THE
STRATEGIC
COUNSEL

EXPERIENCE • PASSION • CREATIVITY

TORONTO | OTTAWA | CALGARY
www.thestrategiccounsel.com

cira

A REPORT TO
CIRA

PERCEPTIONS AND ATTITUDES OF CANADIAN ORGANIZATIONS TOWARD CYBERSECURITY

August 2023

CONTENTS

1

OBJECTIVES AND METHODOLOGY

About the Research

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.

METHODOLOGY

A total of n=500 cybersecurity decision-makers (employees or owners) completed a 10-12 minute online survey in August, 2023. 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 2023 findings are compared to the results from previous years.

2

RESOURCES AND TRAINING

INCIDENCE OF CONDUCTING CYBERSECURITY AWARENESS TRAINING

Most organizations (97%) conduct cybersecurity awareness training. Nine-in-ten indicate that it is mandatory for at least some employees.

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended				
	2023	2023	2023	2023	2019	2020	2021	2022	2023
	500	381	87	37c	502	500	510	500	500
	%	%	%	%	%	%	%	%	%
TOTAL YES	**97**	97	98	97	87	94	93	96	97
Yes, mandatory training for some employees	**48**	51	36	35	32	34	41	44	48
Yes, mandatory training for all employees	**42**	41	48	41	41	48	43	44	42
Yes, optional training (some or all employees)	**7**	5	14	22	15	12	9	8	7
No	**2**	3	2	3	11	6	7	4	2
Don't know	**<1**	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
C Caution: small base size

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				
	2023	2023	2023	2023	2019	2020	2021	2022	2023
	486	369	85	36c	439	467	474	480	486
	%	%	%	%	%	%	%	%	%
In-house developed courses/training materials/(previous) *We create training material and promote it internally*	49	47	53	50	54	57	61	48	49
Refresher training	47	49	36	31	-	-	-	46	47
Third-party developed courses/training materials	47	48	34	31	-	-	-	44	47
Phishing simulations/(previous) *We conduct phishing simulations**	43	43	42	33	21	37	44	42	43
In-house developed lunch-and-learns/workshops/seminars/(previous) *Lunch-and-learns/workshops*	39	40	32	33	36	35	39	39	39
Third-party developed lunch-and-learns/workshops/seminars /(previous) *We hire a third-party to conduct seminar-style training programs*	39	40	28	25	32	31	35	31	39
Extra/supplementary training for high-risk groups	36	35	32	25	-	-	-	37	36
Micro-learning modules	34	34	29	22	-	-	-	29	34
Games	10	9	6	-	-	-	-	10	10
Other	1	1	-	-	2	1	2	<1	1
Don't know	1	1	1	3	1	<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"
C Caution: small base size

FREQUENCY OF CONDUCTING CYBERSECURITY AWARENESS TRAINING

Most organizations conduct cybersecurity awareness training quarterly or less. The proportion that conducts training at least quarterly (70%) continues to trend upward relative to 2019 (58%).

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended				
	2023	2023	2023	2023	2019	2020	2021	2022	2023
	486	369	85	36c	439	467	474	480	486
	%	%	%	%	%	%	%	%	%
Annually or less	30	27	42	36	40	40	41	32	30
Quarterly	57	59	46	50	36	49	46	55	57
Monthly	13	13	8	11	12	9	11	12	13
More than monthly/ongoing	–	-	-	-	10	-	-	-	-
Don't know	1	<1	4	3	2	1	2	1	1

Q8. About how often does your organization conduct cybersecurity awareness training?
Base: Conduct cyber security training at Q6
C Caution, small base size

REASONS FOR NOT CONDUCTING CYBERSECURITY AWARENESS TRAINING

The very small proportion of organizations that don't conduct training tend to cite lack of awareness (have never considered it), cost, and time as reasons.

