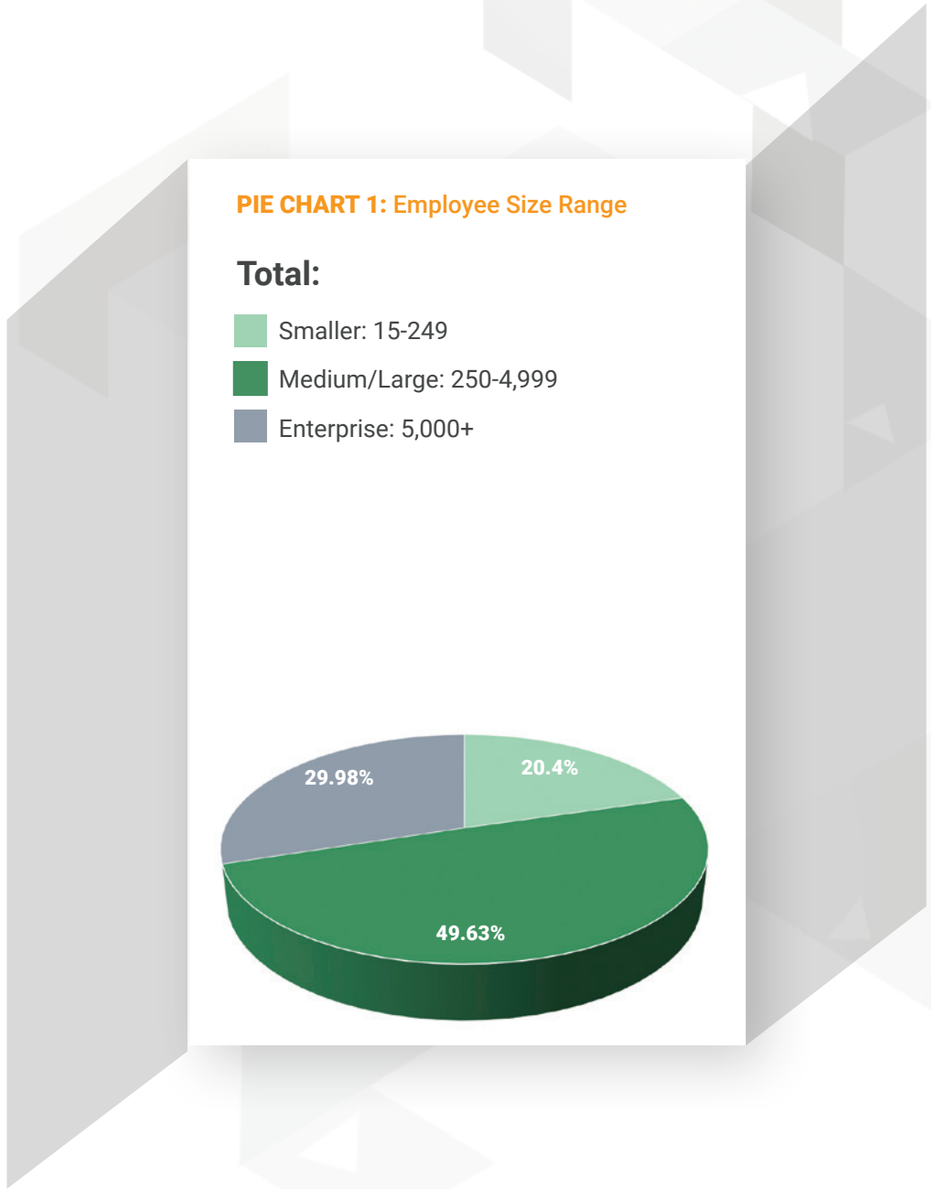
The survey was conducted over the course of September-October 2018 by IDC Canada on behalf of Scalar. Appendix A shows a detailed description of the demographics and firmographics of the survey participants.

Organization Size Segmentation

In this report, Scalar classifies responding organizations as Smaller, Medium/Large, and Enterprise class. 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 preparedness and cyber resilience of Canadian organizations.



Cyber Resilience Fundamentals Segmentation

A statistical segmentation was used to analyze the survey results based on responding organizations who are practicing cyber resilience fundamentals versus those who are not. To be included in the "practices cyber resilience fundamentals" segment respondents were required to provide the following answers across survey questions 8, 11, 12, 24, and 26a as follows:

	SEGMENT: PRACTICES CYBER RESILIENCE FUNDAMENTALS	SEGMENT: DOES NOT PRACTICE CYBER RESILIENCE FUNDAMENTALS
QUESTIONS	**QUALIFYING RESPONSES**	**QUALIFYING RESPONSES**
Q8. Which of the following best describes how your organization approaches the following (multiple questions)	Conducted across select areas/departments of the organization Conducted across the entire organization	Not conducted
Q11. Which of the following best describes how your organization trains employees on the following? (multiple questions)	Formal training with reminders Ad hoc training and reminders	No training
Q12. How long does it take your organization to install security updates/patches or upgrade? (multiple questions)	Immediately when released Within a week Within a month	Within a year A year or more
Q24. Which of the following best describes your organization's security incident response plan?	Fully documented incident response plan and it is regularly updated Documented incident response plan, but it is not often updated Incident response plan is informal	No incident response plan
Q26a. Which of the following best describes your organization's plan for recovery back to trusted state after a data breach?	Fully detailed and documented processes Processes are in place but documentation is not complete	Processes are in place but documentation is not complete Ad hoc processes are in place


100%
of organizations surveyed report experiencing cyber security attacks over the past 12 months
with 58% having data exfiltrated

PART 3:
KEY FINDINGS

PART 3: 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 key findings is as follows:

Cost of compromise is at an all time high

- Average number of attacks per organization per year declined to 440 per organization, down from 455 in 2018
- Average number of breaches per organization per year increased to 12.5 per organization, up from 9.3 in 2018
- A higher percentage of attacks are resulting in major impacts: 3% of attacks resulted in a breach versus 2% in 2018
- The average cost per organization of responding to and recovering from cyber security incidents increased significantly from $3.7 million last year, to between $4.8 million - $5.8 million this year

Detection and response time are too slow, resulting in high costs

- Detection and response can take weeks
- Time to recovery is increasing
- Deficiencies in planning for cyber security incident response and recovery back to trusted state leaves organizations vulnerable when breached
- Planning deficiencies and unrealistic time to recovery expectations result in Canadian organizations underestimating the cost of cyber security incidents
- Organizations that follow fundamental cyber resilience practices spend an average of 16.1 staff work days recovering from cyber security breaches per year versus 20.5 days for organizations that do not

Evolving threats create new opportunities for malicious actors

- All organizations surveyed provide some sort of remote access to their corporate network via the internet
- Organizations attack surface grows exponentially with respect to employee count
- Fifty-five percent of organizations surveyed must comply with three or more government or industry regulations relating to data or privacy
- Organizations that conduct cyber security fundamentals can reduce cyber attack success rates by over 50%

Cloud security strategy is not keeping up with adoption rates

- Cloud environments are targeted and attacked by malicious actors just as often as on-premise
- Over 12% of Canadian organizations have migrated all infrastructure to the cloud
- Less than 60% of organizations update their public cloud environments within a week of patch release

Strategy focus is shifting from protection to detection and response

- Traditional perimeter and endpoint security solutions will continue to be deployed, and will be complimented by AI, machine learning, and new detection techniques
- Canadian organizations see monitoring solutions as a key enabler for enhancing their security posture
- Organizations will be making investments in breach response and forensics tools in the coming years

FINDING 1: COST OF COMPROMISE IS AT AN ALL TIME HIGH

One concept we aim to understand with this study is the total cost of compromise across the different types of cyber security incidents for Canadian organizations. In order to provide a comprehensive and in-depth data analysis on the nature and costs of cyber security incidents, this year's study classifies incidents into three categories:

- **Exfiltration**
- **Infiltration**
- **Denial of Service (DoS)**

Previous editions of this study consisted of a general classification of all incidents, defined as either high or low impact breaches.

Using the new categorization, we found the average number of attacks per responding organization is similar to that reported in 2018, but the cost of attacks has increased. Analysis of the study results shows an average of 440 attacks per organization per year, down from 455 in 2018, with the direct dollars expended addressing cyber attacks rising significantly to $853,000 per organization, up from $215,000 per organization last year.

Further detail on the number and costs of attacks is provided in the tables that follow:

TABLE 1. Number of attacks and breaches faced by Canadian organizations over the past twelve months

2018

MEANS	TOTAL
Base: All Respondents	**(421)**
Total number of attacks per organization	454.75
Total number of breaches per organization	9.33

2019

MEANS	TOTAL
Base: All Respondents	**(407)**
Total number of attacks per organization	439.97
Total number of exfiltration, infiltration, and DoS incidents per organization	30.12 Exfiltration, infiltration, and DoS

On average, responding organizations were attacked more than 440 times per year, resulting in an average of 12.47 exfiltration incidents, 9.83 infiltration incidents, and 7.82 denial of service incidents per organization per year (versus an average of 9.33 breaches per organization in 2018).

The new categorization of attacks as exfiltration, infiltration, or denial of service, rather than high or low impact breaches as used last year, reduces ambiguity and allows improved detail and granularity on the actual nature and costs affecting Canadian organizations.

Malicious actors are becoming more effective

Exfiltration versus breach is the closest to a direct comparison there is between the new 2019 attack categorization and the version used in 2018. The percentage of attacks resulting in exfiltration versus breach shows that malicious actors are becoming more effective. Nearly 3% of attacks resulted in a successful exfiltration this year, versus the 2.1% of attacks resulting in a breach reported in 2018. Due to the high number of attacks per organization, this results in a 33.7% jump in exfiltration versus breaches per organization per year.

TABLE 2. Year over year comparison of attack to breach or exfiltration success rate

MEANS	TOTAL 2018	TOTAL 2019
Base: All Respondents	**(421)**	**(407)**
Total number of attacks per organization	454.75	439.97
Total number of breaches, exfiltrations per organization	9.33	12.47 (33.7% more than 2018)
% of attacks resulting in breach	2.1%	2.83%

While this increase is concerning enough, including the results on infiltration and DoS shows the impact malicious actors are having, and just how significant a percentage of attacks consist of DoS and infiltration. This makes it extremely important for organizations to consider implementing security strategies and solutions that not only protect data, but offer service availability and integrity.

TABLE 3. Impact of infiltration and DoS on overall incidents per organization

MEANS	TOTAL 2019
Base: All Respondents	**(407)**
Total number of attacks per organization	439.97
Exfiltration incidents per organization Infiltration incidents per organization DoS incidents per organization	12.47 9.83 7.82
Total number of incidents per organization	30.12 (2.2x more than reported in 2018)

More than half the organizations who report being subject to an infiltration incident were subject to ransomware demands, encryption of data, and/or deletion of data.

TABLE 4. Percent of reported infiltration incidents where organizations were subject to a major impact

MEANS	ORGANIZATIONS SUBJECT TO RANSOMWARE, ENCRYPTION, OR DELETION OF DATA	TOTAL 2019
Base: All Respondents		**(407)**
Infiltration, incidents per organization		9.83
Percentage of infiltration incidents where organization was subject to: • Ransomware demands	88% (87.74) of organizations that reported infiltration incidents were subject to ransomware demands, encryption of data, or deletion of data	47.74%
• Encryption of data		44.52%
• Deletion of data		31.61%

- 100% of organizations surveyed report experiencing cyber security attacks over the past 12 months
- 58.48% report having data exfiltrated
  - 24.64% of organizations subject to exfiltration had sensitive but non-personally identifiable information (PII) exfiltrated
  - 25.13% of organizations subject to exfiltration had PII customer or employee information/data exfiltrated
- 38.08% report being infiltrated
  - 27.81% of organizations subject to infiltration had sensitive but non-personally identifiable information (PII) involved in their infiltration(s)
  - 22.96% of organizations subject to infiltration had PII customer or employee information/data involved in their infiltration(s)
- 18.18% report having data subjected to ransomware demands
- 16.95% had their data encrypted
- 12.04% had data deleted
- 87.74% of organizations that reported infiltration incidents were subject to ransomware demands, encryption of data or deletion of data
- 34.15% experienced their network going down as a result of DoS attacks

Total cost of compromise has increased dramatically

The percentage of organizations suffering a major cyber security incident and the reported cost of addressing cyber attacks have risen dramatically. Ninety-three percent of responding organizations suffered at least one major cyber security incident in the past 12-months (87% in 2018). Respondents provided feedback on the direct and indirect costs of a security breach, including lost revenue.

The average cost per organization of responding to and recovering from major cyber security incidents ranged from $4.6 million to $5.8 million based on the attack categorization (compared to last year's average of $3.7 million per organization).

