APPENDIX A: Detailed Survey Results

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

	TOTAL
Base: All Respondents (524)	**(524)**
Business/Professional Services (e.g. Legal, Accounting, Engineering,	4,77 %
Architecture, etc.)	5,34 %
4.77%	3,63 %
Personal/Consumer Services (eg. Travel, Beauty, Personal Training,	3,44 %
Dry Cleaning etc.)	6,11 %
5.34%	8,40 %
Construction 3.63%	1,53 %
Hospitality 3.44%	3,05 %
IT Industry 6.11%	13,74 %
Manufacturing 8.40%	13,55 %
Crown Corporation or other publicly funded organization 1.53%	7,25 %
Education College/University 3.05%	3,44 %
Financial Services 13.74%	2,29 %
Government 13.55%	8,40 %
Healthcare 7.25%	1,91 %
Primary (e.g. Agriculture, Mining, Forestry, etc.) 3.44%	3,63 %
Oil & Gas or Field Services related 2.29%	1,53 %
Retail 8.40%	2,86 %
Communications (e.g. Cable and Telecommunications Services, etc.) 1.91%	1,91 %
Media (e.g. Radio/TV Broadcasting) 3.63%	3,24 %
Printing, Publishing, etc. 1.53%	0%
Transportation and Warehousing 2.86%	0%
Utilities 1.91%	
Wholesale and Distribution 3.24%	
Other (please specify) 0%	

S1a. Which level of government best describes your organization?

	TOTAL
Base: All Respondents Who Select Government at S1 (71)	**(71)**
Federal 7.04%	7,04 %
Provincial 28.17%	28,17 %
Municipal/local government 35.21%	35,21 %
Federal government agency or crown corporation 2.82%	2,82 %
Provincial agency 11.27%	11,27 %
Municipal/local agency 15.49%	15,49 %

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

	TOTAL
Base: All Respondents (524)	**(524)**
1-14 0%	0 %
15 - 24 5.15%	5,15 %
25 - 99 4.77%	4,77 %
100 - 249 11.07%	11,07 %
250 - 499 14.31%	14,31 %
500 - 999 15.84%	15,84 %
1,000 - 4,999 19.85%	19,85 %
5,000+ 29.01%	29,01 %
Don't know 0%	0%
Mean 2241.3	2241.66

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

	TOTAL
Base: All Respondents (524)	**(524)**
1% - 9% 0%	0 %
10% - 25% 15.84%	15,84 %
26% - 50% 15.84%	15,84 %
51% - 75% 20.23%	20,23 %
76% - 100% 48.09%	48,09 %
Don't know 0%	0 %
Mean 82.21	82.21

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

	TOTAL
Base: All Respondents (524)	**(524)**
Not headquartered in Canada 2.86%	2,86 %
Western and Central Canada (BC, AB, SK, MB) 20.04%	20,04 %
Ontario 38.55%	38,55 %
Quebec 24.05%	24,05 %
Atlantic Canada (NB, NS, NFLD, PEI) 14.50%	14,50 %
Yukon 0%	0%
Northwest Territories 0%	0%
Nunavut 0%	0%

S5. How many full-time IT staff does your organization have?

	TOTAL
Base: All Respondents (524)	**(524)**
None 0%	0 %
1 - 2 21.56%	21,56 %
3 - 5 24.24%	24,24 %
6 - 15 21.37%	21,37 %
16 - 40 18.89%	18,89 %
41 - 99 9.92%	9,92 %
100 or more 4.01%	4,01 %
Mean 25.47	25.47

S6. Which of the following best describes the department you work for?

	TOTAL
Base: All Respondents (524)	**(524)**
C-level Executive Management excluding IT 8.40%	8,40 %
CIO/CTO/CSO/CISO, etc. 8.02%	8,02 %
IT/IS/MIS/Data Centre/IT Security 74.81%	74,81 %
Legal/Compliance/Risk 8.78%	8,78 %

S6a. Do you directly manage IT security for your organization?

