



THE
**STRATEGIC
COUNSEL**

EXPERIENCE • PASSION • CREATIVITY

TORONTO | OTTAWA | CALGARY
www.thestrategiccounsel.com



A REPORT TO
CIRA

PERCEPTIONS AND ATTITUDES OF CANADIAN ORGANIZATIONS TOWARD CYBERSECURITY

August 2022

CONTENTS

1	Objectives and Methodology	3
2	Resources and Training	5
3	Cybersecurity: Experience and Response	18
4	Remote/Hybrid Work	48
5	Sample Characteristics	56

1

OBJECTIVES AND METHODOLOGY

BACKGROUND AND PURPOSE:

- With a mandate to help build a better online Canada, CIRA is both an innovator and global thought leader at the heart of Canada's internet, and a prominent voice on issues of national and international importance, including cybersecurity.
- In addition to being a leading voice, CIRA provides Canadian organizations with made-in-Canada security products, including its DNS Firewall.
- To continue to build its thought leadership position in Canada and support for its product offerings, CIRA required research among small to medium-sized businesses and public sector organizations (esp. MUSH organizations) to examine their perceptions and attitudes toward cybersecurity.
- Findings from the research will be used to inform CIRA press releases, white papers and other communications, and to build awareness of CIRA through media and other sources.

METHODOLOGY



A total of n=500 cybersecurity decision-makers (employees or owners) completed a 10-12 minute online survey in August, 2022. All organizations have at least 50 employees that use a computer or mobile device at least 20% of the time as part of their employment. Private sector organizations have no more than 999 employees.

Throughout, the findings are reported for the total sample as well as by sector, where appropriate and meaningful:

- Private sector (i.e., for-profit business)
- Public sector (all)
- MUSH (public sector, including only municipal government or agency, hospital or other health care organization, primary or secondary school, college or university, or school board)

Where possible, the 2022 findings are compared to the results from previous years.

2

RESOURCES AND TRAINING

INCIDENCE OF CONDUCTING CYBERSECURITY AWARENESS TRAINING










Most organizations (96%) conduct cybersecurity awareness training that is mandatory for at least some employees.

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended			
	2022	2022	2022	2022	2019	2020	2021	2022
	500	320	122	54	502	500	510	500
	%	%	%	%	%	%	%	%
TOTAL YES	96	96	98	96	87	94	93	96
Yes, mandatory training for some employees	44	45	45	44	32	34	41	44
Yes, mandatory training for all employees	44	45	41	39	41	48	43	44
Yes, optional training (some or all employees)	8	7	11	13	15	12	9	8
No	4	4	2	4	11	6	7	4
Don't know	<1	<1	-	-	1	<1	<1	<1

Q6. Cybersecurity awareness training focuses on topics like building strong passwords, identifying phishing attacks, acceptable social media use, etc. Does your organization conduct cybersecurity awareness training for its employees?
 Base: Total sample

WAYS OF CONDUCTING CYBERSECURITY AWARENESS TRAINING

Most commonly, organizations use training materials (in-house and third-party developed are both common) and phishing simulations.

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended			
	2022	2022	2022	2022	2019	2020	2021	2022
	480	307	119	52	439	467	474	480
	%	%	%	%	%	%	%	%
In-house developed courses/training materials/(previous) <i>We create training material and promote it internally</i>	 48	49	45	46	54	57	61	48
Refresher training	 46	45	45	46	-	-	-	46
Third-party developed courses/training materials	 44	44	37	44	-	-	-	44
Phishing simulations/(previous) <i>We conduct phishing simulations*</i>	 42	44	35	44	21	37	44	42
In-house developed lunch-and-learns/workshops/seminars/(previous) <i>Lunch-and-learns/workshops</i>	 39	36	42	35	36	35	39	39
Extra/supplementary training for high-risk groups	 37	38	27	33	-	-	-	37
Third-party developed lunch-and-learns/workshops/seminars /(previous) <i>We hire a third-party to conduct seminar-style training programs</i>	 31	30	24	15	32	31	35	31
Micro-learning modules	 29	28	29	25	-	-	-	29
Games	 10	9	10	10	-	-	-	10
Other	<1%	-	2	2	2	1	2	<1
Don't know	<1%	<1	1	2	1	<1	<1	<1





Q7. In what ways does your organization conduct cybersecurity awareness training? Select all that apply.

Base: Conduct cyber security training at Q6

• Previous phrasing: "We conduct standalone phishing simulations"

FREQUENCY OF CONDUCTING CYBERSECURITY AWARENESS TRAINING

Most organizations conduct cybersecurity awareness training quarterly or less. The proportion that conducts training at least quarterly is higher in 2022 (67%) than in previous years.

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended			
	2022	2022	2022	2022	2019	2020	2021	2022
	480	307	119	52	439	467	474	480
	%	%	%	%	%	%	%	%
Annually or less	 32	30	41	33	40	40	41	32
Quarterly	 55	57	46	54	36	49	46	55
Monthly	 12	12	11	10	12	9	11	12
More than monthly/ongoing	-	-	-	-	10	-	-	-
Don't know	 1	1	2	4	2	1	2	1







Q8. About how often does your organization conduct cybersecurity awareness training?

Base: Conduct cyber security training at Q6

C Caution, small base size

WAYS OF MEASURING THE IMPACT OF CYBERSECURITY AWARENESS TRAINING

The most common way of measuring the impact of training remains monitoring results and risk scores over time. However, other ways are also common, especially end-user assessments and reduced costs on security incidents.

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended			
	2022	2022	2022	2022	2019	2020	2021	2022
	480	307	119	52	439	467	474	480
	%	%	%	%	%	%	%	%
Monitoring training results and risk scores over time	 56	56	51	54	46	46	53	56
Conducting end-user perception/knowledge assessments	 49	50	45	48	42	38	48	49
Reduced costs on security incidents	 48	49	40	50	25	42	44	48
Saved time on security incidents	 43	43	41	46	27	42	42	43
Comparing training results to industry peers	 34	36	28	27	33	25	37	34
Other	-	-	-	-	1	1	1	-
None/no ability to measure the impact/don't know	 6	5	9	4	11	9	7	6







Q9. How, if at all, does your organization measure the impact of its cybersecurity awareness training program? Select all that apply.