- **Exfiltration:** $4.8 million
- **Infiltration:** $4.6 million
- **Denial of Service:** $5.8 million

TABLE 5. Cost of attacks for exfiltration, infiltration, and DoS for organizations subject to each attack category over the past twelve months

		ATTACK CATEGORY		
		EXFILTRATION	INFILTRATION	DENIAL OF SERVICE
Base: Percent of Total Organizations subject to attack type	Total survey base N=407	(238) = 58.5%	(155) = 38.1%	(139) = 34.2%
Hard and soft costs incurred to respond to and fully recover from all attacks experienced in the category*	$6,033,380	$4,787,220	$4,629,280	$5,780,400
Cost per employee	$2,677	$2,124	$2,054	$2,565
Business days of downtime for organizations that suffered downtime		8.8 business days	15.7 business days	19.2 business days
Employee work days expended responding and recovering	19.4 work days	18.6 work days	23.7 work days	19.0 work days
Average number of files or records compromised for organizations where files/records were affected		134	117	
Percent of files that contained sensitive/proprietary but non-PII data		24.6%	27.8%	
Percent of files that contained customer or employee PII		25.1%	23.0%	
Percent of infiltration attacks where data was subject to:				
Ransomware demands			47.7%	
Encryption			44.5%	
Deletion			31.6%	

*NOTE: Hard and soft costs defined as lost revenue, lost profit, staff time, legal costs, customer outreach, software, services, brand image, competitive standing impacts, and employee morale impacts

Not all organizations will have experienced major cyber security incidents in all three attack categories so these costs should not be considered additive. What they show is the average costs incurred by organizations subject to security compromises across exfiltration, infiltration, and DoS. Malicious actors adapt to an organization's defences and will attack in varied ways, making it critical to adopt cyber security tools and practices that can help address different attacks.

Despite the data, Canadian organizations are still unprepared

When asked how confident they are in their organization's ability to prevent cyber security breaches from happening, only 11% of survey respondents had a "high" degree of confidence. Forty-three percent considered themselves to be confident, but not to the highest degree.

What we see year over year is a very large increase (22%) in the confidence of smaller organizations regarding their ability to prevent cyber security breaches from happening versus medium/large, and enterprise-sized organizations whose confidence has dropped significantly compared to last year (64% and 64% respectively).

TABLE 6. 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	**(407)**	**(83)**	**(202)**	**(122)**
Highly confident	11%	18%	9%	9%
Confident	43%	43%	43%	41%
Neutral	37%	30%	37%	42%
Not confident	9%	8%	10%	8%
Not at all confident	0%	0%	0%	0%

A similar change has occurred in the results for organizations' confidence in their ability to effectively respond to cyber security breaches once they have happened:

- Smaller organizations' overall confidence (highly confident and confident) in their ability to effectively respond (70%) has increased significantly versus 2018 (57%)
- Medium/large (63%) and enterprise (59%) organizations are less confident this year compared to 2018 (66% and 66% respectively) with less enterprise-level organizations reporting high confidence in their ability to respond to cyber security breaches once they have occurred

TABLE 7. How confident are you in your organization's overall ability to detect and respond to cyber security breaches once they have happened?

		ORGANIZATION SIZE		
PERCENTAGE	TOTAL	SMALLER	MEDIUM/LARGE	ENTERPRISE
Base: All Respondents	**(407)**	**(83)**	**(202)**	**(122)**
Highly confident	15%	20%	14%	12%
Confident	48%	49%	49%	47%
Neutral	28%	24%	29%	30%
Not confident	9%	6%	8%	11%
Not at all confident	0%	0%	0%	0%
Cost of responding to and fully recovering from attacks per employee (average across exfiltration, infiltration and DoS)	$2,677	$42,435	$3,199	$2,831

Decrease in enterprise confidence coincides with significant increase in attacks on enterprise

The average number of attacks per organization per year for enterprise increased by 61% to 1,152 attacks per organization versus only 714 in 2018. One possible explanation could be that attackers have significantly increased their attack activities against the enterprise in an attempt to increase their success rates to the same levels achieved against smaller-sized organizations.

TABLE 8. Attacks versus success rate for exfiltration, infiltration and denial of service incidents

		ORGANIZATION SIZE		
	TOTAL	SMALLER	MEDIUM/LARGE	ENTERPRISE
Base: All Respondents	**(407)**	**(83)**	**(202)**	**(122)**
Number of times in the past 12 months that an organization has been subject to:				
IT security-related attack or threat	440	60	166	1,152
Exfiltration	21	14	27	16
Infiltration	26	25	30	19
DoS	23	14	29	21
Success rate of attacks as % of total IT security related attacks or threats faced over the past 12 months				
Exfiltration	4.8%	23.3%	16.3%	1.4%
Infiltration	5.9%	41.7%	18.1%	1.6%
DoS	5.2%	23.3%	17.5%	1.8%
Organizations that conduct NO employee training on identifying attacks such as phishing and other scams	9.0%	14.5%	8.4	6.6

The high success rate of attacks against smaller and medium/large organizations allows malicious actors to shift attack volume to enterprise. Corresponding with a relative deficiency in employee training on identifying attacks such as phishing and other scams, smaller organizations were particularly vulnerable to infiltration.

FINDING 2: DETECTION AND RESPONSE TIME IS TOO SLOW, RESULTING IN HIGH COSTS

It is well known among security professionals that every organization is going to face the threat of a cyber security attack, however, how an organization is prepared to mitigate that attack is, in large part, what determines if sensitive data is compromised or exfiltrated. Every second counts when a malicious actor is inside your network and it is essential to minimize detection and response time in order to keep an attack from becoming an exfiltration, infiltration, or DoS incident.

Detection and response are taking weeks

The majority of respondents have reported that it takes days to weeks to detect and respond to cyber compromise (see Table 9). Detection times for exfiltration and infiltration attacks are similar: Approximately 43% of responding organizations detect within a week (and 10.5% within a month), but the time to respond is longer for exfiltrations, leaving more time for attackers to steal data. Cyber resilience is negatively impacted due to deficiencies in incident response and recovery planning, resulting in more downtime, which increases the cost of cyber security incidents.

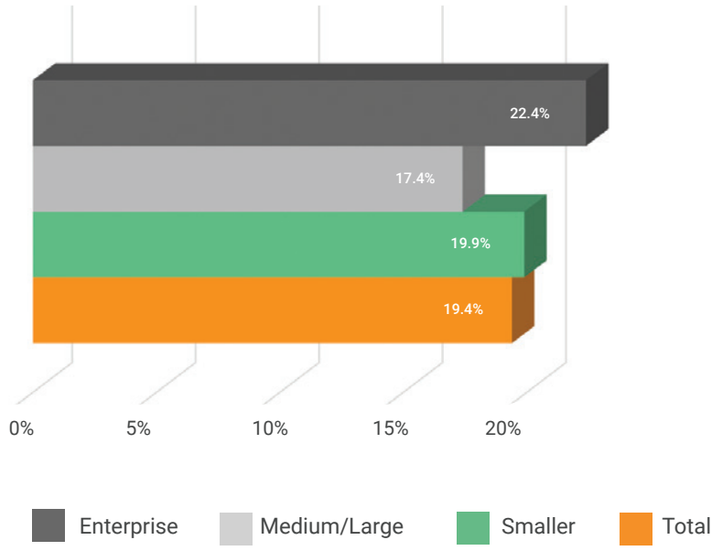
TABLE 9. Detection and response times for infiltration and exfiltration by organization size

		ORGANIZATION SIZE		
PERSENT	**TOTAL**	**SMALLER**	**MEDIUM/LARGE**	**ENTERPRISE**
Base: All Respondents	**(407)**	**(83)**	**(202)**	**(122)**
Detect an infiltration				
Within hours	46.44%	49.40%	45.05%	46.72%
Within a week	42.75%	37.35%	44.55%	43.44%
Within a month	10.81%	13.25%	10.40%	9.84%
Detect a Breach				
Within hours	46.19%	46.99%	48.02%	42.62%
Within a week	43.49%	45.78%	38.61%	50.00%
Within a month	10.32%	7.23%	13.37%	7.38%
Respond to an infiltration				
Within hours	47.17%	46.99%	48.51%	45.08%
Within a week	49.14%	51.81%	46.53%	51.64%
Within a month	3.69%	1.20%	4.95%	3.28%
Respond to a breach				
Within hours	32.68%	33.73%	33.17%	31.15%
Within a week	56.27%	55.42%	54.46%	59.84%
Within a month	11.06%	10.84%	12.38%	9.02%

Recovery time is increasing

The average number of work days spent by an organization's security/IT/legal and any other relevant staff recovering from cyber security breaches increased significantly to 19.4 days, from 16.1 days in 2018. Spending more time returning to a trusted state and normal operations increases the cost of breaches, so this is a key factor in the increased cost of cyber compromise this year.

FIGURE 1. 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?



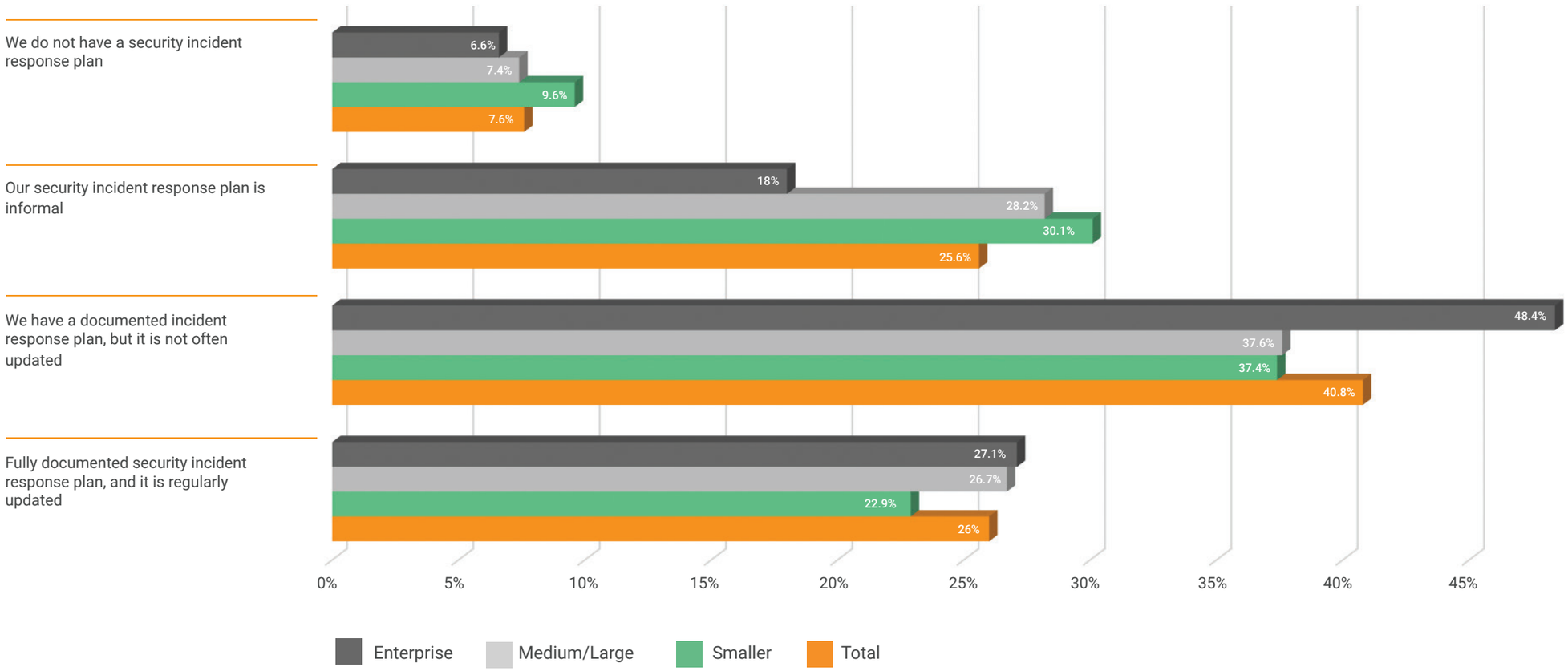
Deficiencies in planning for incident response and recovery back to trusted state leaves organizations vulnerable in the wake of a breach

Survey respondents were asked how they would best describe their organization's incident response plan. 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 included:

- 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 is not often updated
- We have a fully documented security incident response plan and it is regularly updated