	TOTAL
Base: Respondents Who Answered "C Level Executive Management Excluding IT" for S6	**(44)**
Yes	100.00%
No	0%

S7. At your organization, do you play a role in or are you part of any of the following:

	TOTAL
Base: Respondents Who Answered "No" for S6a (480)	**(480)**
Directing the IT function 32.92%	32,92 %
Improving/managing IT security 100.00%	100,00 %
Setting IT priorities 48.54%	48,54 %
Managing IT budgets 36.67%	36,67 %

S8. Which of the following best describes your job title?

	TOTAL
Base: Respondents Who Did Not Select "C-level Executive Management	**(480)**
excluding IT" for S7a	15,84 %
(480)	6,49 %
IT Executive - e.g. CIO/CTO/VP, CSO/CISO 15.84%	5,15 %
IT Director 6.49%	17,56 %
Infosec Director 5.15%	16,22 %
IT Manager 17.56%	6,11 %
Infosec Manager 16.22%	4,20 %
IT Supervisor 6.11%	5,53 %
Infosec Supervisor 4.20%	3,82 %
IT Staff/Associate/Technician 5.53%	1,53 %
IT Associate/Staff 3.82%	9,16 %
IT Consultant/Contractor 1.53%	0%
Legal/Compliance/Risk Executive, Manager or Staff	9.16%
Don't know	0%

S9. 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 (524)	**(524)**
1 – 2 287	287
3 – 5 107	107
6 – 15 130	130
More than 15 0	0
Mean 3.60	3,60

S10. Which of the following ranges would your organization's annual revenue (or budget for government) fall under?

	TOTAL
Base: All Respondents (524)	**(524)**
Less than $10 million 5.34%	5,34 %
$10 million – $25 million 16.41%	16,41 %
$26 million – $99 million 21.76%	21,76 %
$100 million – $499 million 14.69%	14,69 %
$500 million – $999 million 19.66%	19,66 %
$1 billion or more 22.14%	22,14 %
Mean 429.71	429,71

Q1. Which of the following government or industry regulations does your organization need to be compliant with?

	TOTAL
Base: All Respondents	**(524)**
PCI	42.75%
Digital Privacy Act/PIPEDA	75.76%
GDPR	77.10%
FFIEC, ITAR, OSFI, FedRAMP, FISMA	19.47%
SOX, C-SOX	67.94%
HIPAA, PHIPA	12.02%
NERC/FERC	15.27%
Other	0%

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

SUMMARY: Mean	TOTAL
Base: All Respondents	**(524)**
PCs/laptops	1919.41
Smartphones/tablets	1014.03
Servers (virtual or physical)	47.06
TBs of storage capacity attached to/within servers (not in PC, smartphone or other devices)	1616.00
IoT devices	173.76

Q3. Does your organization have any initiatives in any of the following areas?

	TOTAL
Base: All Respondents	**(524)**

1. Digitization/automation of customer facing processes (e.g. customer experience)

Net: Yes	90.27%
Yes – involving both customer and organizational data	42.94%
Yes – involving customer data only	25.76%
Yes – involving organizational data only	21.56%
No	7.63%
Don't know/Not applicable	1.34%

2. Data generation/tracking (e.g. smart production lines, smart buildings, smart products)

Net: Yes	92.18%
Yes – involving both customer and organizational data	29.01%
Yes – involving customer data only	28.82%
Yes – involving organizational data only	34.35%
No	6.11%
Don't know/Not applicable	0.95%

3. Digitization/automation of business partner/supplier facing processes (e.g. automated supply chain, automated procurement)

Net: Yes	91.98%
Yes – involving both customer and organizational data	41.98%
Yes – involving customer data only	26.53%
Yes – involving organizational data only	23.47%
No	7.06%
Don't know/Not applicable	0.19%

4. AI/machine learning (focused on IT security orchestration, service management and automation)

Net: Yes	47.90%
Yes – involving both customer and organizational data	23.47%
Yes – involving customer data only	11.26%
Yes – involving organizational data only	13.17%
No	50.76%
Don't know/Not applicable	0.57%

5. AI/machine learning (focused on cybersecurity analysis)

Net: Yes	59.92%
Yes – involving both customer and organizational data	28.24%
Yes – involving customer data only	17.75%
Yes – involving organizational data only	13.93%
No	38.36%
Don't know/Not applicable	0.95%