Base: Have cyber security training at Q6

C Caution, small base size

PERCEIVED EFFECTIVENESS OF END-USER TRAINING

Most continue to indicate that end-user training is effective in reducing incidents and/or risky online behavior.

	TOTAL	TOTAL – Trended			
	2022	2019	2020	2021	2022
	480	439	467	474	480
	%	%	%	%	%
TOTAL EFFECTIVE	 93	92	93	95	93
Very effective	 38	35	32	32	38
Somewhat effective	 55	57	61	63	55
Not very effective	 6	6	6	4	6
Not effective at all	-	<1	<1	<1	-
TOTAL NOT EFFECTIVE	 6	6	6	4	6
Don't know	 1	2	1	1	1

Q10. In your opinion, how effective has end-user training been in reducing total accidental malware or phishing incidents or in reducing employees' risky online behavior?

Base: Have cyber security training at Q6

REASONS FOR NOT CONDUCTING CYBERSECURITY AWARENESS TRAINING

The very small proportion of organizations that don't conduct training tend to cite insufficient resources as the main reason (58%). Time required (37%) and lack of buy-in (26%) are also mentioned by at least one-quarter of respondents.

	TOTAL	TOTAL – Trended			
	2022	2019	2020	2021	2022
	19c	57	32c	34c	19c
	%	%	%	%	%
Insufficient IT human resources	58	44	31	44	58
Too time consuming	37	14	16	21	37
No executive buy-in	26	12	28	21	26
Have never considered it as a solution*	21	26	13	35	21
Too expensive	16	21	22	21	16
Unsure of best approach/options	16	32	19	21	16
Previous training attempts were unsuccessful	5	5	-	6	5
Prefer to spend budget on other cybersecurity tools	5	-	-	-	5
Don't believe training works*	-	4	3	6	-
Other	11	4	9	12	11
Don't know	5	5	16	9	5

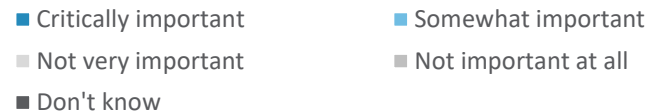
Q11. What are the main reasons that your organization does not conduct cybersecurity awareness training? Select all that apply.

- Base: Do not have cyber security training at Q6
- Previous phrasing: "Have never considered it"
 - Previous phrasing: "Training doesn't work"
- C Caution, small base size

IMPORTANCE OF FEATURES WHEN CONSIDERING A COMPUTER-BASED TRAINING PLATFORM

Modern, high-quality training courses and risk advisory/recommendations are most likely to be rated as ‘critically important’ features when considering a training platform. At least 4-in-10 also rate end-to-end reporting and phishing simulations as critically important.

	TOTAL				% IMPORTANT			
	2022				2019	2020	2021	2022
	500				502	500	510	500
	%				%	%	%	%
Modern, high-quality training courses	45	45	7	2	87	86	88	90
Risk advisory and recommendations	46	43	8	2	91	87	89	89
End-to-end reporting	42	44	11	2	84	82	80	86
Pre-built training curriculum	35	48	14	1	84	81	82	84
Automated phishing simulations	40	42	12	3	83	84	84	83
End-user-facing risk scores and dashboards	37	45	11	3	84	81	80	82
Industry benchmarking	30	51	13	3	-	-	-	82
Off-the-shelf deployment	26	53	15	2	74	76	79	80












Q12. How important is each of the following features when considering software for delivering computer-based cybersecurity training and/or phishing simulations? Please respond even if you have never considered it. (Previous phrasing) How important is each of the following features when considering a computer-based security training platform? Please respond even if you have never considered it.

Base: Total sample

AWARENESS OF TRAINING PROVIDERS

Awareness of training providers is relatively limited; however, 29% are aware of CIRA, which is on par or close to awareness of Proofpoint, Terranova Security and Webroot.

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended			
	2022	2022	2022	2022	2019	2020	2021	2022
	500	320	122	54	502	500	510	500
	%	%	%	%	%	%	%	%
Proofpoint	 32	34	21	22	23	25	26	32
Terranova Security	 30	32	23	15	25	21	25	30
CIRA	 29	30	24	30	25	27	25	29
Webroot	 28	28	28	31	-	27	26	28
KnowBe4	 22	23	24	22	19	21	21	22
Beauceron Security	 18	22	11	11	10	8	9	18
Cofense	 16	18	11	15	14	14	14	16
Other	 2	2	1	-	-	-	-	2
None of the above	 18	15	21	19	35	27	27	18




Q13. Which of the following computer-based security awareness training providers are you familiar with? Please select all that apply.

Base: Total sample

IMPORTANCE OF DATA SOVEREIGNTY VS PRICE

Most consider data sovereignty as more important than price when selecting a cybersecurity service vendor.

- There is no difference in responses based on where organizations operate (i.e., Canada only or internationally).










	TOTAL	PRIVATE	PUBLIC	MUSH
	2022	2022	2022	2022
	500	320	122	54
	%	%	%	%
Data sovereignty	 63	62	66	65
Price	 27	29	23	26
Don't know	 9	9	11	9

Q2022-51H All else being equal, which of the following considerations is more important to you when evaluating and selecting a cybersecurity service vendor?

Base: Total sample

IT BUDGET

Most organizations have sizeable IT budgets (e.g., \$100K+).









	TOTAL	PRIVATE	PUBLIC	MUSH
	2022	2022	2022	2022
	500	320	122	54
	%	%	%	%
Under \$10K	 2	2	1	--
\$10K to just under \$25K	 5	5	5	4
\$25K to just under \$50K	 9	11	3	4
\$50K to just under \$100K	 14	15	10	9
\$100K to just under \$250K	 20	20	17	17
\$250K to just under \$500K	 15	16	11	13
\$500K or more	 19	14	36	33
Prefer not to answer	 8	8	6	6
Don't know	 8	8	11	15

Q53A Approximately what was the IT budget of your organization last year?

Base: Total sample

PERCENTAGE OF BUDGET DEVOTED TO CYBER SECURITY

Most commonly, organizations devote in the range of 5%-15% of their IT budget to cybersecurity.