	TOTAL	TOTAL – Trended				
	2023	2019	2020	2021	2022	2023
	12c	57	32c	34c	19c	12c
	%	%	%	%	%	%
Have never considered it as a solution*	33	26	13	35	21	33
Too expensive	25	21	22	21	16	25
Too time consuming	25	14	16	21	37	25
Insufficient IT human resources	17	44	31	44	58	17
No executive buy-in	8	12	28	21	26	8
Previous training attempts were unsuccessful	8	5	-	6	5	8
Prefer to spend budget on other cybersecurity tools	8	-	-	-	5	8
Unsure of best approach/options	-	32	19	21	16	-
Don't believe training works*	-	4	3	6	-	-
Other	17	4	9	12	11	17
Don't know	17	5	16	9	5	17

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 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	TOTAL – Trended	
	2023	2023	2023	2023	2022	2023
	500	381	87	37c	500	500
	%	%	%	%	%	%
Data sovereignty	69	68	72	70	63	69
Price	30	31	25	30	27	30
Don't know	1	1	2	-	9	1

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
C Caution, small base size

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

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended	
	2023	2023	2023	2023	2022	2023
	500	381	87	37c	500	500
	%	%	%	%	%	%
Under $10K	1	1	1	-	2	1
$10K to just under $25K	4	5	-	-	5	4
$25K to just under $50K	9	10	9	3	9	9
$50K to just under $100K	16	18	10	16	14	16
$100K to just under $250K	23	23	20	32	20	23
$250K to just under $500K	18	18	18	22	15	18
$500K or more	19	18	24	14	19	19
Prefer not to answer	4	4	2	-	8	4
Don’t know	6	4	15	14	8	6

Q53A Approximately what was the IT budget of your organization last year?
Base: Total sample
C Caution, small base size

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	TOTAL – Trended	
	2023	2023	2023	2023	2022	2023
	500	381	87	37c	500	500
	%	%	%	%	%	%
None	1	1	-	-	-	1
Less than 2%	5	6	5	3	7	5
2% to just under 5%	18	18	11	8	15	18
5% to just under 10%	26	25	33	41	24	26
10% to just under 15%	23	26	11	8	19	23
15% to just under 20%	12	11	14	19	11	12
20% or more	7	7	6	5	7	7
Prefer not to answer	2	3	1	-	7	2
Don’t know	6	3	18	16	10	6

Q53B. Approximately what percentage of your organization’s IT budget is devoted to cyber security?
Base: Total sample
C Caution, small base size

SUFFICIENCY OF BUDGET DEVOTED TO CYBER SECURITY

Most (65%) believe that their organization's budget for cyber security is sufficient to protect against cyber attacks.

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended	
	2023	2023	2023	2023	2022	2023
	500	381	87	37c	500	500
	%	%	%	%	%	%
Yes	65	70	49	43	58	65
No	19	17	22	30	20	19
Prefer not to answer	2	1	3	3	6	2
Don't know	14	12	25	24	16	14

Q54C: Is your organization's budget for cyber security sufficient to protect against cyber attacks?
Base: Total sample
C Caution, small base size

CHANGE IN HUMAN RESOURCES DEVOTED TO IT SYSTEMS MANAGEMENT AND CYBERSECURITY

Most (70%) indicate that the human resources their organization devotes to IT systems management and cybersecurity have increased in the past 12 months.

	TOTAL	PRIVATE	PUBLIC	MUSH
	2023	2023	2023	2023
	500	381	87	37c
	%	%	%	%
Yes	**70**	71	60	54
No	**25**	24	32	41
Prefer not to answer	**<1**	<1	-	-
Don't know	**5**	4	8	5

Q2023-14A Have the human resources your organization devotes to IT systems management and cybersecurity increased in the past 12 months?
Base: Total answering
C Caution, small base size

REASONS FOR LACK OF INCREASE IN HUMAN RESOURCES

The most common reason for not increasing human resources in the past 12 months is lack of need/having sufficient staff. Considerably fewer cite other reasons.

	TOTAL	PRIVATE	PUBLIC	MUSH
	2023	2023	2023	2023
	125	93	28c	15c
	%	%	%	%
No need/have sufficient staff	49	52	39	33
Lack of financial resources to hire more staff	27	24	43	53
Difficulty finding qualified candidates	19	19	18	20
Difficulty recruiting qualified candidates due to competition	14	15	7	7
Our organization outsources IT systems management and cybersecurity	11	13	4	-
Other	1	1	-	-
Don't know	3	3	4	-

Q2023-14B What are the main reasons that human resources devoted to IT systems management and cybersecurity have not increased in the past 12 months? Select all that apply.
Base: No at Q14A
C Caution, small base size

CHANGE IN FINANCIAL RESOURCES ALLOCATED TO IT SYSTEMS MANAGEMENT AND CYBERSECURITY IN PAST 12 MONTHS

Almost three-quarters (73%) indicate that the financial resources allocated to IT systems management and cybersecurity have increased in the past 12 months.