6. AI/machine learning (focused on customer data and analysis)

Net: Yes	57.63%
Yes – involving both customer and organizational data	29.20%
Yes – involving customer data only	17.56%
Yes – involving organizational data only	10.88%
No	41.03%
Don't know/Not applicable	0.57%

7. IoT data and analytics

Net: Yes	73.47%
Yes – involving both customer and organizational data	41.41%
Yes – involving customer data only	23.28%
Yes – involving organizational data only	8.78%
No	11.83%
Don't know/Not applicable	13.93%

8. 5G/mobile solutions or applications

Net: Yes	17.75%
Yes – involving both customer and organizational data	10.31%
Yes – involving customer data only	4.77%
Yes – involving organizational data only	2.67%
No	47.52%
Don't know/Not applicable	33.97%

9. None of the above

Sum	0.76%

Q3a. What infrastructure and compute resources are being used by your organization to support these initiatives?

1.

	TOTAL
Base: Respondents Who Have a Digitization/Automation of Customer Facing Processes (e.g. Customer Experience) Initiative	**(473)**
On-premise and cloud provider infrastructure and compute resources	47.57%
On-premise infrastructure and compute resources only	34.04%
Cloud provider infrastructure and compute resources only	17.55%
Don't know	0.85%

2.

	TOTAL
Base: All Respondents Who Have a Data Generation/Tracking (e.g. Smart Production Lines, Smart Buildings, Smart Products) Initiative	**(483)**
On-premise and cloud provider infrastructure and compute resources	41.61%
On-premise infrastructure and compute resources only	34.16%
Cloud provider infrastructure and compute resources only	24.02%
Don't know	0.21%

3.

	TOTAL
Base: Respondents Who Have a Digitization/Automation of Business Partner/Supplier Facing Processes (e.g. Automated Supply Chain, Automated Procurement) Initiative	**(482)**
On-premise and cloud provider infrastructure and compute resources	45.23%
On-premise infrastructure and compute resources only	36.72%
Cloud provider infrastructure and compute resources only	17.63%
Don't know	0.41%

4.

	TOTAL
Base: Respondents Who Have an AI/Machine Learning (Focused on Cybersecurity Analysis) Initiative	**(314)**
On-premise and cloud provider infrastructure and compute resources	52.23%
On-premise infrastructure and compute resources only	28.98%
Cloud provider infrastructure and compute resources only	18.47%
Don't know	0.32%

5.

	TOTAL
Base: Respondents Who Have an AI/Machine Learning (Focused on Customer Data and Analysis) Initiative	**(302)**
On-premise and cloud provider infrastructure and compute resources	43.38%
On-premise infrastructure and compute resources only	37.75%
Cloud provider infrastructure and compute resources only	18.87%
Don't know	0%

6.

	TOTAL
Base: Respondents Who Have an IoT Data and Analytics Initiative	**(385)**
On-premise and cloud provider infrastructure and compute resources	50.91%
On-premise infrastructure and compute resources only	32.99%
Cloud provider infrastructure and compute resources only	15.32%
Don't know	0.78%

7.

	TOTAL
Base: Respondents Who Have a 5G/Mobile Solutions or Applications Initiative	**(93)**
On-premise and cloud provider infrastructure and compute resources	22.58%
On-premise infrastructure and compute resources only	43.01%
Cloud provider infrastructure and compute resources only	25.81%
Don't know	8.60%

Q3b. Has your organization deployed an EDR solution?

	TOTAL
Base: All Respondents	**(524)**
Yes – for corporately managed laptops/PCs, tablets, mobile devices	61.83%
Yes – for both corporately managed and non-managed/BYOD laptops/PCs, tablets, mobile devices	27.48%
No	9.16%
Don't know	1.53%

Q3c. Does your EDR solution extend to IoT?

	TOTAL
Base: Respondents Who Answered Yes for Q3b	**(468)**
Not applicable/we don't have any IoT deployments	21.15%
Yes	59.83%
No	16.88%
Don't know	2.14%

Q3d. Has your organization implemented any cybersecurity related AI/machine learning tools or functionality?