	TOTAL	PRIVATE	PUBLIC	MUSH
	2022	2022	2022	2022
	500	320	122	54
	%	%	%	%
Less than 2%	 7	7	10	7
2% to just under 5%	 15	16	12	7
5% to just under 10%	 24	24	24	22
10% to just under 15%	 19	20	15	17
15% to just under 20%	 11	12	10	9
20% or more	 7	6	6	11
Prefer not to answer	 7	7	6	6
Don't know	 10	8	19	20





Q53B. Approximately what percentage of your organization's IT budget is devoted to cyber security?

Base: Total sample

SUFFICIENCY OF BUDGET DEVOTED TO CYBER SECURITY

Most (58%) believe that their organization’s budget for cyber security is sufficient to protect against cyber attacks.

- Just over three-quarters (77%) of organizations that devote at least 15% of their IT budget to cyber security believe that it is sufficient.

	TOTAL	PRIVATE	PUBLIC	MUSH
	2022	2022	2022	2022
	500	320	122	54
	%	%	%	%
Yes	 58	60	48	46
No	 20	18	25	26
Prefer not to answer	 6	7	6	6
Don't know	 16	15	21	22

Q54C: Is your organization’s budget for cyber security sufficient to protect against cyber attacks?





Base: Total sample

3

CYBERSECURITY: EXPERIENCE AND RESPONSE

INCIDENCE OF USING A CLOUD DNS FIREWALL

Most organizations (87%) have a firewall solution.

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended *				
	2022	2022	2022	2022	2018	2019	2020	2021	2022
	500	320	122	54	500	502	500	510	500
	%	%	%	%	%	%	%	%	%
Yes	 87	86	89	83	42	63	62	73	87
No	 9	10	8	11	23	14	19	17	9
Prefer not to answer	 1	1	-	-	2	5	3	2	1
Don't know	 3	3	3	6	32	18	15	7	3





Q15. Does your organization currently have a firewall solution? (Previous wording) Does your organization currently have a cloud DNS firewall that uses the DNS to detect and block malicious domains (e.g., CIRA D-Zone DNS Firewall, Cisco Umbrella, OpenDNS, etc.)? 2018 wording: Does your organization currently have a cloud firewall that uses the DNS to detect and block malicious domains based on DNS queries rather than on packet inspection or URL filtering?

* Significant wording change over time

Base: Total sample

TYPE OF FIREWALL SOLUTION

Both cloud-based and on-premise firewall solutions are common.

	TOTAL	PRIVATE	PUBLIC	MUSH
	2022	2022	2022	2022
	433	274	108	45c
	%	%	%	%
Cloud-based	 33	32	39	38
On-premise	 27	28	24	24
Both	 38	38	33	36
Don't know	 1	<1	3	2
Prefer not to answer	<1	<1	1	-








Q15A. Is your organization's firewall solution on-premise or cloud-based?

Base: Yes at Q15

C Caution, small base size

FIREWALL CAPABILITIES

Most organizations' firewall solutions include malware blocking, IP blocking and protected DNS. Botnet blocking is least common.

	TOTAL	PRIVATE	PUBLIC	MUSH
	2022	2022	2022	2022
	433	274	108	45c
	%	%	%	%
Malware blocking	 73	75	63	60
IP blocking	 69	70	65	62
Protected DNS	 63	64	56	51
HTTPS website re-direction	 52	55	44	36
Botnet blocking	 44	42	44	49
None of the above	 1	1	-	-
Don't know	 4	1	10	16




Q15B. Which of the following capabilities does your organization's firewall solution include? Select all that apply.

Base: Have a firewall solution

C Caution, small base size

INCIDENCE OF CYBER ATTACKS IN LAST 12 MONTHS

Over 4-in-10 (44%) indicate that their organization has experienced a cyber attack in the last 12 months (attempted or successful).

	TOTAL	PRIVATE	PUBLIC	MUSH
	2022	2022	2022	2022
	500	320	122	54
	%	%	%	%
Yes	 44	44	52	46
No	 52	51	44	50
Don't know	 4	5	3	4

Q2022-16A. Has your organization experienced any cyber attacks in the last 12 months (attempted or successful)?

Base: Total sample

WAYS IN WHICH ORGANIZATION WAS IMPACTED BY CYBER ATTACKS IN LAST 12 MONTHS

The most common impact of cyber attacks is preventing employees from carrying out work. However, at least 2-in-10 experienced direct costs, such as report or recovery costs (22%).

	TOTAL	TOTAL – Trended				
	2022	2018	2019	2020	2021	2022
	219	194	502	315	323	219
	%	%	%	%	%	%
Minor incident(s)	44	29	30	37	45	44
Prevented employees from carrying out day-to-day work	32	25	28	30	33	32
Repair or recovery costs paid to suppliers*	22	20	23	16	19	22
Damage to reputation of organization	19	6	13	15	19	19
Loss of revenue	17	8	11	17	18	17
Discouraged us from carrying out a future planned activity	17	6	7	10	13	17
Loss of customers	15	6	7	12	13	15
Fines from regulators or authorities	14	4	7	14	9	14
Paid ransom payment	12	4	6	9	7	12
Other	<1	1	1	<1	1	<1
No impact at all	12	19	16	16	13	12
Don't know the full extent of the impact	2	5	6	4	3	2
No answer	<1	3	5	1	1	<1

Q20. In what ways, if any, was your organization impacted by cyber attacks in the last 12 months? Select all that apply. (2018 wording: In what ways was your organization impacted by the cyberattacks it experienced in the last 12 months? Select all that apply.)




Base: Among those who say their organization has experienced a cyberattack in the last 12 months

C Caution, small base size

Previous phrasing: "Additional repair or recovery costs"

INCIDENCE OF SUCCESSFUL RANSOMWARE ATTACK

Just over 2-in-10 (22%) indicate that their organization has been a victim of a successful ransomware attack in the last 12 months.




	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended	
	2022	2022	2022	2022	2021	2022
	500	320	122	54	510	500
	%	%	%	%	%	%
Yes	 22	24	22	19	17	22
No	 74	72	72	76	75	74
Don't know	 4	3	6	6	8	4

Q20A. Has your organization been the victim of a successful ransomware attack in the last 12 months?