	TOTAL	PRIVATE	PUBLIC	MUSH
	2023	2023	2023	2023
	500	381	87	37c
	%	%	%	%
Yes	73	74	62	59
No	23	23	31	35
Prefer not to answer	1	1	-	-
Don't know	3	2	7	5

Q2023-14C Have the financial resources your organization allocates to IT systems management and cybersecurity increased in the past 12 months?
Base: Total answering
C Caution, small base size

PERCENTAGE CHANGE IN FINANCIAL RESOURCES ALLOCATION IN PAST 12 MONTHS

Most commonly, the financial resources allocated to IT systems management and cybersecurity increased by 10%-25%.

	TOTAL	PRIVATE	PUBLIC	MUSH
	2023	2023	2023	2023
	366	282	54	22c
	%	%	%	%
Less than 10%	14	15	15	18
Between 10% and 25%	53	56	41	36
Between 26% and 50%	25	25	20	18
More than 50%	5	3	9	9
Prefer not to answer	1	-	2	-
Don’t know	2	1	13	18

Q2023-14D By approximately what percentage did the financial resources allocated to IT systems management and cybersecurity increase in the past 12 months?
Base: Yes at Q14C
C Caution, small base size

Hardware is most likely to be selected as the oldest technology still in use.

	TOTAL	PRIVATE	PUBLIC	MUSH
	2023	2023	2023	2023
	500	381	87	37c
	%	%	%	%
Hardware	**39**	43	29	30
Software	**26**	23	31	27
Operating system	**24**	24	28	30
Prefer not to answer	**3**	3	3	-
Don’t know	**7**	7	9	14

Q2023-51R As far as you know, which of the following is the oldest technology still used in your organization?
Base: Total answering
C Caution, small base size

YEAR OLDEST TECHNOLOGY WAS RELEASED

Over one-third (37%) are using technology released prior to 2010.

	TOTAL	PRIVATE	PUBLIC	MUSH
	2023	2023	2023	2023
	500	381	87	37c
	%	%	%	%
1970-1989	10	8	18	19
1990-1999	7	5	14	16
2000-2009	20	21	14	8
2010-2019	38	41	25	30
2020-2023	8	9	3	3
Don't know	18	16	25	24

Q2023-52S As far as you know, in what year was the oldest technology still used in your organization released?
Base: Total answering
C Caution, small base size

3

CYBERSECURITY: EXPERIENCE AND RESPONSE

INCIDENCE OF CYBER ATTACKS IN LAST 12 MONTHS

Four-in-ten (41%) indicate that their organization has experienced a cyber attack in the last 12 months (attempted or successful).

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended	
	2023	2023	2023	2023	2022	2023
	500	381	87	37c	500	500
	%	%	%	%	%	%
Yes	**41**	40	43	38	44	41
No	**56**	59	49	57	52	56
Don't know	**3**	1	8	5	4	3

Q2022-16A. Has your organization experienced any cyber attacks or incidents in the last 12 months? (previous phrasing) Has your organization experienced any cyber attacks in the last 12 months (attempted or successful)?
Base: Total sample
C Caution, small base size

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 loss of revenue (29%), or repair or recovery costs (22%).

	TOTAL	TOTAL – Trended					
	2023	2018	2019	2020	2021	2022	2023
	205	194	502	315	323	219	205
	%	%	%	%	%	%	%
Minor incident(s)	38	29	30	37	45	44	38
Prevented employees from carrying out day-to-day work	36	25	28	30	33	32	36
Loss of revenue	29	8	11	17	18	17	29
Damage to reputation of organization	24	6	13	15	19	19	24
Repair or recovery costs paid to suppliers*	22	20	23	16	19	22	22
Discouraged us from carrying out a future planned activity	22	6	7	10	13	17	22
Loss of customers	20	6	7	12	13	15	20
Paid ransom payment	19	4	6	9	7	12	19
Fines from regulators or authorities	18	4	7	14	9	14	18
Other	<1	1	1	<1	1	<1	<1
No impact at all	6	19	16	16	13	12	6
Don’t know the full extent of the impact	1	5	6	4	3	2	1
No answer	-	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 (23%) indicate that their organization has been a victim of a successful ransomware attack in the last 12 months.