	TOTAL
Base: All Respondents	**(524)**
Yes – for security orchestration, administration and response purposes (SOAR)	16.98%
Yes – for cybersecurity analysis purposes	36.45%
Yes – for both SOAR and cybersecurity analysis	10.31%
No	30.92%
Don't know	5.34%

Q3e. On the following 1 – 5 scale, how much additional effectiveness would you say the AI/machine learning tools/functionality have provided?

	TOTAL
Respondents Who Answered Yes for Q3d	**(334)**
5 = Significant additional effectiveness	29.94%
4	44.61%
3	21.56%
2	2.99%
1 = Relatively little additional effectiveness	0.90%

Q3f. How easy has it been to utilize AI/machine learning for cybersecurity purposes?

	TOTAL
Respondents Who Answered Yes for Q3d	**(334)**
Tricky to consume correctly	55.39%
Easy	34.13%
Basic consumption is easy but making it effective is tricky	10.48%

Q4. Which CIA (confidentiality, integrity, availability) category is most critical for your organization's:

	TOTAL
Base: All respondents	**(524)**

1. Top Secret/Highly Confidential Data

Availability	1.34%
Integrity	14.69%
Confidentiality	83.97%

2. Proprietary/Internal Use Data

Availability	15.08%
Integrity	58.21%
Confidentiality	26.72%

3. Public Data

Availability	51.72%
Integrity	31.68%
Confidentiality	16.60%

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

	TOTAL
Base: All respondents	**(524)**
Mean	$10.45 million

Q6. What percentage of your organization's total annual IT budget is devoted to IT security specifically (including tools, solutions, staff, training, IT security services, consulting, etc.)?

	TOTAL
Base: All respondents	**(524)**
Mean	11.01%

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

	TOTAL
Base: All respondents	**(524)**
Staff portion of IT security budget	34.84%
All other costs	65.16%

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

	TOTAL
Base: All respondents	**(524)**

1. Taking inventory of applications, devices and systems

Not conducted	2.86%
Conducted across select areas/departments of the organization	51.15%
Conducted across the entire organization	45.99%

2. Discovering/assessing security weaknesses/vulnerabilities across applications, devices and systems

Not conducted	3.24%
Conducted across select areas/departments of the organization	47.52%
Conducted across the entire organization	49.24%

3. Assessing the business impact of data loss/corruption, disruption of work

Not conducted	16.22%
Conducted across select areas/departments of the organization	48.47%
Conducted across the entire organization	35.31%

4. Prioritizing deployment of specific security solutions

Not conducted	10.50%
Conducted across select areas/departments of the organization	48.66%
Conducted across the entire organization	40.84%

5. Assessing and tracking security risks as part of an organizational risk management program

Not conducted	4.20%
Conducted across select areas/departments of the organization	47.71%
Conducted across the entire organization	48.09%

Q8a. Are your cybersecurity and enterprise risk management strategies and programs fully integrated?

	TOTAL
Base: All respondents	**(524)**
Yes	17.56%
Partially	62.60%
No	19.85%

Q8b. Are your cybersecurity and enterprise risk management strategies centralized or do subsidiaries, operating units or LOBs implement their own cybersecurity and risk management?

	TOTAL
Base: All respondents	**(524)**
Centralized	12.40%
Some centralization, some subsidiary, operating unit or LOB implementation	61.83%
Primarily subsidiary, operating unit or LOB implementation	25.76%

Q8c. How does your organization quantify the return of cybersecurity investments?

	TOTAL
Base: All respondents	**(524)**
Cyber security investment is justified because it is a cost of doing business	24.81%
We do not currently calculate ROI for cyber security investments	7.82%
We calculate ROI for our cyber security investments based on reduction of risk metrics	63.36%
We calculate ROI for our cyber security investments based on reduction of risk AND business ROI	3.82%
Don't know	0.19%

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	**(524)**
Yes – in a comprehensive manner	36.64%
Yes – but we should look at this in more detail	56.68%
No	6.68%
Not sure/don't know	0%

Q9a. Approximately how many third-party partners does your organization work with today?