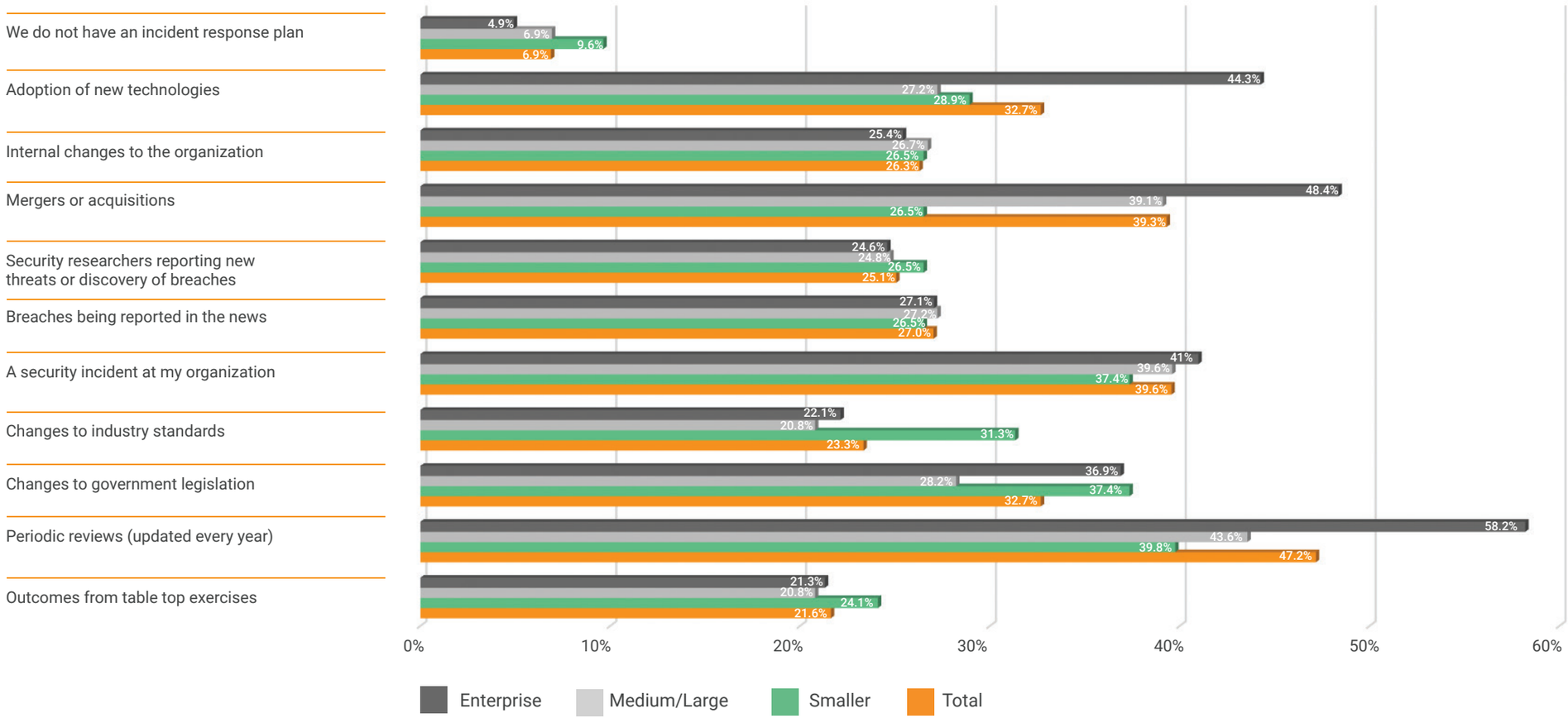
An organization's security incident response plan represents its blueprint for responding to exfiltration, infiltration, and DoS cyber security attacks and encompasses roles and responsibilities, assessment of incidents, how the plan relates to other organizational policies and procedures and any applicable reporting requirements. Approximately one quarter of survey respondents indicated that their organizations had a fully documented plan, down from 32% in 2018.

FIGURE 2. Which of the following best describes your organization's incident response plan?



An out of date incident response plan can impair an organization's response as the people, processes, and technologies it refers to may no longer be relevant. Plans need to be updated regularly, and especially whenever a significant change to an organization occurs. Adoption of new technologies, changes in staff, new legislation, and mergers and acquisitions are all examples of changes to an organization that need to be reflected in updates to its incident response plan. As more and more breaches are being reported, organizations need to be ready with an effective response plan.

FIGURE 3. What triggers your organization to update your incident response plan?



Survey respondents indicated that yearly reviews and security incidents were the top reasons for updating their incident response plans. Periodic reviews are a good starting point, but ideally plans should be updated whenever any of the events in Figure 3 occur. It is critical for organizations to conduct proactive reviews and updates of their incident response plan. The midst of a security incident is not the time to discover that your incident response plan is in urgent need of an update. If the plan is found to be out of date during an incident, of course those updates are not any less important, however, ideally this should not be the second highest reason the incident response plan is reviewed. Proactive incident response posturing leads to minimized damages and losses from a breach. For example, it may prevent an intrusion from becoming an exfiltration. Planning ahead allows for faster response.

Depending on the severity of a cyber security incident, an organization may have a long journey ahead before recovering to a trusted state and normal operations. A key objective of a proactive cyber resilience posture is reducing the amount of time an organization spends recovering to a trusted state. Recovery and business continuity planning therefore make up crucial elements of any cyber resilience plan.

Survey respondents were asked how they would best describe their organization's plans for recovery back to a trusted state and normal operations (Table 10). This included short term plans for initial response to a data breach and long-term plans for returning to normal operation.

TABLE 10. Which of the following best describes your organization's plan for recovery back to trusted state after a data breach?

		ORGANIZATION SIZE		
PERCENT	TOTAL	SMALLER	MEDIUM/LARGE	ENTERPRISE
Base: All Respondents	**(407)**	**(83)**	**(202)**	**(122)**
Provides a step-by-step process for the initial response to a data breach				
Fully detailed and documented processes	27.03%	22.89%	26.24%	31.15%
Processes are in place but documentation is not complete	37.59%	46.99%	34.65%	36.07%
Processes are in place but there is no documentation as of yet	23.10%	15.66%	25.74%	23.77%
Ad hoc processes are in place	12.29%	14.46%	13.37%	9.02%
Provides a process for recovering to a trusted state and normal operation after a breach				
Fully detailed and documented processes	36.36%	32.53%	36.14%	39.34%
Processes are in place but documentation is not complete	31.70%	33.73%	33.66%	27.05%
Processes are in place but there is no documentation as of yet	16.46%	19.28%	15.35%	16.39%
Ad hoc processes are in place	15.48%	14.46%	14.85%	17.21%

The percentage of survey respondents indicating their organization only has ad hoc plans for returning to a trusted state (15.5%) and normal operation is double the ad hoc percentage for incident response plans (7.6%). This indicates organizations are better prepared to deal with the initial response to a data breach than they are with returning to normal operations after a breach has occurred.

Having cyber resilience fundamentals in place significantly improves detection, response, and downtimes

Organizations that practice cyber resilience fundamentals experience reduced response and recovery times. When done, infiltration, breach detection, and response are more likely to occur within hours-to-a-week as opposed to weeks-to-a-month for organizations that do not.

TABLE 11. Including basic incident response and recovery plans in security planning significantly reduces time to detect and respond

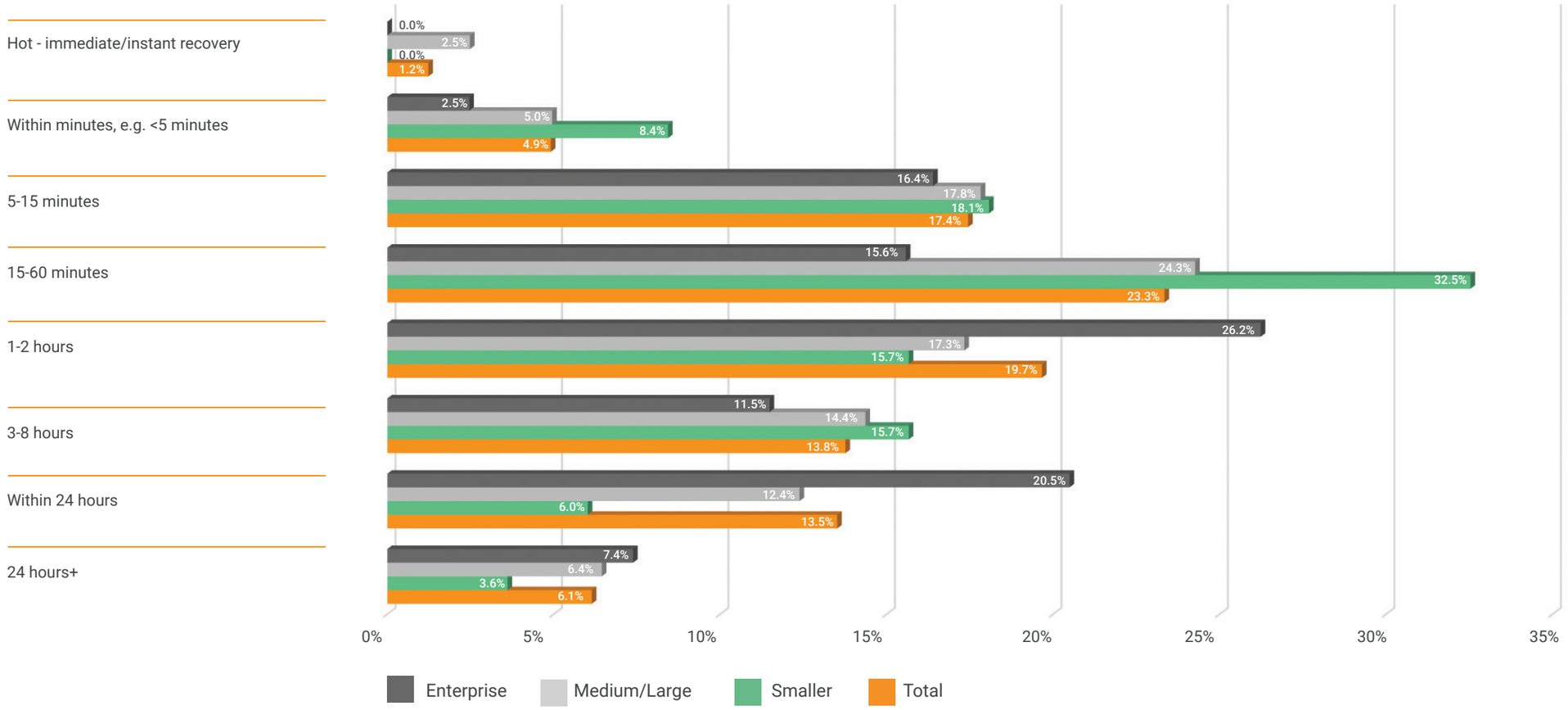
PERCENT	TOTAL	INCLUDES BASIC INCIDENT RESPONSE AND RECOVERY PLANS IN SECURITY PLANNING	BASIC INCIDENT RESPONSE AND RECOVERY PLANNING NOT INCLUDED
Base: All Respondents	**(407)**	**(110)**	**(297)**
Detect an infiltration			
Within hours-to a week	89.19%	93.63%	87.54%
Within weeks-to a month	10.81%	6.36%	12.46%
Detect a Breach			
Within hours-to a week	89.68%	91.82%	88.89%
Within weeks-to a month	10.32%	8.18%	11.11%
Respond to an infiltration			
Within hours-to a week	96.31%	98.19%	95.62%
Within weeks-to a month	3.69%	1.82%	4.38%
Respond to a breach			
Within hours-to a week	88.95%	91.82%	87.88%
Within weeks-to a month	11.06%	8.18%	12.12%

The impact of practicing cyber resilience fundamentals is especially noticeable in reducing overall time spent recovering from breaches. The average number of work days spent by an organization's security/IT/legal and any other relevant staff recovering from cyber security breaches increases from 16.4 days for organizations that practice the fundamentals (i.e. at least a basic level of overall security planning, training, patching/updating, and incident response and recovery planning) to 20.5 days for those that miss performing the fundamentals in any of these areas.

Organizations' expectations for time-to-recovery back to a trusted state remains unrealistic

Despite only 36.4% of the organizations surveyed having fully detailed and documented recovery plans, 66.5% expect to fully recover back to a trusted state and normal operations in less than 2 hours. Many organizations, particularly smaller organizations, have high but unrealistic expectations for a rapid, full recovery after a data breach.

FIGURE 4. Organization's expectations for time-to-recovery back to trusted state after a data breach situation for mission critical processes

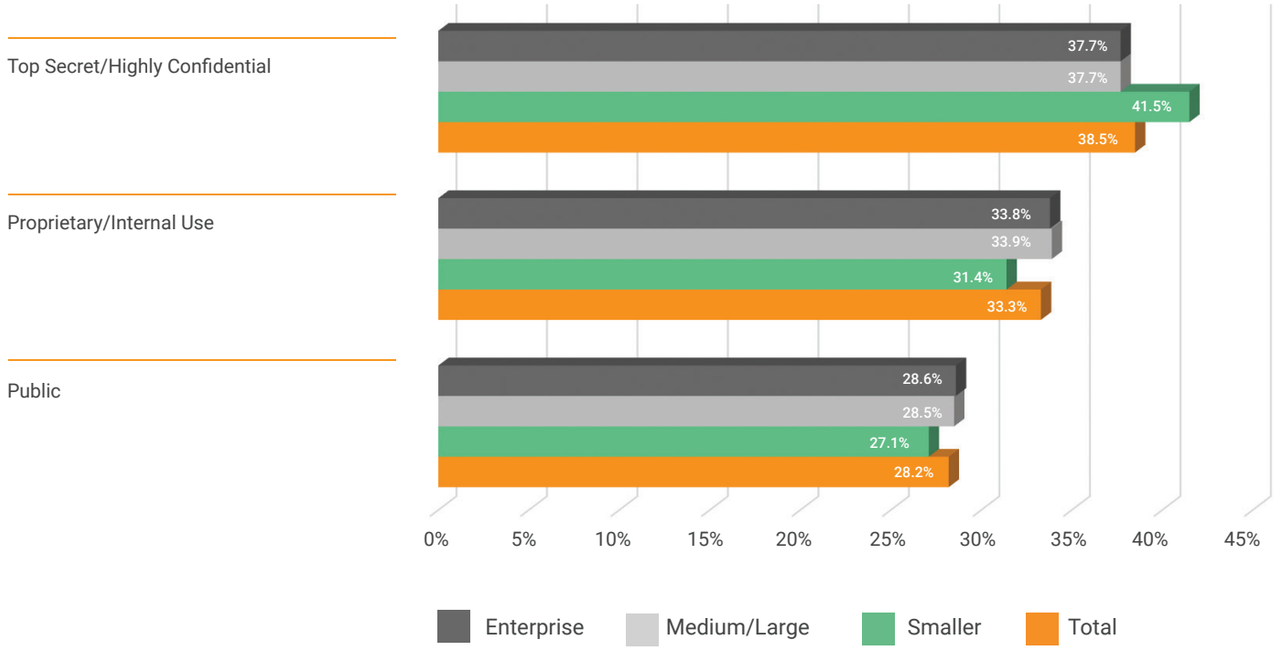


Percentage of highly confidential data is on the rise

The increase in confidential data coincides with the increased awareness of regulatory requirements such as the Canadian Data Privacy Act and GDPR. The increase in data collection for the ever expanding application of data analytics may also contribute to the increase in confidential data storage.