Base: Total sample

INCIDENCE OF EXFILTRATION OF DATA

Among those that experienced a ransomware attack, 70% indicate that data was exfiltrated (the increase from 59% in 2021 would not be considered statistically significant).




	TOTAL	TOTAL – Trended	
	2022	2021	2022
	111	87	111
	%	%	%
Yes	 70	59	70
No	 28	36	28
Don't know	 2	6	2

Q20B. As part of the ransomware attack, was data exfiltrated from your organization's corporate network or cloud-based service?

Base: Organization has been the victim of a ransomware attack in the last 12 months

INCIDENCE OF PAYING RANSOM DEMANDS

Among those that experienced a ransomware attack, 73% indicate that the organization paid ransom demands.

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended	
	2022	2022	2022	2022	2021	2022
	111	78	BTS (27)	BTS (10)	87	111
	%	%	%	%	%	%
Yes	 73	77	59	60	69	73
No	 23	19	37	30	26	23
Don't know	 4	4	4	10	5	4

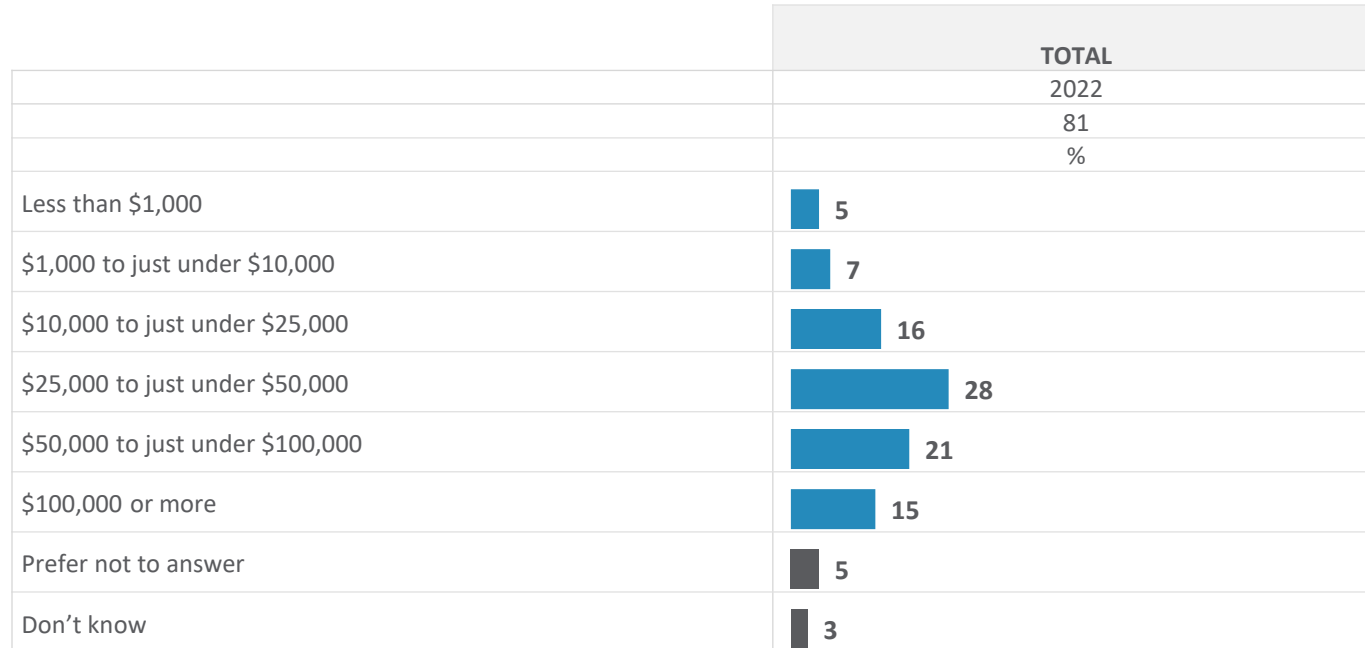
Q20C. Did you or an authorized representative of your organization pay the ransom demands?

Base: Organization has been the victim of a ransomware attack in the last 12 months

BTS Base size too small to report

AMOUNT OF RANSOM PAID

Organizations that paid a ransom typically paid at least \$25,000.











Q20D. Approximately how much, in Canadian dollars, was the ransom payment?

Base: Organization has been the victim of a ransomware attack in the last 12 months

SUPPORT FOR LEGISLATION THAT PROHIBITS RANSOM PAYMENTS





Seven-in-ten (71%) support legislation that would prohibit ransom payments.

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended	
	2022	2022	2022	2022	2021	2022
	500	320	122	54	510	500
	%	%	%	%	%	%
TOTAL SUPPORT	 71	71	71	74	64	71
Strongly support	 35	32	36	28	38	35
Somewhat support	 37	38	35	46	26	37
Neither	 21	22	19	15	22	21
Somewhat oppose	 2	1	6	9	5	2
Strongly oppose	 3	3	1	-	3	3
TOTAL OPPOSE	 6	5	7	9	7	6
Don't know	 3	3	3	2	6	3

Q20F. To what extent would you support or oppose legislation that prohibits Canadian organizations from making ransom payments in response to a ransomware attack?
 Base: Total sample

ANTICIPATED CHANGE IN HUMAN RESOURCES DEVOTED TO CYBERSECURITY IN THE NEXT 12 MONTHS

Almost half (48%) anticipate an increase in human resources devoted to cybersecurity in the next 12 months.





	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended				
	2022	2022	2022	2022	2018	2019	2020	2021	2022
	500	320	122	54	500	502	500	510	500
	%	%	%	%	%	%	%	%	%
Decrease	 11	12	9	6	3	5	9	7	11
Stay the same	 40	38	43	50	66	45	53	44	40
Increase	 48	48	47	41	28	45	34	43	48
Don't know	 1	2	2	4	4	5	4	5	1

Q24. (Previously Q22) Do you anticipate that the **human resources** your organization devotes to cybersecurity will increase, decrease or stay the same in the next 12 months?