	TOTAL
Base: All respondents	**(524)**
Mean	47.57

Q9b. Do any of your organization's third-party partners handle:

	TOTAL
Base: All respondents	**(524)**
A core business process(es) for your organization	29.01%
Proprietary business information	49.43%
Customer data	37.21%
Administration/maintenance/management of a business function	17.75%
None of the above	1.34%

Q9c. Has your organization ever experienced a security breach due to the poor security hygiene of a third-party partner?

	TOTAL
Base: All respondents	**(524)**
Yes	81.68%
No	16.98%
Don't know	1.34%

Q10. Please select the five security controls, tactics or tools you feel have been the most effective at protecting your organization from cybersecurity threats:

Most effective over the past year

	TOTAL
Base: All respondents	**(524)**

1. Most effective over the past year

Identity and Access Management	56.11%
Email Security	54.77%
Web Content Filtering	54.01%
Endpoint Protection	49.81%
Security Awareness Training	48.09%
Vulnerability Management	46.37%
Data Security (Encryption/DLP)	27.29%
Next Generation Firewalls/IPS	25.57%
Security Monitoring (SIEM, Log Management)	24.24%
DNS Security	21.18%
User Behaviour Analytics	16.60%
Threat Hunting	14.31%
Breach Response and Forensics Tools	13.17%
Endpoint Detection and Response (EDR)	12.79%
AI/ML Security Analysis Tools	11.83%
Risk and Compliance Automation	10.50%
Security Orchestration, Automation and Response (SOAR)	7.25%
AI/ML Security Automation Tools	6.11%

2. Most interested in looking at to add effectiveness over the next three years

Security Monitoring (SIEM, Log Management)	52.10%
Next Generation Firewalls/IPS	50.76%
Data Security (Encryption/DLP)	48.28%
Threat Hunting	43.32%
User Behaviour Analytics	40.65%
Breach Response and Forensics Tools	33.78%
Endpoint Detection and Response (EDR)	33.02%
Endpoint Protection	24.81%
Security Awareness Training	24.81%
Vulnerability Management	23.28%
AI/ML Security Automation Tools	21.95%
DNS Security	19.85%
Web Content Filtering	16.41%
Identity and Access Management	15.46%
Email Security	14.12%
Risk and Compliance Automation	13.74%
Security Orchestration, Automation and Response (SOAR)	12.79%
AI/ML Security Analysis Tools	10.88%

Q11. How does your organization train employees on the following?

To frequently update PC and smartphone OS and apps

	TOTAL
Base: All respondents	**(524)**

1. To frequently update PC and smartphone OS and apps

No training	7.44%
Ad hoc training and reminders	40.84%
Formal training with reminders as required by new threats, etc.	51.72%

2. How to use end-user security tools

No training	5.53%
Ad hoc training and reminders	44.85%
Formal training with reminders as required by new threats, etc.	49.62%

3. How to securely use technology

No training	10.88%
Ad hoc training and reminders	39.69%
Formal training with reminders as required by new threats, etc.	49.43%

4. How to identify attacks such as phishing and other scams

No training	7.63%
Ad hoc training and reminders	42.37%
Formal training with reminders as required by new threats, etc.	50.00%

5. Proper care of sensitive data such as customer/other employee private data

No training	3.63%
Ad hoc training and reminders	44.08%
Formal training with reminders as required by new threats, etc.	52.29%

6. Cloud security responsibilities

No training	10.88%
Ad hoc training and reminders	44.08%
Formal training with reminders as required by new threats, etc.	45.04%

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

	TOTAL
Base: All respondents	**(524)**

1. On-premise databases, apps, servers (and the operating systems + applications running on your on-premise infrastructure)

Immediately when released	23.66%
Within a week	51.34%
Within a month	23.28%
Within a quarter	1.72%
Within a year	0%
A year or more	0%

2. Web applications

Immediately when released	28.82%
Within a week	49.05%
Within a month	21.95%
Within a quarter	0.19%
Within a year	0%
A year or more	0%

3. Network equipment

Immediately when released	8.97%
Within a week	52.48%
Within a month	32.25%
Within a quarter	5.92%
Within a year	0.38%
A year or more	0%

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

Immediately when released	5.92%
Within a week	49.43%
Within a month	39.31%
Within a quarter	4.58%
Within a year	0.76%
A year or more	0%