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended		
	2023	2023	2023	2023	2021	2022	2023
	500	381	87	37c	510	500	500
	%	%	%	%	%	%	%
Yes	23	21	24	22	17	22	23
No	73	75	68	70	75	74	73
Prefer not to answer	<1	<1	-	-	-	-	<1
Don't know	4	3	8	8	8	4	4

Q20A. Has your organization been the victim of a successful ransomware attack in the last 12 months?
Base: Total sample
C Caution, small base size

INCIDENCE OF EXFILTRATION OF DATA

Among those that experienced a ransomware attack, 71% indicate that data was exfiltrated (the increase from 59% in 2021 would not be considered statistically significant).

	TOTAL	TOTAL – Trended		
	2023	2021	2022	2023
	113	87	111	113
	%	%	%	%
Yes	**71**	59	70	71
No	**25**	36	28	25
Don’t know	**4**	6	2	4

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, 70% indicate that the organization paid ransom demands.

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended		
	2023	2023	2023	2023	2021	2022	2023
	113	81	21c	8c	87	111	113
	%	%	%	%	%	%	%
Yes	**70**	69	67	50	69	73	70
No	**29**	31	29	50	26	23	29
Don't know	**1**	-	5	-	5	4	1

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
C Caution, small base size

AMOUNT OF RANSOM PAID

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

	TOTAL	TOTAL – Trended	
	2023	2022	2023
	79	81	79
	%	%	%
Less than $1,000	4	5	4
$1,000 to just under $10,000	18	7	18
$10,000 to just under $25,000	23	16	23
$25,000 to just under $50,000	25	28	25
$50,000 to just under $100,000	22	21	22
$100,000 or more	6	15	6
Prefer not to answer	1	5	1
Don’t know	1	3	1

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

Three-quarters (75%) support legislation that would prohibit ransom payments (up from 64% in 2021).

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended		
	2023	2023	2023	2023	2021	2022	2023
	500	381	87	37c	510	500	500
	%	%	%	%	%	%	%
TOTAL SUPPORT	**75**	74	78	86	64	71	75
Strongly support	**31**	31	32	30	38	35	31
Somewhat support	**44**	43	46	57	26	37	44
Neither	**17**	19	11	5	22	21	17
Somewhat oppose	**4**	3	5	5	5	2	4
Strongly oppose	**2**	2	2	3	3	3	2
TOTAL OPPOSE	**6**	6	7	8	7	6	6
Don't know	**2**	2	3	-	6	3	2

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
C Caution, small base size

CYBERSECURITY RISKS/THREATS THAT COULD HAVE GREATEST NEGATIVE IMPACT

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

TOP THREAT -- % RANKED #1	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended	
	2023	2023	2023	2023	2022	2023
	500	381	87	37c	500	500
	%	%	%	%	%	%
Unauthorized access, manipulation, or theft of data	22	22	23	30	22	22
Malicious software	22	22	21	16	21	22
Scams and fraud (e.g., phishing)	17	18	16	22	15	17
Theft or compromise of software or hardware	10	10	10	8	9	10
Denial of service	8	8	10	8	9	8
Generative artificial intelligence-enabled attacks	8	8	6	5	-	8
Identity theft	7	8	8	8	12	7
Disruption or defacing of web presence	6	6	3	3	9	6
Other	<1	-	1	-	-	<1
None of the above	<1	-	-	-	2	<1
Don't know	<1	-	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

C Caution, small base size

CYBERSECURITY RISKS/THREATS THAT COULD HAVE GREATEST NEGATIVE IMPACT

The biggest perceived risks/threats are unauthorized access/theft of data, malicious software, and scams/fraud. Two-in-ten (21%) select generative AI-enabled attacks.