Base: Total sample

ANTICIPATED CHANGE IN FINANCIAL RESOURCES DEVOTED TO CYBERSECURITY IN THE NEXT 12 MONTHS










Half (51%) anticipate that the financial resources devoted to cybersecurity will increase in the next 12 months.

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended				
	2022	2022	2022	2022	2018	2019	2020	2021	2022
	500	320	122	54	500	502	500	510	500
	%	%	%	%	%	%	%	%	%
Decrease	 9	9	10	9	3	6	10	10	9
Stay the same	 38	37	43	44	60	35	44	40	38
Increase	 51	52	46	43	30	54	43	47	51
Don't know	 1	1	2	4	6	5	3	3	1

Q25. Do you anticipate that the **financial resources/spending** your organization devotes to cybersecurity will increase, decrease or stay the same in the next 12 months?

Base: Total sample

The biggest perceived risks/threats are unauthorized access/theft of data and malicious software.

TOP THREAT -- % RANKED #1	TOTAL	PRIVATE	PUBLIC	MUSH
	2022	2022	2022	2022
	500	320	122	54
	%	%	%	%
Unauthorized access, manipulation, or theft of data	 22	19	28	26
Malicious software	 21	22	20	20
Scams and fraud (e.g., phishing)	 15	16	13	19
Identity theft	 12	11	14	13
Denial of service	 9	9	9	11
Theft or compromise of software or hardware	 9	9	7	6
Disruption or defacing of web presence	 9	10	7	4
None of the above	 2	3	2	2
Don't know	 1	1	1	--

Q26. In general, which of the following cybersecurity risks or threats do you think could have the biggest negative impact on your organization? Please select the top 3 biggest risks/threats, in order of potential impact. (Previous wording) In general, which of the following cybersecurity risks or threats do you think could have the greatest negative impact on your organization? Select all that apply.

Base: Total sample

The biggest perceived risks/threats are unauthorized access/theft of data and malicious software.

BIGGEST THREATS -- % RANKED #1, #2 OR #3	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended *				
	2022	2022	2022	2022	2018	2019	2020	2021	2022
	500	320	122	54	500	502	500	510	500
	%	%	%	%	%	%	%	%	%
Malicious software	57	61	51	48	61	57	57	60	57
Scams and fraud	46	46	44	48	44	49	55	51	46
Unauthorized access, manipulation, or theft of data	57	53	69	72	56	55	55	50	57
Identity theft	37	37	38	48	41	40	42	44	37
Denial of service	32	34	31	28	23	34	33	39	32
Theft or compromise of software or hardware	31	30	31	33	30	33	30	37	31
Disruption or defacing of web presence	26	25	25	17	28	32	30	30	26
None of the above	2	3	2	2	3	2	2	2	2
Don't know	1	1	1	--	4	4	3	3	1

Q26. In general, which of the following cybersecurity risks or threats do you think could have the biggest negative impact on your organization? Please select the top 3 biggest risks/threats, in order of potential impact. (Previous wording) In general, which of the following cybersecurity risks or threats do you think could have the greatest negative impact on your organization? Select all that apply.

Base: Total sample

* Significant wording change from 2021

The most common activity undertaken to identify cybersecurity risks is monitoring of the firewall.





	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended				
	2022	2022	2022	2022	2018	2019	2020	2021	2022
	500	320	122	54	500	502	500	510	500
	%	%	%	%	%	%	%	%	%
Monitoring firewall	59	58	61	59	61	63	64	58	59
Monitoring employees’ use of computers and the internet	45	45	45	41	41	48	44	46	45
Formal risk assessment of cyber security practices	44	41	48	46	29	39	38	47	44
Security framework/certification	40	41	35	35	-	35	30	42	40
Operation/use of a SOC	38	38	39	39	-	-	-	-	38
Penetration testing	36	35	41	33	23	39	41	40	36
Complete external audit of IT systems	35	33	36	30	24	40	35	38	35
Use of a SIEM	26	29	20	15	-	21	18	24	26
Other	<1	<1	-	-	-	-	<1	1	<1
None	2	2	1	-	8	1	2	2	2
Prefer not to answer	3	3	2	2	4	4	4	3	3
Don’t know	2	2	2	2	10	5	4	3	2

Q27. Which of the following activities, if any, does your organization undertake to identify cybersecurity risks? Select all that apply.

Base: Total sample

INCIDENCE OF MAINTAINING A FORMAL PATCHING POLICY

Six-in-ten (59%) organizations maintain a formal patching policy.






	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended				
	2022	2022	2022	2022	2018	2019	2020	2021	2022
	500	320	122	54	500	502	500	510	500
	%	%	%	%	%	%	%	%	%
Yes	 59	59	62	65	29	56	49	53	59
No	 26	28	19	20	36	19	24	25	26
Prefer not to answer	 5	5	4	2	8	11	11	9	5
Don't know	 11	8	15	13	27	14	16	13	11

Q31. Does your organization maintain a formal patching policy?

Base: Total sample

CYBERSECURITY INSURANCE COVERAGE

Three-quarters (74%) of organizations have cybersecurity insurance coverage. Over one-third (36%) have a cybersecurity-specific policy.







	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended	
	2022	2022	2022	2022	2021	2022
	500	320	122	54	510	500
	%	%	%	%	%	%
Yes, a cybersecurity-specific policy	 36	39	28	24	29	36
Yes, as part of a business insurance policy	 38	38	35	43	30	38
No	 15	13	16	11	17	15
Prefer not to answer	 4	3	5	4	7	4
Don't know	 8	6	16	19	18	8

Q31A. Does your organization currently have cybersecurity insurance coverage? (previous wording) Does your organization have cybersecurity insurance coverage?

Base: Total sample

CHANGES TO CYBERSECURITY INSURANCE POLICY

Most organizations with a policy indicate that their provider has make changes to the coverage. The most common changes are proof/verification of security measures in place and increased premiums.