Q13. Does your organization understand the potential security risks and vulnerabilities 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	**(6)**
No	0%
Not fully, we need more education	16.67%
Yes – and there's really no good reason why we don't update/patch sooner	83.33%
Yes– but for various IT or business-related reasons we can't update/patch any sooner	0%
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	0%

Q14. Please estimate how many times your organization has been subject to an IT security related attack or threat over the past 12 months:

	TOTAL
Base: All respondents	**(524)**
0	0
1–50	4.96%
51–100	3.82%
101–200	19.85%
201–500	31.30%
501–700	15.65%
701–1000	16.79%
1001–1500	5.34%
1501–2000	1.72%
2001–3000	0.57%
3001–4000	0%
4001–5000	0%
5000+	0%
Mean	513.94

Q15. Is your organization entirely on-premise or entirely cloud-based?

	TOTAL
Base: All respondents	**(524)**
We are a hybrid of on-premise and cloud data centre	68.89%
Entirely on-premise	21.56%
Entirely cloud-based (e.g. AWS, Azure, GCP, etc.)	9.54%

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	**(524)**
Denial of service (network went down)	36.45%
Infiltration (attackers gained access to the organization's network/infrastructure/data but no data was exfiltrated)	40.46%
Breach (data was exfiltrated)	59.54%
None of these apply	0.76%

Q17a. For the past year, please estimate the:

	TOTAL
Base: All Organizations Subject to DoS Incidents Over the Past 12 Months	**(191)**
1. Number of denial of service incidents your organization experienced	
Mean	28.48
2. Total amount of downtime (in business days) your organization experienced from DoS attacks	
Mean	23.98
3. Hard costs (staff time, legal, customer outreach, software, services, etc.)	
Mean	$4.86 million
4. Soft costs (brand image, competitive standing, employee morale, etc.)	
Mean	$3.51 million

Q17b. Infiltration Branch: For the past year, please estimate the:

	TOTAL
Base: All Organizations Subject to DoS Incidents Over the Past 12 Months	**(212)**
1. Number of infiltration incidents your organization experienced	
Mean	26.19
2. Total amount of downtime (in business days) your organization experienced from infiltration incidents	
Mean	18.32
3. Hard costs (staff time, legal, customer outreach, software, services, etc.)	
Mean	3.93 million
4. Soft costs (brand image, competitive standing, employee morale, etc.)	
Mean	2.72 million
5. How many hosts were impacted	
Mean	69.95

Q17br6. Was any of your data subject to an attacker:

	TOTAL
Base: All Organizations Subject to Infiltration incidents Over the Past 12 Months	**(212)**
Making ransomware demands	50.47%
Encrypting it	33.49%
Deleting it	29.25%
None of these	2.83%

Q17br7. How was data impacted by the infiltration? Was there:

	TOTAL
Base: All Organizations Subject to Infiltration incidents Over the Past 12 Months	**(212)**
Disclosure of confidential data to unauthorized parties	22.64%
Modification/corruption of data	54.25%
Lack of access to data (i.e. ransomware)	33.96%
Don't know	0.94%

Q17br8. Has your organization ever been subject to the same ransomware repeating after recovery?

	TOTAL
Base: All Organizations Subject to Infiltration incidents Over the Past 12 Months	**(212)**
Yes	80.19%
No	19.81%

Q17c. For the past year, please estimate the:

	TOTAL
Base: All Organizations Subject to Breach Incidents Over the Past 12 Months	**(312)**
1. Number of breaches your organization experienced	
Mean	23.46
2. Total amount of downtime (in business days) your organization experienced from breaches	
Mean	17.09
3. Number of files/records that were affected	
Mean	150.38
4. Percentage of files exfiltrated that contained sensitive but not personal data	
Mean	26.75
5. Percentage of files exfiltrated that contained customer or employee information	
Mean	27.65
6. Hard costs (staff time, legal, customer outreach, software, services, etc.)	
Mean	3.06 million
7. Soft costs (brand image, competitive standing, employee morale, etc.)	
Mean	2.62 million