FIGURE 5. Organizations are storing more highly confidential data than ever

Large organizations have more data, but the percentage which is highly confidential is independent of business size.



Has your organization identified and classified all its data assets? In the event of a cyber security attack do you have a plan to ensure the confidentiality, integrity, and continued availability of your data? Does your organization train users on the proper handling of data – whether confidential, proprietary or public?

In terms of cyber resilience fundamentals, the end user is critical in dealing with risks to confidential and proprietary data.

Training end users on the proper handling procedures, policies, and practices for the different data classifications – confidential, proprietary, and public – is becoming more and more important as the amount of confidential and proprietary data increases. Despite the increase in awareness about training, 48.4% of the organizations surveyed (half of them medium/large) reported they practice no, or only ad hoc training on data handling. Furthermore, 14.5% of smaller organizations conduct no employee training at all on identifying attacks such as phishing and other scams. Correspondingly, the success rate of exfiltration and infiltration attacks against medium/large and smaller organizations is dramatically higher than it is for enterprise (see Table 12).

TABLE 12. Success rate of cyber attacks by organization size and attack type

		ORGANIZATION SIZE		
PERCENTAGE	**TOTAL**	**SMALLER**	**MEDIUM/LARGE**	**ENTERPRISE**
Base: All Respondents	**(407)**	**(83)**	**(202)**	**(122)**
Success rate of attacks as % of total IT security-related attacks or threats faced over the past 12 months				
Exfiltration	4.8%	23.3%	16.3%	1.4%
Infiltration	5.9%	41.7%	18.1%	1.6%

Study participants' top three organizational concerns all relate to end-user risk:

- Insider/malicious employee threat or risk (for example untrained end-users)
- Mobile threats (primarily target untrained end-users)
- Data not being backed up (end users may contribute significantly to this problem in many organizations)

Does your organization train users on the proper handling procedures of different data classifications?

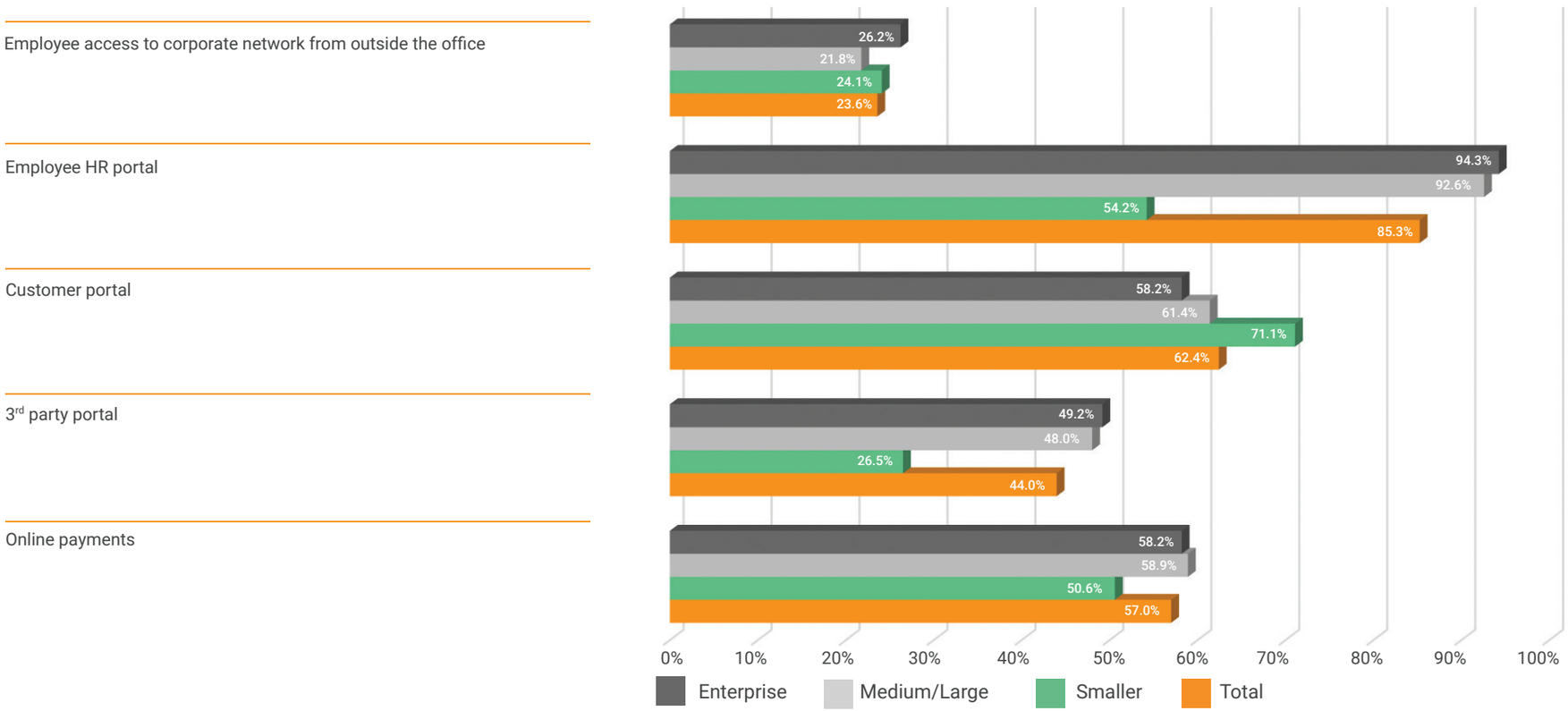

The average cost of a breach per end user is
$2,677*
*Average across all size organizations

FINDING 3: EVOLVING THREATS CREATE NEW OPPORTUNITIES FOR MALICIOUS ACTORS

Security coverage requirements keep growing

In order to help assess the level of exposure of organizational networks have to external access, survey respondents were asked how their organizations provide remote access to their networks via the internet. While these types of exposure are often necessary for business purposes, they create opportunities for malicious actors to circumvent organizational network security controls by using “man in the middle” or phishing style attacks to exfiltrate user credentials to gain access to the organization’s network.

FIGURE 6. Organizations providing remote access to their network via the internet



*Man-in-the-middle (MITM) attack is a form of eavesdropping where communication between parties who believe they are directly communicating with each other is monitored and modified by an unauthorized party. This attack type comprises a victimized party and the person they are communicating with, as well as "the man in the middle", who without any party's knowledge is intercepting the communications or data.

All survey respondents indicated their organization provides at least one type of remote access to their network through the internet. Employee HR portals are so widespread a majority of smaller organizations have even adopted them (see Figure 6). Other forms of remote access including customer portals, third party portals, online payments, and mobile employee access to the corporate network also have significant adoption. As organizations continue to adopt Software as a Service (SaaS) solutions, this will continue to increase.

Training employees to recognize attacks and to use proper password and identity management controls – especially for organizations with mobile and VPN access to the corporate network is a crucial component of practicing cyber resilience fundamentals. Smaller and medium/large organizations in particular have been deficient in this area: 14.5% of smaller organizations conduct no employee training at all on identifying attacks such as phishing and other scams, and 55.4% of medium/large organizations conduct only ad hoc or no training (Table 12 shows phishing attacks are much more successful against smaller and medium/large organizations than they are against enterprise).

Enterprise and medium/large organizations can have dozens of third-party suppliers, partners, and vendors with access to their network and data. It is important that organizations realize they are responsible for any personally identifiable information (PII) that they collect, including data that is stored and accessed by third parties. Any security strategy needs to have a holistic view of data-flows between organizations and be planned accordingly.

You are responsible for properly securing your network and training your employees, as well as for ensuring that third parties are properly handling and securing your data. Ensure you understand the data-flow between third-party suppliers, partners, and vendors and your organization.

Year over year Canadian organizations are taking partner security more seriously, with 38% indicating they have considered partner security in a comprehensive manner when creating a security plan, up from 26% in 2018.

TABLE 13. Does your security plan consider your key suppliers and third-party relationships, and the data flows between them?

		ORGANIZATION SIZE		
MEANS	TOTAL	SMALLER	MEDIUM/LARGE	ENTERPRISE
Base: All Respondents	**(407)**	**(83)**	**(202)**	**(122)**
Yes - in a comprehensive manner	38%	41%	37%	37%
Yes - but we should look at this in more detail	54%	57%	54%	51%
No	9%	2%	9%	12%
Not sure/don't know	0%	0%	0%	0%

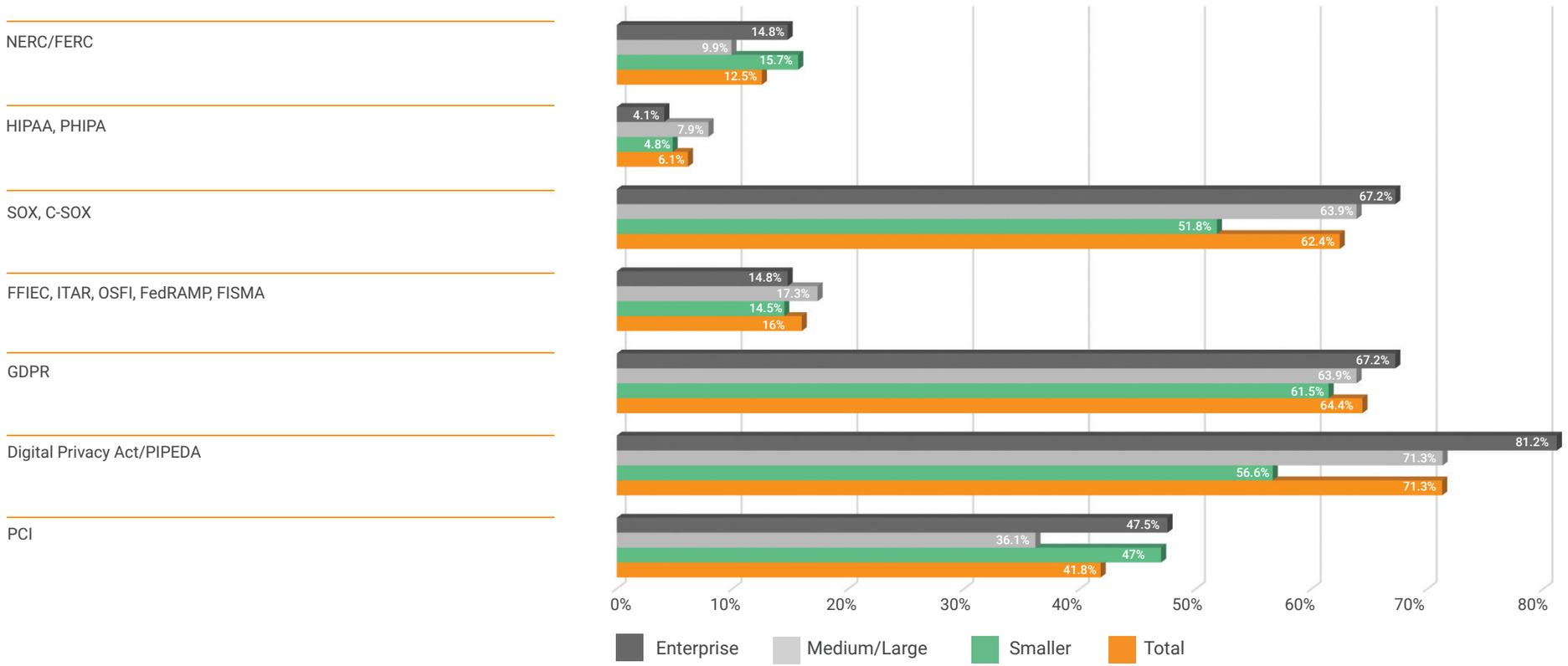
Still, 54% of organizations admit they have not considered third-party relationships in a comprehensive manner, and 9% indicate they have not considered third-party relationships at all. This is especially concerning for enterprise organizations with 12% admitting they have not considered third-party relationships when creating their security plan.

Canadian organizations are becoming more concerned about third-party security but there is more work to be done. Only 38% of survey respondents indicated that their organizations consider third-party security in a comprehensive manner when creating a security plan.