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended	
	2022	2022	2022	2022	2021	2022
	368	247	77	36c	300	368
	%	%	%	%	%	%
Requested new forms of proof/verification of cybersecurity measures in place	 42	40	35	33	34	42
Increased premiums	 39	39	36	36	35	39
Changed eligibility criteria for obtaining/renewing coverage	 33	33	35	28	29	33
Reduced reimbursement amounts for ransomware attacks	 29	29	23	28	23	29
Other	<1	-	-	-	-	<1
None/no changes	 15	17	10	11	15	15
Don't know	 7	5	13	17	11	7



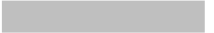




Q31B. In the past year, has your cybersecurity insurance provider made any of the following changes to your organization's coverage?

Base: Organization has cybersecurity insurance coverage

C Caution, small base size

CHANGE IN MEASURES/AUDIT CONTROL WITH THIRD PARTY VENDORS

Six-in-ten (61%) indicate that cybersecurity measures or audit controls are more common requirements in contracts with third party vendors.




	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended	
	2022	2022	2022	2022	2021	2022
	500	320	122	54	510	500
	%	%	%	%	%	%
TOTAL MORE COMMON	 61	62	55	57	56	61
Much more common	 24	24	24	22	22	24
A little more common	 36	37	31	35	34	36
No change	 35	35	37	33	35	35
A little less common	 1	1	2	2	1	1
Much less common	-	-	-	-	-	-
TOTAL LESS COMMON	 1	1	2	2	1	1
Don't know	 3	2	7	7	8	3

Q31C. In the past year, have you noticed any change in cybersecurity measures/audit control required for your organization's contracts with external third-party vendors? Would you say that such requirements are...?

Base: Total sample

AWARENESS OF BILL C-27




Just over half (55%) are aware of Bill C-27.

	TOTAL	PRIVATE	PUBLIC	MUSH
	2022	2022	2022	2022
	500	320	122	54
	%	%	%	%
Yes	 55	56	52	48
No	 41	39	45	48
Don't know	 4	5	3	4

Q2022-38. On June 16, 2022, the Canadian government tabled Bill C-27 “An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts.” The Bill is designed to update Canada’s federal private sector privacy law, the Personal Information Protection and Electronic Documents Act (PIPEDA), to create a new tribunal, and to propose new rules for artificial intelligence (AI) systems. Were you aware of Bill C-27 before now?

Base: Total sample

Three-quarters of those aware of Bill C-27 indicate that their organization is ready to implement the new requirements.

	TOTAL	PRIVATE	PUBLIC	MUSH
	2022	2022	2022	2022
	276	180	63	26c
	%	%	%	%
Yes	 75	76	73	73
No	 18	19	11	4
Don't know	 7	5	16	23








Q2022-39. Is your organization ready to implement the new requirements regarding consumer privacy protection that are outlined in the legislation?

Base: Aware of legislation

C Caution, small base size

LEVEL OF CONCERN ABOUT IMPACT OF BILL C-27

Six-in-ten (59%) are concerned about the potential impact of Bill C-27 on their organization.









	TOTAL	PRIVATE	PUBLIC	MUSH
	2022	2022	2022	2022
	500	320	122	54
	%	%	%	%
TOTAL CONCERNED	 59	61	52	56
Very concerned	 16	15	15	19
Somewhat concerned	 43	46	37	37
Not very concerned	 26	27	30	31
Not concerned at all	 4	4	3	-
TOTAL NOT CONCERNED	 31	31	33	31
Don't know	 10	9	16	13

Q2022-40. How concerned are you about the potential impact of Bill C-27 on your organization?

Base: Total sample

RATING OF PRIVACY PROTECTION FOR CONSUMERS IN CANADA

Half (49%) rate privacy protection for consumers in Canada as excellent or good. Overall, relatively few rate it as poor (14%); an exception is those in ‘MUSH’ organizations (30% rate it as poor).





	TOTAL	PRIVATE	PUBLIC	MUSH
	2022	2022	2022	2022
	500	320	122	54
	%	%	%	%
TOTAL EXCELLENT/GOOD	 49	52	40	39
Excellent	 11	12	11	9
Good	 38	40	30	30
Average	 36	36	38	31
Poor	 10	8	16	22
Very poor	 4	3	6	7
TOTAL POOR/VERY POOR	 14	11	22	30
Don't know	 1	2	-	-

Q2022-41 Overall, how would you rate privacy protection for consumers in Canada?

Base: Total sample

INCIDENCE OF STORING PERSONAL INFORMATION OF CUSTOMERS/EMPLOYEES/SUPPLIERS/VENDORS/PARTNERS

Most (66%) indicate their organization stores the personal information of customers, employees, suppliers, vendors or partners.








	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended				
	2022	2022	2022	2022	2018	2019	2020	2021	2022
	500	320	122	54	500	502	500	510	500
	%	%	%	%	%	%	%	%	%
Yes	 66	63	74	74	59	64	66	66	66
No	 24	26	17	17	27	18	22	20	24
Prefer not to answer	 7	8	6	6	10	13	9	10	7
Don't know	 3	3	3	4	5	5	3	4	3

Q41. Does your organization store any personal information of customers, employees, suppliers, vendors or partners?

Base: Total sample

ESTIMATED NUMBER OF BREACHES IN LAST YEAR

Three-in ten (29%) organizations experienced a breach of customer and/or employee data last year.








	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended			
	2022	2022	2022	2022	2019	2020	2021	2022
	500	320	122	54	502	500	510	500
	%	%	%	%	%	%	%	%
0	 32	33	25	20	42	38	36	32
1	 7	10	-	-	4	7	7	7
2	 8	8	7	6	4	5	5	8
3 to 4	 4	4	5	2	3	4	3	4
5 to 9	 4	4	3	6	3	4	5	4
10 or more	 5	6	5	6	4	5	5	5
Don't know	 39	36	56	61	40	38	39	39

Q41A. As far as you know, how many breaches of customer and/or employee data did your organization experience in the last year?

Base: Total sample

WHO WAS INFORMED ABOUT DATA BREACHES

Among organizations that experienced a data breach, just over half (53%) informed management/senior leadership, 49% informed the Board, and 44% informed customers.