Q18a. How long would you estimate it takes your organization to detect via tools, tactics or controls and for IT security staff to become aware of: **Infiltration (attackers gained access to the organization's network/infrastructure/data but no data was exfiltrated)**

	TOTAL
Base: All Respondents	**(524)**
1 hour or less	6.49%
Within hours	50.95%
Within a week	34.54%
Within a month	7.82%
Within a year	0.19%
A year or more	0%

Q18b. How long would you estimate it takes your organization to detect via tools, tactics or controls and for IT security staff to become aware of: **Breach (data was exfiltrated)**

	TOTAL
Base: All Respondents	**(524)**
1 hour or less	3.82%
Within hours	45.99%
Within a week	37.02%
Within a month	12.40%
Within a year	0.76%
A year or more	0%

Q18c. After detection how long would you estimate it takes your organization to remediate against: **Infiltration (attackers gained access to the organization's network/infrastructure/data but no data was exfiltrated)**

	TOTAL
Base: All Respondents	**(524)**
Within hours	46.18%
Within a week	48.47%
Within a month	4.96%
Within a year	0.38%
A year or more	0%

Q18d. After detection how long would you estimate it takes your organization to remediate against: **Breach (data was exfiltrated)**

	TOTAL
Base: All Respondents	**(524)**
Within hours	34.92%
Within a week	51.91%
Within a month	12.02%
Within a year	1.15%
A year or more	0%

Q19. How many cumulative workdays 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	**(524)**
Mean	34.21

Q20. How does your organization internally monitor and investigate security alerts?

	TOTAL
Base: All Respondents	**(524)**
24x7x365 monitoring by in-house security analysts	16.41%
9-to-5 monitoring by in-house security analysts	58.02%
Ad hoc monitoring	16.41%
No monitoring	8.59%
Don't know	0.57%

Q21. What percentage of your total security budget is spent on external third party managed security services (e.g. monitoring, management, intelligence and response services, etc.)?

	TOTAL
Base: All Respondents	**(524)**
Mean	39.55%

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

	TOTAL
Base: Respondents answering >0 for Q21	**(524)**
SOC-as-a-Service	31.49%
NGFW/Firewalls	45.04%
SIEM	33.59%
Endpoint Protection, Detection and Response	54.96%
Breach Response	20.04%
Vulnerability Management	46.76%
Data Loss Prevention (DLP)	66.03%
Web Application Firewall	54.01%
DDoS	33.02%
IDaaS (Identity-as-a-Service)	48.85%
None of the above	0.38%

Q23. Which of the following best describes how often your organization uses the following external security services?

	TOTAL
Base: All Respondents	**(524)**
1. Security Threat Risk Assessment	
Monthly	8.78%
Quarterly	46.56%
Semi-annually	30.92%
Annually	11.26%
Every 2 years or more	2.29%
Don't use	0.19%
2. Vulnerability Assessment	
Monthly	13.55%
Quarterly	34.73%
Semi-annually	36.26%
Annually	12.98%
Every 2 years or more	2.10%
Don't use	0.38%
3. Penetration Testing	
Monthly	2.10%
Quarterly	9.73%
Semi-annually	17.37%
Annually	35.31%
Every 2 years or more	20.80%
Don't use	14.69%
4. Audit and Assurance Services	
Monthly	4.01%
Quarterly	15.46%
Semi-annually	41.79%
Annually	32.82%
Every 2 years or more	5.73%
Don't use	0.19%
5. Security Awareness Training	
Monthly	29.58%
Quarterly	39.31%
Semi-annually	16.41%
Annually	12.21%
Every 2 years or more	2.48%
Don't use	0%

Q24. Do you have an incident response or breach retainer with a security service provider?

	TOTAL
Base: All Respondents	**(524)**
Yes and we have used it	6.87%
Yes but we have never used the retainer	45.80%
Not currently but we have had and used a retainer in the past	27.29%
Not currently and we have never used one	14.50%
Don't know	5.53%

Q24a. On the following 1 – 5 scale, how effective has your incident response or breach retainer been in helping your organization with response and recovery?