Canadian organizations faced stringent government regulations in 2018

The majority of Canadian organizations report that their organizations are required to comply with a number of government or industry regulations, which indicates that they have fairly high privacy/data security protocols. Fifty-five percent of respondents indicate their organization must comply with three or more of the government or industry regulations we asked them about. While not all organizations handle personal information in the course of commercial activity as detailed in PIPEDA or the Digital Privacy Act, it would still be favourable to comply with the general principles advocated by those legislations.

FIGURE 7. Which of the following government or industry regulations does your organization need to be compliant with?

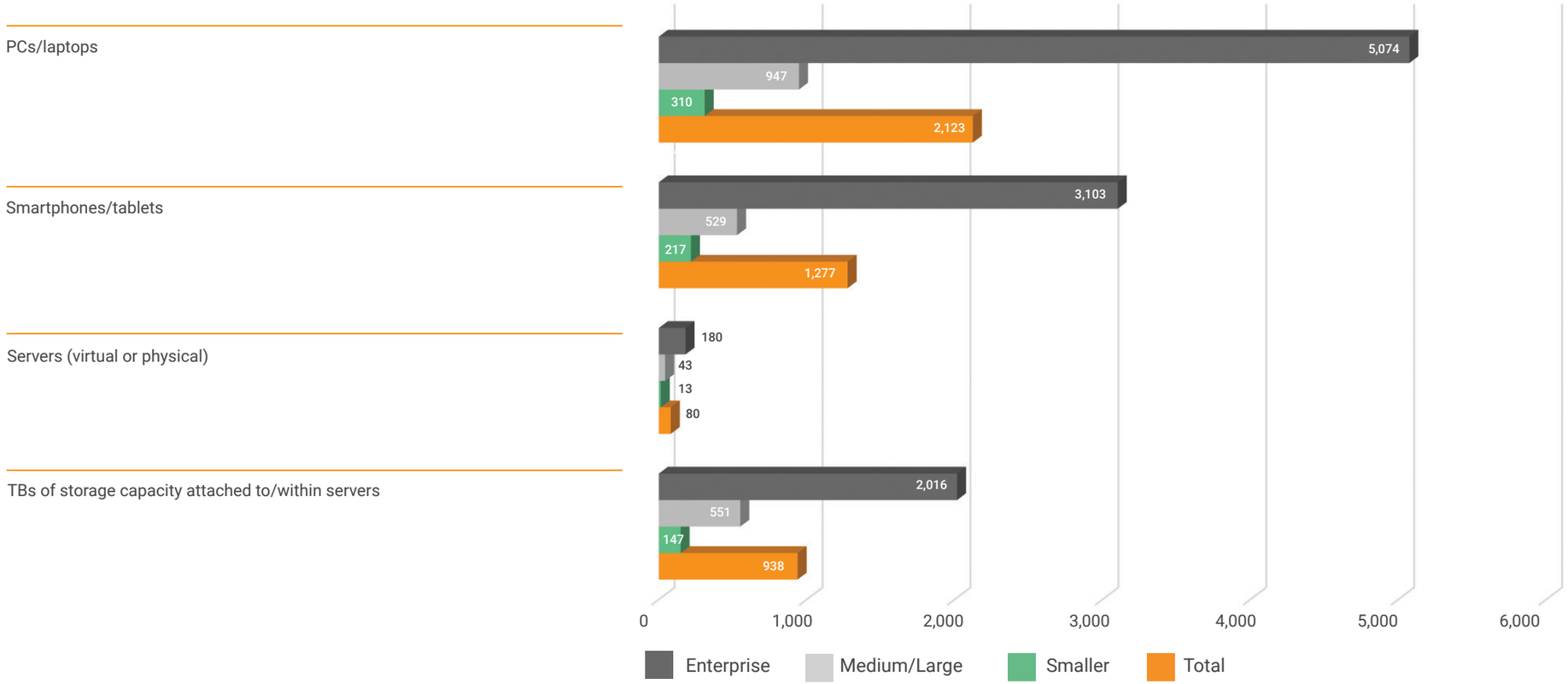


On November 1st, 2018 Mandatory Breach notification was brought into effect under PIPEDA, bringing steep fines to organizations who fail to disclose data breaches to the Privacy Commissioner and affected customers. This legislation applies to the vast majority of Canadian organizations that handle personal information in the course of commercial activity. If one of your partner organizations is breached and your data is exposed, your organization could be liable as well.

The Attack Surface Continues to Evolve

The attack surface for devices was estimated by asking respondents for their networked device and hardware counts. The number of networked devices and hardware increased exponentially with organization size, yet the larger attack surface for enterprise organizations did not translate to a higher number of security incidents. In general, enterprise organizations appear to be doing a better job of securing their attack surface despite having much more devices and hardware.

FIGURE 8. Attack surface in terms of average number of networked devices/hardware increases exponentially as organization size increases



In terms of device/hardware counts, market trends including "Bring Your Own Device" (BYOD), cloud adoption, and lower storage prices have affected what is connected to the network. Within the organization sizes surveyed (minimum 15 employees for smaller organizations, enterprise is 5,000+ employees) laptop deployment decreased to 2,123 per organization in 2019 versus 2,333 in 2018, smartphones decreased to 1,277 in 2019 versus 1,716 in 2018, and servers decreased to 80 in 2019 versus 187 in 2019, while storage capacity increased by 344% to 938 TB from 273 TB in 2018.

FINDING 4: CLOUD SECURITY STRATEGY IS NOT KEEPING UP WITH THE RATE OF ADOPTION

Canadian organizations have embraced cloud (see Figure 9), but many have not done so in a secure way. An organization's cloud strategy needs to be integrated into its cyber security strategy, but for many, securing the cloud comes as an afterthought. Recently the media has highlighted several large-scale breaches of IaaS and PaaS environments caused by a lack of basic security controls and configuration errors. Organizations need to understand that securing public cloud environments is a shared responsibility between customer and provider, and customers' responsibilities vary between SaaS, PaaS, and IaaS. In reality, malicious actors are not concerned with where an organization's data is stored and will seek out vulnerabilities regardless of the IT environment. It is crucial for organizations to integrate security into their cloud roadmap and understand their responsibilities for securing these environments.

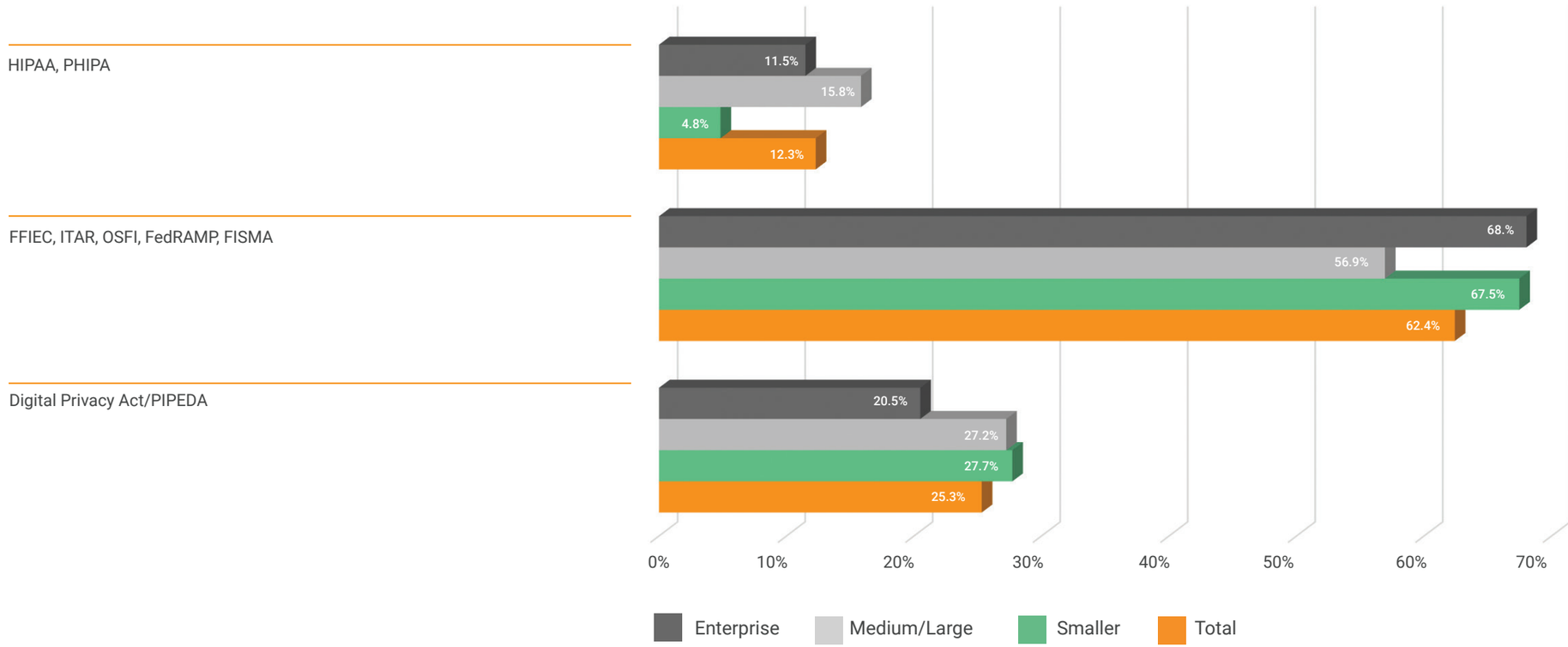
TABLE 14. Number of attacks on on-premise infrastructure and applications versus cloud-based infrastructure and applications

		ORGANIZATION SIZE		
MEANS	**TOTAL**	**SMALLER**	**MEDIUM/LARGE**	**ENTERPRISE**
Base: All Respondents	**(407)**	**(83)**	**(202)**	**(122)**
Attacks against on-premise infrastructure/applications	214.06	35.73	85.22 (139% increase from Smaller)	548.71 (544% increase from Medium/Large)
Attacks against cloud-based infrastructure/applications	216.05	22.83	77.23 (238% increase from Smaller)	577.36 (648% increase from Medium/Larger)

One in ten Canadian organizations have completely migrated to cloud

In Canada, 75% of organizations have either fully adopted cloud or are using a hybrid model of on-premise environments complimented by either IaaS or PaaS. Smaller organizations are more likely to remain on-premise, while medium/large and enterprise organizations are more likely to go entirely cloud-based.

FIGURE 9. Three quarters of organizations have embraced cloud but not necessarily in a secure way



Organizations fail to update and patch cloud environments as quickly as on-premise

When updating and patching, Canadian organizations give higher priority to their on-premise infrastructure, operating systems, and applications than their public cloud environments. Survey respondents indicated that their organizations are patching on-premise network equipment, databases, apps, servers, and web applications faster than their public cloud environments. Less than 60% of Canadian organizations update/patch public cloud environments within a week of patch releases, versus 63% for on-premise network equipment, and 75% for on-premise databases, apps, servers, and web applications. Medium/large organizations are the slowest to update and patch their cloud environments.

TABLE 15. On-premise IT environments are given priority for installing security updates/patches and upgrades over public cloud

		ORGANIZATION SIZE		
MEANS	**TOTAL**	**SMALLER**	**MEDIUM/LARGE**	**ENTERPRISE**
Base: All Respondents	**(407)**	**(83)**	**(202)**	**(122)**
Network Equipment				
Immediately when released	10%	10%	11%	9%
Within a week	53%	52%	51%	58%
Within a month	31%	33%	33%	28%
Within a year or longer	5%	6%	5%	5%
On-premise databases, apps, servers				
Immediately when released	23%	30%	20%	22%
Within a week	52%	45%	54%	55%
Within a month	25%	25%	25%	23%
Within a year or longer	0%	0%	1%	0%
Web Applications				
Immediately when released	29%	30%	29%	28%
Within a week	47%	40%	49%	48%
Within a month	24%	30%	22%	24%
Within a year or longer	0%	0%	0%	0%
Public Cloud				
Immediately when released	7%	5%	7%	10%
Within a week	51%	58%	48%	53%
Within a month	38%	35%	43%	34%
Within a year or longer	3%	2%	3%	3%

Updating/patching within a reasonable time period is a key component of practicing cyber resilience fundamentals. Taking longer than a month to install security updates, patches, and upgrades leaves a significant amount of time for malicious actors to exploit vulnerabilities in out-of-date infrastructure, operating systems, and solutions.

Of the survey respondents, 8.4% indicated that it took them longer than a month to patch an aspect of their IT environment. Over 90% of these respondents understood the risks associated with unpatched IT environments, with 59% unable to update/patch faster due to IT and business reasons. Of greater concern, one third of these respondents indicated that they were aware of the risks they were exposing their organization to but were willing to take these risks or had no particular reason why they didn't patch or update sooner.

TABLE 16. Does your organization understand the potential security risks and vulnerability it is exposing itself to by not updating/patching on a timely basis?