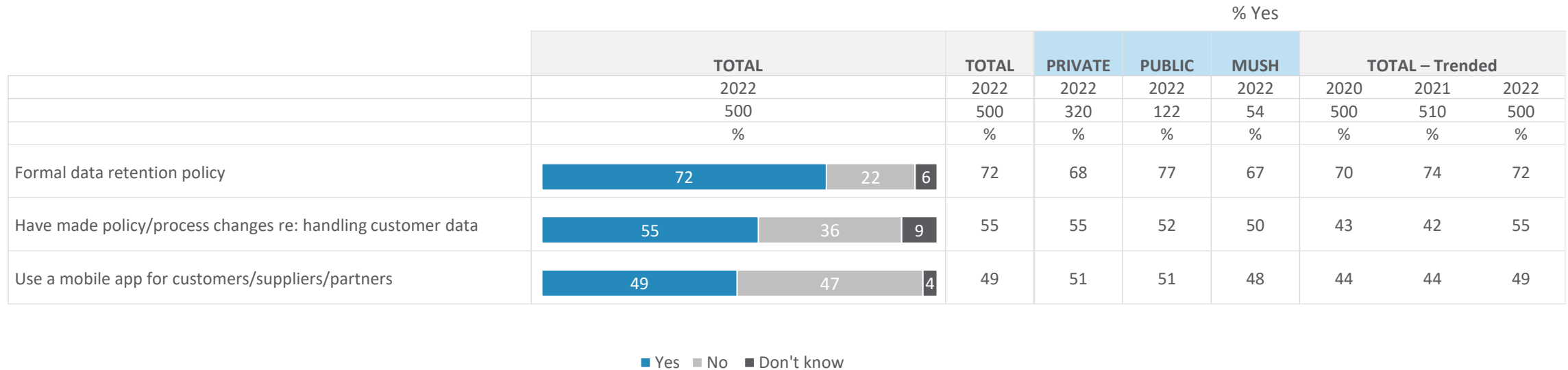
	TOTAL	TOTAL – Trended			
	2022	2019	2020	2021	2022
	144	90	122	127	144
	%	%	%	%	%
Management/senior leadership	 53	40	50	50	53
Board of Directors	 49	21	34	43	49
Customers	 44	48	44	41	44
Regulatory body	 35	58	36	39	35
Law enforcement	 35	37	31	29	35
Other	-	-	2	2	-
None of the above	 1	-	2	4	1
Prefer not to answer	 1	2	1	2	1

Q41B. Which of the following, if any, did you inform about the data breach? Select all that apply.

Base: 1 or more at Q41a

CHANGE IN POLICY OR PROCESSES

Most organizations (72%) have a formal data retention policy. Half or more indicate they use a mobile app and/or have made policy or process changes in how data is handled. The proportion that has made policy/process changes re: handling customer data is up from 42% in 2021 to 55% in 2022.



- Q41C. Has your organization made any policy or process changes in how it handles customer data since 2019? (Previous wording) Has your organization made any policy or process changes in how it handles customer data since the implementation of the new PIPEDA requirements?
- Q41D. Does your organization have a formal data retention policy?
- Q41E. Does your organization use a mobile app for customers, suppliers and/or partners?
- Base: Total sample

MOBILE APP TRACKING

Those that use a mobile app are most likely to say it tracks contact information (61%). User location and device identifiers are also commonly tracked.

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended		
	2022	2022	2022	2022	2020	2021	2022
	247	163	62	26c	219	222	247
	%	%	%	%	%	%	%
Contact information (email or phone number)	61	63	56	50	51	56	61
Device identifiers (UDID or IMEI)	48	52	40	42	39	43	48
User location (GPS or other methods)	44	49	34	46	42	46	44
Clipboard data	34	34	26	27	34	23	34
Other	<1	1	-	-	1	-	<1
None of the above	4	2	5	-	5	6	4
Don't know	3	1	8	15	7	6	3




Q41F. What does the mobile app track?

Base: Yes at 41e

C Caution, small base size

USE OF THIRD-PARTY INTEGRATION SERVICE PARTNERS

Half (51%) use third-party integration service partners.

	TOTAL	PRIVATE	PUBLIC	MUSH
	2022	2022	2022	2022
	500	320	122	54
	%	%	%	%
Yes	 51	50	55	46
No	 42	43	36	37
Don't know	 7	7	9	17

Q2022-42 Does your organization use any third-party integration service partners?





Base: Total sample

4

REMOTE/HYBRID WORK

ORGANIZATION'S WORK ENVIRONMENT

One-half of organizations have hybrid work environments.









	TOTAL	PRIVATE	PUBLIC	MUSH
	2022	2022	2022	2022
	500	320	122	54
	%	%	%	%
Hybrid (partially on-site/remote)	 50	49	48	39
Fully on-site/in office	 34	32	40	48
Fully remote	 15	18	11	11
No answer	 1	1	1	2

Q2022-51A Which of the following best describes your organization's work environment?

Base: Total sample

VULNERABILITY TO CYBER THREATS DUE TO REMOTE WORK ENVIRONMENT

Just over half (55%) characterize their organization as more vulnerable to cyber threats because its employees work remotely.

	TOTAL	PRIVATE	PUBLIC	MUSH
	2022	2022	2022	2022
	324	214	72	BTS (27)
	%	%	%	%
TOTAL MORE VULNERABLE	 55	58	49	48
Much more vulnerable	 11	10	13	11
Somewhat more vulnerable	 44	48	36	37
About the same level of vulnerability	 38	34	47	52
Somewhat less vulnerable	 5	6	3	-
Much less vulnerable	 1	1	-	-
TOTAL LESS VULNERABLE	 6	7	3	-
Don't know	 1	1	1	-








Q2022-51B Would you say that your organization is more or less vulnerable to cyber threats because employees work remotely?

Base: Fully remote/Hybrid at Q51A

BTS Base size too small to report

PREPAREDNESS TO RESPOND TO CYBER THREATS

Most (86%) indicate that their organization is prepared to combat cyber threats that arise because employees work remotely.

	TOTAL	PRIVATE	PUBLIC	MUSH
	2022	2022	2022	2022
	324	214	72	27c
	%	%	%	%
TOTAL PREPARED	 86	87	82	81
Very prepared	 26	27	21	15
Somewhat prepared	 61	60	61	67
Not very prepared	 10	11	13	15
Not prepared at all	 1	<1	3	-
TOTAL NOT PREPARED	 11	11	15	15
Don't know	 2	2	3	4

Q2022-51C How prepared is your organization to combat cyber threats that arise because employees work remotely?