	TOTAL
Base: Organizations indicating they have used an incident response or breach retainer at Q24	**(179)**
5 = Extremely effective (5)	18.44%
4	45.25%
3	31.84%
2	4.47%
1 = Not effective	0%

Q24b. What were the main reasons your incident response or breach retainer was not effective?

	TOTAL
Base: Respondents answering "1" or "2" for Q24a	**(8)**
Retainer did not include enough hours to be helpful when responding and/or recovering	37.50%
Provider lacked knowledge to properly help respond and recover	37.50%
Provider lacked tools to properly help respond and recover	37.50%
Provider lacked staff to properly help respond and recover	50.00%
Provider's lack of geographic coverage/local office resulted in inadequate response	37.50%

Q25. Which of the following best describes your organization's security incident response plan?

	TOTAL
Base: All Respondents	**(524)**
We do not have a security incident response plan	6.30%
Our security incident response plan is informal	26.53%
We have a documented security incident response plan, but it's not often updated	50.38%
We have a fully documented security incident response plan and it is regularly updated	16.79%

Q26a. Which of the following best describes your organization's plan for recovery back to trusted state after a data breach:

	TOTAL
Base: All Respondents	**(524)**
We have a fully documented recovery plan and it is regularly updated	20.23%
We have a documented recovery plan, but it's not often updated	44.08%
Our recovery plan is informal	34.54%
We do not have a recovery plan	1.15%

Q26b. Given the processes, tools and resources you have today, what would you estimate your actual time-to-recovery back to a trusted state would be in a data breach situation that could be described as affecting a mission critical business process, service, application or workload?

	TOTAL
Base: All Respondents	**(524)**
Hot – immediate/instant recovery	0.19%
Within minutes, e.g. <5 minutes	1.53%
5–14 minutes	11.83%
15–59 minutes	21.76%
1–2 hours	23.85%
3–8 hours	21.76%
Within 24 hours	11.26%
Within 3 days	5.92%
Within a week	1.91%
Within a month	0%
More than a month	0%

Q26c. Is what you can deliver for time-to-recovery back to trusted state for a data breach affecting a mission critical business process, service, application or workload aligned with your organization's expectations on the business side?

	TOTAL
Base: All Respondents	**(524)**
YES	73.28%
NO	26.72%

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 Answering	**(524)**
5 = Highly involved leadership	28.82%
4	45.04%
3	23.85%
2	2.10%
1 = Uninvolved leadership	0.19%

Q28. Please rank the following from 1–5 in order of how much of a concern they are for you (Where 1 equals the biggest concern)

	TOTAL
Base: All Respondents	
Business executives and managers taking responsibility for cybersecurity and sponsoring appropriate action to protect the organization	#1
Obtaining cooperation between business and IT on security planning	#2
Exposure to insider threats from employee or contractors	#3
Obtaining adequate budget for IT security/cybersecurity	#4
Finding and recruiting qualified security staff	#5
More than a month	

Q29. From the following please identify the top three attack types you believe your organization should be concerned with. Ranking from 1–3 of top three attack types. Attack types outside top three listed in declining order of response.

	TOTAL
Base: All Respondents	
Insider/malicious employee threat	#1
Ransomware	#2
Denial of Service (DoS)	#3
Phishing and spear phishing	
SQL injection	
Drive-by-downloads	
Zero-day	
Cross-Site scripting	
Social engineering	
Mining cryptocurrencies	
Man-in-the-middle/hijacking	
Advanced persistent threat	
Password/brute force	
Macro viruses	

Q30. How confident are you in your organization's overall ability to prevent cybersecurity breaches from happening?

	TOTAL
Base: All Respondents	**(524)**
5 = Highly confident	15.27%
4	40.46%
3	38.17%
2	4.77%
1 = Not at all confident	1.34%

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	**(524)**
5 = Highly confident	32.63%
4	33.21%
3	30.73%
2	2.86%
1 = Not at all confident	0.57%

Q32. How confident are you in your organization's ability to recover to a trusted state following a breach?

	TOTAL
Base: All Respondents	**(524)**
5 = Highly confident	17.94%
4	29.01%
3	39.69%
2	12.21%
1 = Not at all confident	1.15%

CDW PEOPLE WHO GET IT™

IDC

Research independently conducted by IDC Canada | Published February 2020