		ORGANIZATION SIZE		
MEANS	**TOTAL**	**SMALLER**	**MEDIUM/LARGE**	**ENTERPRISE**
Base: All Respondents	**(34)**	**(7)**	**(17)**	**(10)**
No				
No Not fully, we need more education	9%	14%	6%	10%
Yes (net)	91%	86%	94%	90%
Yes - and there's really no good reason why we don't update/patch sooner	24%	29%	24%	20%
Yes - but for various IT or business-related reasons we can't update/patch any sooner	59%	43%	65%	60%
Yes - but for our risk profile versus the pain/issues we have implementing certain updates/patches it's a risk we are willing to take	9%	14%	6%	10%

FINDING 5: STRATEGY FOCUS IS SHIFTING FROM PROTECTION TO DETECTION AND RESPONSE

In a market as heavily fragmented as security, selecting the proper security controls, tactics, and tools is an ongoing priority for Canadian organizations. As budgets are finite, organizations must carefully consider and invest in the security solutions that will be most effective at reducing risk based on each individual environment and their business objectives. Today, many organizations find traditional perimeter and endpoint security controls most effective at protecting their organizations, but this viewpoint is set to change significantly over the next three years. By 2022, Canadian organizations expect that detection controls based on artificial intelligence and machine learning will significantly add to the security of their organizations.

Table 17 presents survey respondents' perception of the security controls/tactics/tools that will be most effective at adding to their security position three years from now versus what is most effective today.

TABLE 17. Which controls, tactics, or tools do you feel have been the most effective at protecting your organization from cyber security threats over the past year, and which would be most interested in looking at to add additional effectiveness over the next three years?

	ORGANIZATION SIZE	
SECURITY CONTROL/TACTIC/TOOL	TODAY	3 YEARS
Controls		
Email Security	61%	18%
Identity and Access Management	60%	15%
Web Content Filtering	58%	20%
Vulnerability Management	48%	22%
Endpoint Protection	43%	25%
Data Security (encryption/DLP)	26%	50%
Security Monitoring (SIEM, Log Management)	24%	53%
DNS Security	23%	21%
Next Generation Firewalls/IPS	20%	57%

Continued on next page

Continued from previous page

	ORGANIZATION SIZE	
SECURITY CONTROL/TACTIC/TOOL	**TODAY**	**3 YEARS**
User Behaviour Analytics (UBA)	20%	45%
Endpoint Detection and Response (EDR)	17%	33%
Tactic		
Security Awareness Training	44%	19%
Threat Hunting	19%	50%
Tools		
Risk and Compliance Automation	17%	14%
Breach Response and Forensics Tools	13%	46%
Security Orchestration Tools	6%	13%

The following are the major trends in technology, tactics, and tools we expect to see over the next 3 years:

Organizations use the full feature set of their Next Generation Firewalls (NGFWs). Many organizations have next generation firewalls in place, but few actually use them to their full advantage. Modern NGFWs can handle items such as identity management, malware, antivirus analysis, and compliance, however complex configurations, licensing fees, and throughput concerns hamper adoption. As more vendors build out security platforms and fabrics, Canadian organizations expect tight integration between their NGFWs and other security controls to better secure their organizations. Higher performing ASICs and simpler licensing will allow more organizations to leverage advanced NGFW features.

Monitoring controls become a necessity. Continuous monitoring of the network and endpoint via SIEM and EDR is viewed as being pertinent to security effectiveness in the future. Monitoring controls are becoming more important, but so are monitoring tactics such as threat hunting.

Increased focus on internal threats. Data security controls such as data loss protection (DLP) control user access under specified conditions, while UBA can detect unusual user activity. The ability of UBA to increase proactive cyber resilience by helping identify anomalous behaviour will increase over time as the amount of data available for analysis (alerts generated) increases with protection technology deployment.

Increased breach response and forensics tools adoption. Breach response and forensics tools trailed only NGFWs in respondents' perception of security controls that will be most effective at adding to their security position in the future. An increased focus on response will improve the cyber resilience of Canadian organizations.

Enterprise organizations see tactics and tools as the most effective way to secure their organizations

Today, regardless of size category, organizations have similar views as to what security controls are most effective at securing their organizations, but there is significant divergence looking ahead. Enterprise organizations are the only organizations to rank security awareness training as a top 5 most effective technology, tactic, or tool today, but over the next three years threat hunting, and breach response and forensics tools will top their lists. Respondents from Smaller and Medium/Large organizations indicated that NGFWs will be the most effective at securing their businesses in three years' time.

TABLE 18. Most effective security controls/tactic/tools by organization today

RANK	SMALLER	MEDIUM/LARGE	ENTERPRISE
1	Web Content Filtering	Identity and Access Management	Email Security
2	Identity and Access Management	Email Security	Web Content Filtering
3	Email Security	Web Content Filtering	Identity and Access Management
4	Vulnerability Management	Vulnerability Management	Security Awareness Training
5	Data Security (encryption/DLP)	Endpoint Protection	Endpoint Protection

TABLE 19. Security controls/tactics/tools most interested in looking at to add additional effectiveness over the next three year

RANK	SMALLER	MEDIUM/LARGE	ENTERPRISE
1	Next Generation Firewalls/IPS	Next Generation Firewalls/IPS	Threat Hunting
2	User Behaviour Analytics	Security Monitoring	Breach Response and Forensics Tools
3	Security Monitoring	Data Security (encryption/DLP)	Security Monitoring
4	Data Security (encryption/DLP)	Threat Hunting	Next Generation Firewalls/IPS
5	Threat Hunting	Breach Response and Forensics Tools	User Behaviour Analytics

PART 4:
CONCLUSIONS

PART 4: CONCLUSIONS

Canadian organizations are still too confident in their capabilities to successfully defend against cyber security attacks, but changes in behaviour are occurring. The new normal of cyber security breaches occurring on a regular basis has organizations rethinking their cyber security strategies. Many recognize future need to adopt technologies, leveraging artificial intelligence and machine learning that can more proactively detect malicious activity on networks and devices, but still have deficiencies in how they handle the security risk created by people and inadequate cyber security planning. Organizations that understand cyber resilience and take a holistic approach encompassing more than just the protection provided by security controls suffer far fewer security incidents, and significantly reduce the costs associated with them.

Although the average number of cyber attacks per organization declined slightly this year, the costs associated with cyber security incidents has risen. Malicious actors shifted their attack volume to enterprise, as attack success rates were dramatically lower for this size group than for smaller and medium/large organizations. The average annual hard and soft costs per organization of addressing cyber security incidents varies by category: $4.8 million for exfiltration, $4.6 million for infiltration, and $5.8 million for DoS. Increased network downtime and days spent recovering after a breach were significant factors in the higher cost of cyber security incidents reported this year.

KEY CALLS-TO-ACTION FOR CANADIAN ORGANIZATIONS

Conduct Regular Threat Risk Assessments (TRAs)

Before a cyber resilience plan can be created or updated, an organization must understand its current vulnerabilities and the risks associated with them. There are a number of frameworks available for assessing risk such as NIST 800-30 and Open FAIR, but calculating risk is complicated and many organizations turn to a third party for help. As modern organizations have a constantly evolving attack surface, it is important to understand the acceptable level of risk before investing in resources to secure assets. TRAs can provide insight into these considerations, and should be conducted regularly, and especially whenever any significant change occurs to the business.

Create a cyber resilience plan and keep it up to date

The NIST Cyber Security Framework is an excellent guide for organizations to create a cyber resilience plan. Many organizations focus too strongly on protection – investing in security controls – rather than detection and response capabilities. Ensure your plan covers the full NIST cyber security stack including identify, protect, detect, respond, and recover. Cyber resilience plans need to be updated whenever a TRA is conducted. However, following a framework does not guarantee security. It is important to ensure you implement a framework in an effective way, based on your business objectives and environment. Know which assets require the highest levels of protection. Be sure that you have a well-defined and up to date incident response plan that is reviewed and rehearsed often through simulated exercises.

Practice cyber resilience fundamentals

Creating a cyber resilience plan is a great start but adhering to it can be challenging. Organizations that conduct the fundamentals of cyber resilience on an ongoing basis significantly improve their security posture; implementing even basic incident response and recovery plans has significant benefits versus having no plans at all.

Cloud security should be included in adoption roadmap planning

As the rate of cloud adoption continues to accelerate, considerations regarding cyber resilience planning for cloud is critical, including patching, visibility, and the shared responsibility model. Cloud infrastructure is targeted as often as on-premise infrastructure and therefore its security posturing should be defined as a part of the migration. To help with this, be sure you are familiar with the applicable shared responsibility for your consumption model.

Shifting sole focus from protection, to including monitoring and response

If your protection strategy is effective, we do not recommend discontinuing it. However, there are an ever-increasing number of logs and alerts as more effective protection solutions are deployed. Keep an eye on how machine learning and AI are affecting solutions and offerings in the marketplace.
If your organization handles PII, and a breach does happen to occur, having a strong monitoring & response strategy will be key in your ability to report on the breach and remediation.

PART 5:
CAVEATS

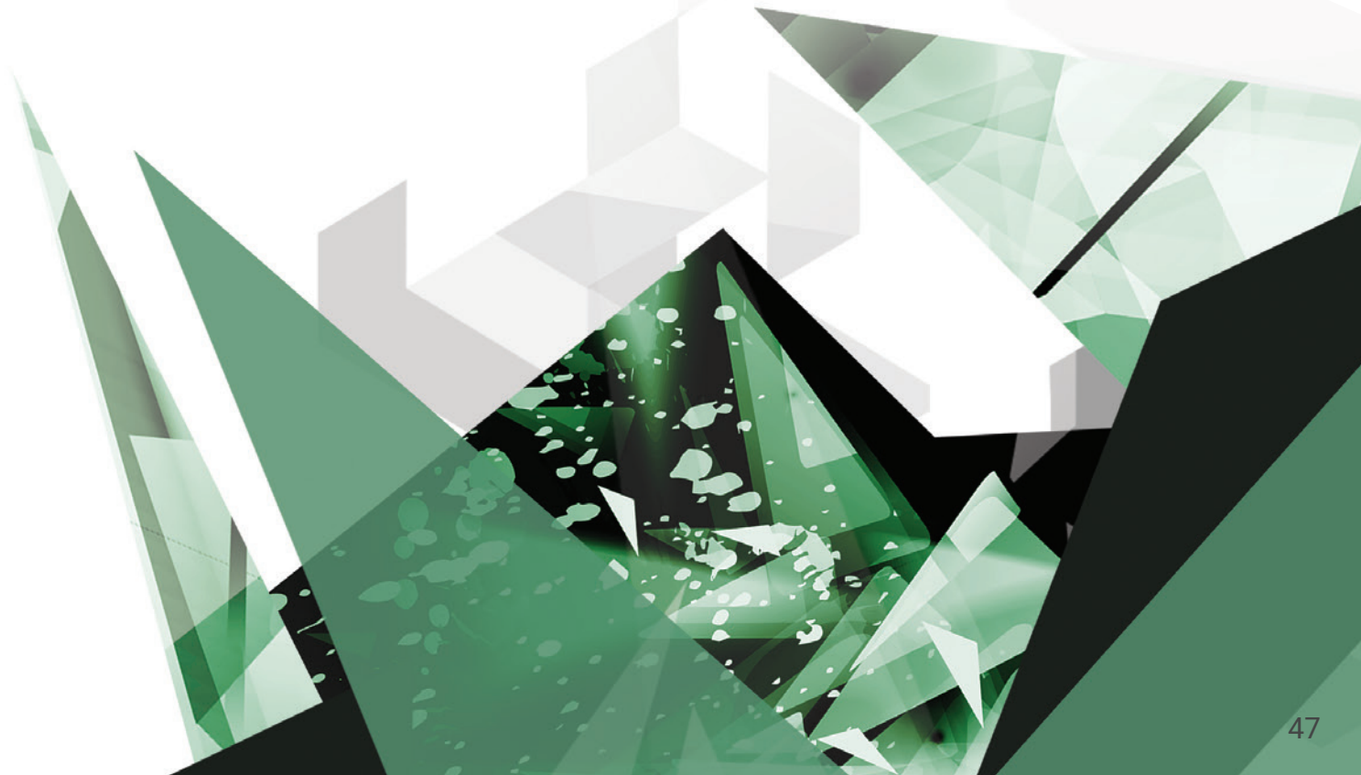
PART 5: CAVEATS

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.



APPENDIX:
DETAILED SURVEY RESULTS

APPENDIX A: DETAILED SURVEY RESULTS

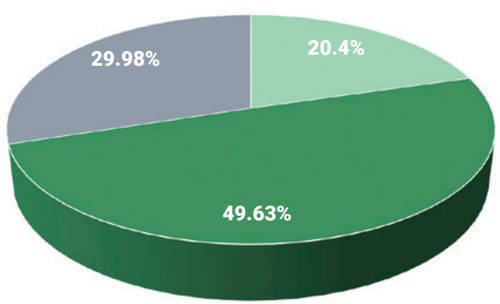
DEMOGRAPHICS: A sampling frame of 4,688 Canadian IT security and risk & compliance professionals were selected to receive invitations to participate in this survey. All survey participants were screened for direct involvement in improving or managing their organization's IT security. The following table shows the returns including the removal of certain participants based on screening and reliability checks. Our final sample consisted of 407 surveys, or an 8.6% response rate.