Base: Fully remote/Hybrid at Q51A

C Caution, small base size

REASONS ORGANIZATION IS NOT PREPARED

The small proportion that indicates their organization is unprepared to combat threats tend to mention budget constraints, lack of talent or resources devoted cyber security, and insufficient training for employees.







VERBATIM RESPONSES:

- Budget constraint
- lack of funding
- The network resources are limited and may not encompass every variable when WFH and with personal actions and reactions online
- not enough staff
- Talent
- The IT department is useless
- poor audit
- It's too sensitive to say.
- Can't control employees as well on insecure networks.
- employees using their own devices
- (Employees) need way more education on these concepts and technology than we have given them or can spare time for.
- old device security system
- Its late and there are some financial issues to be ready for that types of threats
- too quick and ad-hoc, little security consideration
- systemic incompetence within the public service, they cant even pay their employees correctly (phoenix)
- Remote work introduces greatly increased use of personal devices to access our systems.
- they are not trained to well
- The threats do not arise
- We have not had a breach that I am aware of, so it would be the tech teams first time dealing with it

Q2022-51D What are the main reasons that your organization is not prepared to combat cyber threats that arise because employees work remotely? Please be as specific as possible.

Base: Total sample

Most (82%) indicate that their organization has a cyber incident response plan.







	TOTAL	PRIVATE	PUBLIC	MUSH
	2022	2022	2022	2022
	500	320	122	54
	%	%	%	%
TOTAL YES	 82	83	80	74
Yes, a comprehensive plan	 37	39	33	28
Yes, a basic plan	 45	44	47	46
No, but currently developing one	 9	8	9	11
No plan	 5	5	4	2
Don't know	 4	4	7	13

Q2022-51E Does your organization have a cyber incident response plan?

Base: Total sample

USE OF CYBER INCIDENT RESPONSE PLAN

Six-in-ten organizations have used their cyber incident response plan in the last 12 months.

	TOTAL	PRIVATE	PUBLIC	MUSH
	2022	2022	2022	2022
	411	267	97	40c
	%	%	%	%
None	 33	33	31	28
1-5	 36	35	36	43
6-10	 15	19	11	5
11-15	 6	7	4	5
More than 15	 2	1	2	5
Don't know	 7	4	15	15




Q2022-51F How many times have you used your cyber incident response plan in the last 12 months?

Base: Organization has a cyber incident response plan

C Caution, small base size

ALERT FATIGUE

Just over one-third (35%) indicate that they have experienced ‘alert fatigue’ in the last 12 months.

	TOTAL	PRIVATE	PUBLIC	MUSH
	2022	2022	2022	2022
	411	267	97	40c
	%	%	%	%
Yes	 35	36	38	33
No	 59	60	53	55
Don't know	 6	4	9	13

Q2022-51G ‘Alert fatigue’ occurs when monitoring systems send so many alerts that the alerts get ignored or are too overwhelming in volume to handle. In the last 12 months, have you experienced alert fatigue?

Base: Organization has a cyber incident response plan

C Caution, small base size

5

SAMPLE CHARACTERISTICS

Sample Characteristics



AGE

Total sample n=500	%
18-29	9
30-39	30
40-49	33
50-59	21
60 or older	8



PROVINCE OR TERRITORY

Total sample n=500	%
Newfoundland	1
Prince Edward Island	<1
Nova Scotia	2
New Brunswick	1
Quebec	11
Ontario	52
Manitoba	2
Saskatchewan	1
Alberta	11
British Columbia	18

REGION

Total sample n=500	%
Atlantic	4
Quebec	11
Ontario	52
West	34



GENDER

Total sample n=500	%
Male	75
Female	23
Non-binary	1
Prefer not to answer	1



EMPLOYEE OR SELF-EMPLOYED

Total sample n=500	%
Employee/Contractor working for a single organization	88
A business owner	12



TYPE OF ORGANIZATION

Employees n=442	%
Private sector	72
Public/Not-for-profit sector	28



PUBLIC SECTOR ORGANIZATION

Public sector n=122	%
Municipal government or agency	6
Provincial government or agency	12
Federal government or agency	26
Hospital or other health care organization	9
Primary or secondary school	2
College or university	20
School board	7
Public utility	5
Charity	2
Non-profit	9
Other	1



COUNTRY IN WHICH ORG OPERATES

Total sample n=500	%
In Canada only	62
In countries outside of Canada	10
Both	26
Prefer not to answer	1

Sample Characteristics

ANNUAL REVENUE

Private organization n=320	%
Under \$1M	2
\$1M to just under \$10M	18
\$10M to just under \$25M	22
\$25M to just under \$100M	22
\$100M to just under \$250M	13
\$250M or more	15
Prefer not to answer	7
Don't know/Not sure	3



NUMBER OF YEARS IN OPERATION

Total sample n=500	%
Less than 1 year	1
1-2	4
3-5	11
6-10	19
11-20	22
More than 20 years	41
Prefer not to answer	2



EMPLOYEES USE COMPUTER/MOBILE DEVICE AT LEAST 20% OF THE TIME

Total sample n=500	%
50-99	22
100-249	30
250-499	17
500-999	19
1000 or more (public sector only)	11



FAMILIARITY WITH ORGANIZATION'S COMPUTER SYSTEMS/IT FUNCTIONS

Total sample n=500	%
Very familiar	62
Somewhat familiar	38



IT AREAS INCLUDED WITHIN JOB

Employees n=500	%
System administration	56
Desktop IT	58
Cybersecurity	64
Networking	59
Other technical	26
Non-technical decision-making	33
Other non-technical areas (e.g., HR, finance, admin, etc.)	22

IT BUDGET

Total sample n=500	%
Under \$10,000	2
\$10,000 to just under \$25,000	5
\$25,000 to just under \$50,000	9
\$50,000 to just under \$100,000	14
\$100,000 to just under \$250,000	20
\$250,000 to just under \$500,000	15
More than \$500,000	19
Prefer not to answer	8
Don't know	8