The survey firmographics and demographics are as follows:

PIE CHART 1: Employee Size Range

Total:

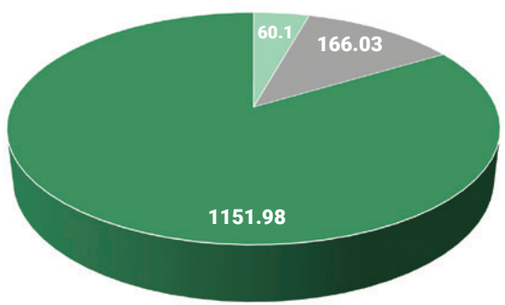
- Smaller: 15-249
- Medium/Large: 250-4,999
- Enterprise: 5,000+



PIE CHART 2: Classification Based on Attacks per Year

Total:

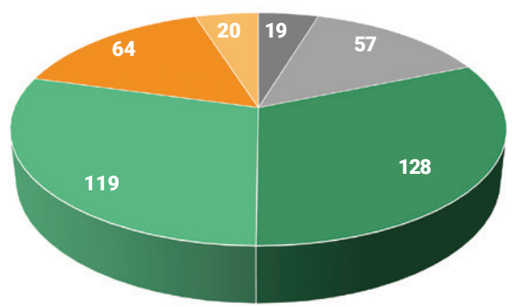
- Smaller
- Medium/Large
- Enterprise



PIE CHART 3: Number of Full-Time IT Staff

Total:

- 1-2
- 3-5
- 6-15
- 16-40
- 41-99
- 100 or more

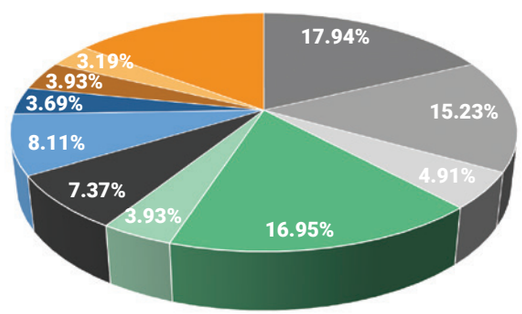


PIE CHART 4: Level of Respondent

Total:

- IT Executive - eg. CIO/CTO/VP, CSO/CISO
- IT Director
- Infosec Director
- IT Manager
- Infosec Manager
- IT Supervisor
- Infosec Supervisor
- IT Staff/Associate/Technician
- IT Associate/Staff
- IT Consultant/Contractor
- Legal/Compliance/Risk

Executive,Manager or Staff



Detailed Survey Results

S1.

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

	TOTAL
Base: All Respondents	**(407)**
Business/Professional Services (eg. Legal, Accounting, Engineering, Architecture, etc.)	7.62%
Personal/Consumer Services (eg. Travel, Beauty, Personal Training, Dry Cleaning etc.)	3.93%
Construction	6.63%
Hospitality	6.14%
IT industry	9.58%
Not for profit	
Manufacturing	8.60%
Crown Corporation or other publicly funded organization	0.25%
Education K-12	
Education College/University	3.93%
Financial Services	7.62%
Government	3.69%
Healthcare	4.67%
Primary (eg. Agriculture, Mining, Forestry, etc.)	
Oil & Gas or Field Services related	4.18%
Retail	5.16%
Communications (eg. Cable and Telecommunications Services, etc.)	4.18%
Media (eg. Radio/TV Broadcasting)	5.90%
Printing, Publishing, etc.	3.93%
Transportation and Warehousing	5.16%
Utilities	4.67%
Wholesale and Distribution	4.18%
Other (please specify)	
Don't know	

S1a.

Which level of government best describes your organization?

	TOTAL
Base: All Respondents Who Select Government at S1	**(15)**
Federal	13.33%
Provincial	73.33%
Municipal	13.33%

S2.

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

	TOTAL
Base: All Respondents	**(407)**
1 - 14	
15 - 24	5%
25 - 99	4%
100 - 249	11%
250 - 499	13%
500 - 999	18%
1,000 - 4,999	18%
5,000+	30%
Don't know	
Mean	2,253.60

S3.

What percentage of your total employees are located within Canada?

	TOTAL
Base: All Respondents	**(15)**
1% - 9%	
10% - 25%	15%
26% - 50%	15%
51% - 75%	20%
76% - 100%	50%
Don't know	
Mean	64.84%

S4.

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

	TOTAL
Base: All Respondents	**(407)**
Not headquartered in Canada	
Western and Central Canada (BC, AB, SK, MB)	25.06%
Ontario	24.82%
Québec	25.06%
Atlantic Canada (NB, NS, NFLD, PEI)	25.06%
Yukon	
Northwest Territories	
Nunavut	

S6.

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

	TOTAL
Base: All Respondents	**(407)**
None	
1 - 2	5%
3 - 5	14%
6 - 15	31%
16 - 40	29%
41 - 99	16%
100 or more	5%
Mean	28.04

S7.

Which of the following best describes the department you work for?

	TOTAL
Base: All Respondents	**(407)**
Administration	
Customer Support	
C-level Executive Management excluding IT	9.83%
Line of Business Management excluding IT	
CIO/CTO/CSO/CISO, etc.	8.35%
Finance/Accounting	
Human Resources	
IT/IS/MIS/Data Centre/IT Security	67.81%
Legal/Compliance/Risk	14.00%
Logistics	
Manufacturing/Production	
Sales/Marketing	
Purchasing/Procurement	
Research & Development/Engineering excluding IT	
Other	

S7a.

Do you directly manage IT security for your organization?

	TOTAL
Base: All Answering "C Level Executive Management Excluding IT" at S7	**(40)**
YES	100.00%
NO	

S8.

At your organization, do you play a role in, or are you part of any of the following:

	TOTAL
Base: All Respondents Answering "No" to Q: S7a	**(367)**
Directing the IT function	45.78%
Improving/Managing IT security	100.00%
Setting IT priorities	35.69%
Managing IT budgets	33.24%

S9.

Which of the following best describes your job title?

	TOTAL
Base: All Respondents	**(407)**
IT Executive - eg. CIO/CTO/VP, CSO/CISO	17.94%
IT Director	15.23%
Infosec Director	4.91%
IT Manager	16.95%
Infosec Manager	3.93%
IT Supervisor	7.37%
Infosec Supervisor	8.11%
IT Staff/Associate/Technician	3.69%
IT Associate/Staff	3.93%
IT Consultant/Contractor	3.19%
Legal/Compliance/Risk Executive, Manager, or Staff	14.74%
Don't know	

S10.

How many IT security staff are employed at your organization?

	TOTAL
Base: All Respondents	**(407)**
1 - 2	19
3 - 5	57
6 - 15	128
16 - 40	119
41 - 99	64
100 or more	20
Mean	6.43

S11.

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

	TOTAL
Base: All Respondents	**(407)**
Less than $10 million	5.41%
$10 million - $25 million	18.67%
$26 million - $99 million	26.29%
$100 million - $499 million	28.50%
$500 million - $999 million	14.99%
$1 billion or more	6.14%
Mean	364.45

Q1.

Which of the following government or industry regulations does your organization need to be compliant with?

	TOTAL
Base: All Respondents	**(407)**
PCI	41.77%
Digital Privacy Act/PIPEDA	71.25%
GDPR	64.37%
FFIEC, ITAR, OSFI, FedRAMP, FISMA	15.97%
SOX, C-SOX	62.41%
HIPAA, PHIPA	6.14%
NERC/FERC	12.53%
Other	0.25%

Q2.

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

SUMMARY: Mean	TOTAL
Base: All Respondents	**(389)**
PCs/Laptops	2,122.97
Smartphones/Tablets	1,276.56
Servers (virtual or physical)	80.33
TBs of storage capacity attached to/within servers (not in PC, smartphone, or other devices)	938.13

Q3.

Please indicate how your organization uses the internet to connect with its employees, partners, and customers.

	TOTAL
Base: All Respondents	**(407)**
Online payments	57.00%
3rd party portal	43.98%
Customer portal	62.41%
Employee HR portal	85.26%
Employee access to corporate network from outside the office	23.59%
None of these apply	

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	**(407)**
Top Secret/Highly Confidential	38.45%
Proprietary/Internal Use	33.32%
Public	28.23%

Q5.

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

	TOTAL
Base: All Respondents	**(407)**
Mean	10,503.69

Q6.

Percentage of total annual IT budget devoted to security?

	TOTAL
Base: All Respondents	**(407)**
Mean	9.78%

Q7.

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

	TOTAL
Base: All Respondents	**(407)**
Staff Portion of IT security budget	35.45%
All other costs	64.55%

Q8.

Which of the following best describes how your organization approaches the following:

	TOTAL
Base: All Respondents	**(407)**
a. Taking inventory of applications, devices and systems.	
Not conducted	7.62%
Conducted across select areas/departments of the organization	51.60%
Conducted across the entire organization	40.79%
b. Discovering/assessing security weaknesses/ vulnerabilities across applications, devices, and systems.	
Not conducted	5.41%
Conducted across select areas/departments of the organization	51.84%
Conducted across the entire organization	42.75%
c. Assessing the business impact of data loss/corruption, disruption of work.	
Not conducted	17.20%
Conducted across select areas/departments of the organization	46.93%
Conducted across the entire organization	35.87%
d. Prioritizing deployment of specific security solutions.	
Not conducted	11.79%
Conducted across select areas/departments of the organization	50.37%
Conducted across the entire organization	37.84%

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	**(407)**
YES - in a comprehensive manner	37.84%
YES - but we should look at this in more detail	53.56%
NO	8.60%
Not sure/Don't know	

Q10.

Please select the five security controls, tactics or tools you feel have been the most effective at protecting your organization from cybersecurity threats over the past year, and which (different) five you would be most interested in looking at to add additional effectiveness over the next three years:

PAST YEAR	TOTAL
Base: All Respondents	**(407)**
Data Security (Encryption/DLP)	26.04%
DNS Security	23.10%
Identity and Access Management	60.44%
Next Generation Firewalls/IPS	20.39%
Web Content Filtering	57.99%
Email Security	60.93%
Security Monitoring (SIEM, Log Management)	24.32%
User Behaviour Analytics	20.15%
Vulnerability Management	47.91%
Endpoint Protection	43.00%
Endpoint Detection and Response (EDR)	17.20%
Threat Hunting	19.16%
Security Awareness Training	43.73%
Breach Response and Forensics Tools	13.27%
Risk and Compliance Automation	16.71%
Security Orchestration Tools	5.65%

NEXT THREE YEARS	TOTAL
Base: All Respondents	**(407)**
Data Security (encryption/DLP)	50.37%
DNS Security	20.64%
Identity and Access Management	15.23%
Next Generation Firewalls/IPS	57.25%
Web Content Filtering	20.15%
Email Security	17.69%
Security Monitoring (SIEM, Log Management)	53.07%
User Behaviour Analytics	44.96%
Vulnerability Management	21.62%
Endpoint Protection	24.57%
Endpoint Detection and Response (EDR)	32.68%
Threat Hunting	49.88%
Security Awareness Training	18.92%
Breach Response and Forensics Tools	45.95%
Risk and Compliance Automation	14.25%
Security Orchestration Tools	12.78%

Q11.

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

	TOTAL
Base: All Respondents	**(407)**
a. To frequently update PC and smartphone OS and apps.	
No training	10.07%
Ad hoc training and reminders	37.35%
Formal training with reminders as required by new threats, etc.	52.58%
b. How to use security technology.	
No training	12.29%
Ad hoc training and reminders	38.33%
Formal training with reminders as required by new threats, etc.	49.39%
c. How to identify attacks such as phishing and other scams.	
No training	9.09%
Ad hoc training and reminders	41.03%
Formal training with reminders as required by new threats, etc.	49.88%
d. Proper care of sensitive data such as customer/other employee private data.	
No training	8.11%
Ad hoc training and reminders	40.29%
Formal training with reminders as required by new threats, etc.	51.60%

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?

	TOTAL
Base: All Respondents	**(407)**
a. On-premise databases, apps, servers (and the operating systems + applications running on your on-premise infrastructure).	
Immediately when released	22.85%
Within a week	52.33%
Within a month	24.57%
Within a year	
A year or more	0.25%

b. Web applications.

Immediately when released	28.99%
Within a week	46.68%
Within a month	24.32%
Within a year	
A year or more	

c. Network equipment.

Immediately when released	10.32%
Within a week	53.07%
Within a month	31.20%
Within a year	4.91%
A year or more	0.49%

d. Public cloud (IaaS/PaaS) (and the operating systems + applications running on cloud infrastructure that your organization administers/manages).

Immediately when released	7.37%
Within a week	51.35%
Within a month	38.33%
Within a year	2.95%
A year or more	

Q13.

Does your organization understand the potential security risks and vulnerability it is exposing itself to by not updating/patching on a timely basis?

	TOTAL
Base: Respondents Answering "Within a Year" or "A Year or More" for Q12	**(34)**
NO	
Not fully, we need more education	8.82%
YES (NET)	91.18%
YES - and there's really no good reason why we don't update/patch sooner	23.53%
YES - but for various IT or business-related reasons we can't update/patch any sooner	58.82%
YES - but for our risk profile versus the pain/issues we have implementing certain updates/patches it's a risk we are willing to take	8.82%

Q14.

Please estimate how many times your organization has been subject to an IT security related attack or threat over the past twelve months:

	TOTAL
Base: All Respondents	**(407)**
0	
1 - 50	34.64%
51 - 100	16.22%
101 - 200	17.44%
201 - 500	18.43%
501 - 700	3.19%
701 - 1000	1.97%
1001 - 1500	0.98%
1501 - 2000	1.72%
2001 - 3000	1.47%
3001 - 4000	0.74%
4001 - 5000	2.21%
5000 +	0.98%
Mean	439.97

Q14a.

Is your organization entirely on-premise or entirely cloud-based?

	TOTAL
Base: All Respondents	**(407)**
We are a mix of on-premise and cloud	62.41%
Entirely on-premise	25.31%
Entirely cloud-based	12.29%

Q15.

Please estimate the number of attacks your on-premise infrastructure/applications were subject to versus your cloud-based infrastructure/applications:

a. **Attacks against on-premise infrastructure/ applications.**

	TOTAL
Base: All Respondents	**(407)**
Mean	214.06

b. **Attacks against cloud-based infrastructure/ applications.**

Mean	216.05

Q16.

Please indicate whether your organization experienced any of the following as a result of attacks it faced over the past year:

	TOTAL
Base: All Respondents	**(407)**
Denial of service (network went down)	34.15%
Infiltration (attackers gained access to the organization's network/infrastructure/data but no data was exfiltrated)	38.08%
Breach (data was exfiltrated)	58.48%
None of these apply	1.97%

Q17a.

For the past year, please estimate the:

	TOTAL
Base: All Organizations Subject to DoS Incidents Over the Past Twelve Months	**(139)**

1. **Number of denial of service incidents your organization experienced.**

Mean	22.91

2. **Total amount of downtime (in business days) your organization experienced from DoS attacks.**

Mean	19.17

3. **Hard costs (eg. staff time, legal, customer outreach, software, services, etc.) $000's.**

Mean	4,739.21

4. **Soft costs (eg. brand image, competitive standing, employee morale, etc.) $000's.**

Mean	3,509.42

Q17b.

For the past year, please estimate the:

		TOTAL
	Base: All Organizations Subject to Infiltration Incidents Over the Past Twelve Months	**(155)**
1. Number of infiltration incidents your organization experienced.	Mean	25.82
2. Total amount of downtime (in business days) your organization experienced from infiltration incidents.	Mean	15.71
3. Hard costs (eg. staff time, legal, customer outreach, software, services, etc.) $000's.	Mean	4,007.59
4. Soft costs (eg. brand image, competitive standing, employee morale, etc.) $000's.	Mean	2,595.14
5. Number of files/records that were affected.	Mean	116.9
6. Percentage of files impacted that contained sensitive but not personal data.	Mean	27.81

7. **Percentage of files impacted that contained customer or employee information.**

Mean	22.96

Q17br6.

For infiltration incidents, was any of your data subject to an attacker:

	TOTAL
Base: All Organizations Subject to Infiltration Incidents Over the Past Twelve Months	**(155)**
Making ransomware demands	47.74%
Encrypting it	44.52%
Deleting it	31.61%
None of these apply	12.26%

Q17c.

For the past year, please estimate the:

	TOTAL
Base: All Organizations Subject to Breach Incidents Over the Past Twelve Months	**(238)**

1. **Number of breaches your organization experienced.**

Mean	21.32

2. **Total amount of downtime (in business days) your organization experienced from breaches.**

Mean	8.80

3. **Number of files/records that were affected.**

Mean	134.20

4. **Percentage of files exfiltrated that contained sensitive but not personal data.**

Mean	24.64

5. Percentage of files exfiltrated that contained customer or employee information.	
Mean	25.13
6. Hard costs (eg. staff time, legal, customer outreach, software, services, etc.) $000's.	
Mean	2,957.56
7. Soft costs (eg. brand image, competitive standing, employee morale, etc.) $000's.	
Mean	2,104.24

Q18a.

How long would you estimate it takes your organization to detect:

	TOTAL
Base: All Respondents	**(407)**
1. Infiltration (attackers gained access to the organization's network/infrastructure/data but no data was exfiltrated).	
Within hours	46.44%
Within a week	42.75%
Within a month	10.81%
Within a year	
A year or more	
2. Breach (data was exfiltrated).	
Within hours	46.19%
Within a week	43.49%
Within a month	10.32%
Within a year	
A year or more	

Q18b.

After detection how long would you estimate it takes your organization to respond to:

1. Infiltration (attackers gained access to the organization's network/infrastructure/data but no data was exfiltrated).

	TOTAL
Base: All Respondents	**(407)**
Within hours	47.17%
Within a week	49.14%
Within a month	3.69%
Within a year	
A year or more	

2. Breach (data was exfiltrated).

	TOTAL
Within hours	32.68%
Within a week	56.27%
Within a month	11.06%
Within a year	
A year or more	

Q19.

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	**(407)**
Mean	19.38

Q20.

Which of the following best describes the in-house resources your organization devotes to monitoring its security technologies and network for potential harmful activity:

	TOTAL
Base: All Respondents	**(407)**
24x7x365 monitoring by in-house security analysts	11.06%
9-to-5 monitoring by in-house security analysts who are also on call outside of work hours in case of an incident	52.09%
9-to-5 monitoring by in-house security analysts but they are not on call outside of work hours	16.95%
Ad hoc monitoring by in-house security analysts	12.29%
Monitoring by non-IT security specific staff	7.13%
No monitoring	0.25%
Don't know	0.25%

Q21.

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

	TOTAL
Base: All Respondents	**(407)**
Mean	38.6

Q22.

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

	TOTAL
Base: Respondents Answering >0 for Q21	**(380)**
DDoS	32.37%
NGFW/Firewalls	42.11%
SIEM	36.84%
Endpoint Protection, Detection, and Response	46.58%
Web Application Firewall	50.26%
Vulnerability Management	45.53%
Data Loss Prevention (DLP)	52.63%
None of the above	0.26%

Q23.

Which of the following best describes how often your organization uses the following external security services?

a. Security Program Consulting.

	TOTAL
Base: All Respondents	**(407)**
Monthly	8.85%
Quarterly	13.51%
Semi-annually	32.43%
Annually	38.57%
Every 2 years or more	5.16%
Don't use	1.47%

b. Security Threat Risk Assessment.

Monthly	8.60%
Quarterly	44.96%
Semi-annually	29.48%
Annually	11.06%
Every 2 years or more	4.42%
Don't use	1.47%

c. Data Privacy Impact Assessment.

Monthly	28.50%
Quarterly	30.96%
Semi-annually	25.80%
Annually	8.35%
Every 2 years or more	4.18%
Don't use	2.21%

d. Vulnerability Assessment.

Monthly	12.29%
Quarterly	33.66%
Semi-annually	35.87%
Annually	14.74%
Every 2 years or more	2.46%
Don't use	0.98%

e. Penetration Testing.

Monthly	3.19%
Quarterly	7.37%
Semi-annually	18.67%
Annually	23.83%
Every 2 years or more	20.39%
Don't use	26.54%

f. IT Operational Risk Assessment.

Monthly	8.35%
Quarterly	15.97%
Semi-annually	33.66%
Annually	36.36%
Every 2 years or more	4.42%
Don't use	1.23%

g. ITIL Consulting.

Monthly	7.62%
Quarterly	13.27%
Semi-annually	25.31%
Annually	29.48%
Every 2 years or more	21.13%
Don't use	3.19%

h. Virtual CSO.

Monthly	3.44%
Quarterly	10.32%
Semi-annually	19.41%
Annually	15.48%
Every 2 years or more	6.39%
Don't use	44.96%

i. Breach Response and Forensics.

Monthly	9.34%
Quarterly	15.97%
Semi-annually	19.90%
Annually	48.16%
Every 2 years or more	4.42%
Don't use	2.21%

j. Audit and Assurance Services.

Monthly	6.88%
Quarterly	17.20%
Semi-annually	40.79%
Annually	28.75%
Every 2 years or more	4.42%
Don't use	1.97%

k. Security Awareness Training.

Monthly	30.22%
Quarterly	34.15%
Semi-annually	17.20%
Annually	13.51%
Every 2 years or more	2.95%
Don't use	1.97%

Q24.

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

	TOTAL
Base: All Respondents	**(407)**
We do not have a security incident response plan	7.62%
Our security incident response plan is informal	25.55%
We have a documented security incident response plan, but it's not often updated	40.79%
We have a fully documented security incident response plan and it is regularly updated	26.04%

Q25.

What triggers your organization to update your incident response plan?

	TOTAL
Base: All Respondents	**(407)**
Outcomes from table top exercises	21.62%
Periodic reviews (updated every year)	47.17%
Changes to government legislation	32.68%
Changes to industry standards	23.34%
A security incident at my organization	39.56%
Breaches being reported in the news	27.03%
Security researchers reporting new threats or discovery of breaches	25.06%
Mergers or acquisitions	39.31%
Internal changes to the organization	26.29%
Adoption of new technologies	32.68%
We do not have an incident response plan	6.88%

Q26.

Which of the following best describes your organization's plan for recovery back to trusted state after a data breach:

	TOTAL
Base: All Respondents	**(407)**

a. Provides a step-by-step process for the initial response to a data breach.

Fully detailed and documented processes	27.03%
Processes are in place but documentation is not complete	37.59%
Processes are in place but there is no documentation as of yet	23.10%
Ad hoc processes are in place	12.29%

b. Provides a process for recovering to a trusted state and normal operation after a breach.

Fully detailed and documented processes	36.36%
Processes are in place but documentation is not complete	31.70%
Processes are in place but there is no documentation as of yet	16.46%
Ad hoc processes are in place	15.48%

C. What would you say is your organization's expectation for time-to-recovery back to trusted state in a data breach situation that could be described as affecting a mission critical business process, service, application or workload?

Hot - immediate/instant recovery	1.23%
Within minutes, eg. <5 minutes	4.91%
5 - 15 minutes	17.44%
15 - 60 minutes	23.34%
1 - 2 hours	19.66%
3 - 8 hours	13.76%
Within 24 hours	13.51%
24 hours+	6.14%

d. Would you say this time-to-recovery expectation is reasonable given the amount of budget your organization devotes to IT security and recovery?

YES (NET)	81.33%
YES	28.26%
YES - but the expectation should be higher and we should give IT security and recovery more budget	53.07%
NO - the expectation is too high for the budget we have	13.76%
NO - our IT security and recovery budget is fine but the expectation is too high	4.42%
Don't know	0.49%

Q27.

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?

	TOTAL
Base: All Respondents	**(407)**
Mean	3.60

Q28.

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

SUMMARY TABLE OF TOP 2 BOX	TOTAL
Base: All Respondents	**(407)**
Obtaining adequate budget	56.51%
Achieving organization-wide implementation and compliance with your security plan	51.35%
Obtaining cooperation between business and IT on security planning	53.07%
Exposure to insider threats from employee or contractors	53.32%
Finding and recruiting qualified security staff	52.33%
Not having enough operational personnel to meet security objectives	53.32%
Getting the organization to conduct regular cybersecurity risk assessments and audits	53.07%
Not being able to identify the threats that could jeopardize infrastructure and data	53.32%
Not being able to protect against sophisticated Advanced Persistent Threats even if they are identified	51.84%
Business executives and managers taking responsibility for cybersecurity and sponsoring appropriate action to protect the organization	46.44%

Q29.

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

SUMMARY TABLE OF TOP 2 BOX	TOTAL
Base: All Respondents	**(407)**
Insider/Malicious employee threat	67.32%
Ransomware	45.70%
Mobile threats	67.08%
IoT security	46.44%
Data not being backed up	65.85%
Cloud security	41.03%
Public exposure of customer data	67.57%
State Sponsored Attacks	31.70%
Hacktivism	56.51%
Security related downtime of business-critical IT resources	46.19%

Q30.

How confident are you in your organization's overall ability to prevent cybersecurity breaches from happening?

	TOTAL
Base: All Respondents	**(407)**
Highly confident (5)	11.06%
4	42.51%
3	37.10%
2	9.34%
Not at all confident (1)	

Q31.

How confident are you in your organization's overall ability to find and respond to cybersecurity breaches once they have happened?

	TOTAL
Base: All Respondents	**(407)**
Highly confident (5)	14.99%
4	48.16%
3	28.26%
2	8.60%
Not at all confident (1)	

Q32.

How confident are you in your organization's ability to recover to a trusted state following a breach?

	TOTAL
Base: All Respondents	**(407)**
Highly confident (5)	16.71%
4	32.92%
3	30.96%
2	14.25%
Not at all confident (1)	5.16%

ABOUT SCALAR:

Scalar is Canada's leading IT solutions provider, focused on security, infrastructure, and cloud. Founded in 2004, Scalar is headquartered in Toronto, with offices in Montreal, Ottawa, Winnipeg, Calgary, Edmonton, Vancouver, and Victoria. Scalar was recently named one of Canada's Best Managed Companies, named to CRN's 2018 Solution Provider 500 List, and listed on the Growth 500 for the ninth 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 -2018 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 2019