BIGGEST THREATS -- % RANKED #1, #2 OR #3	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended *					
	2023	2023	2023	2023	2018	2019	2020	2021	2022	2023
	500	381	87	37c	500	502	500	510	500	500
	%	%	%	%	%	%	%	%	%	%
Malicious software	57	57	55	62	61	57	57	60	57	57
Unauthorized access, manipulation, or theft of data	52	51	53	54	56	55	55	50	57	52
Scams and fraud	50	49	52	76	44	49	55	51	46	50
Identity theft	34	33	38	30	41	40	42	44	37	34
Theft or compromise of software or hardware	33	35	25	27	30	33	30	37	31	33
Disruption or defacing of web presence	25	27	20	16	28	32	30	30	26	25
Denial of service	24	25	26	16	23	34	33	39	32	24
Generative artificial intelligence-enabled attacks	21	22	18	16	-	-	-	-	-	21
Other	<1	-	1	-	-	-	-	-	-	<1
None of the above	<1	-	-	-	3	2	2	2	2	<1
Don't know	<1	-	1	-	4	4	3	3	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

C Caution, small base size

The most common activity undertaken to identify cybersecurity risks remains monitoring of the firewall. Monitoring employees' use of computers and the internet is also common.

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended					
	2023	2023	2023	2023	2018	2019	2020	2021	2022	2023
	500	381	87	37c	500	502	500	510	500	500
	%	%	%	%	%	%	%	%	%	%
Monitoring firewall	57	56	63	68	61	63	64	58	59	57
Monitoring employees' use of computers and the internet	52	51	47	41	41	48	44	46	45	52
Formal risk assessment of cyber security practices	46	47	44	30	29	39	38	47	44	46
Security framework/certification	44	46	38	41	-	35	30	42	40	44
Penetration testing	42	41	44	46	23	39	41	40	36	42
Complete external audit of IT systems	41	44	33	24	24	40	35	38	35	41
Operation/use of a SOC	37	36	36	30	-	-	-	-	38	37
Use of a SIEM	24	23	26	19	-	21	18	24	26	24
Other	–	-	-	-	-	-	<1	1	<1	-
None	1	1	1	-	8	1	2	2	2	1
Prefer not to answer	–	-	-	-	4	4	4	3	3	-
Don't know	1	-	3	3	10	5	4	3	2	1

Q27. Which of the following activities, if any, does your organization undertake to identify cybersecurity risks? Select all that apply.
Base: Total sample
C Caution, small base size

CYBERSECURITY INSURANCE COVERAGE

Just over three-quarters (77%) of organizations have cybersecurity insurance coverage. Over one-third (36%) have a cybersecurity-specific policy.

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended		
	2023	2023	2023	2023	2021	2022	2023
	500	381	87	37c	510	500	500
	%	%	%	%	%	%	%
Yes, a cybersecurity-specific policy	36	35	32	35	29	36	36
Yes, as part of a business insurance policy	41	46	25	32	30	38	41
No	16	14	24	19	17	15	16
Prefer not to answer	2	2	3	3	7	4	2
Don’t know	5	3	15	11	18	8	5

Q31A. Does your organization currently have cybersecurity insurance coverage? (previous wording) Does your organization have cybersecurity insurance coverage?
Base: Total sample
C Caution, small base size

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 increased premiums, proof/verification of security measures in place, and changed eligibility criteria.

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended		
	2023	2023	2023	2023	2021	2022	2023
	385	307	50	25c	300	368	385
	%	%	%	%	%	%	%
Increased premiums	**41**	42	32	24	35	39	41
Requested new forms of proof/verification of cybersecurity measures in place	**39**	39	42	40	34	42	39
Changed eligibility criteria for obtaining/renewing coverage	**37**	33	48	44	29	33	37
Reduced reimbursement amounts for ransomware attacks	**29**	26	38	32	23	29	29
Other	**<1**	-	-	-	-	<1	<1
None/no changes	**16**	18	8	8	15	15	16
Don't know	**4**	3	12	20	11	7	4

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

Over six-in-ten (64%) indicate that cybersecurity measures or audit controls are more common requirements in contracts with third party vendors.

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended		
	2023	2023	2023	2023	2021	2022	2023
	500	381	87	37c	510	500	500
	%	%	%	%	%	%	%
TOTAL MORE COMMON	**64**	65	53	54	56	61	64
Much more common	**20**	19	20	27	22	24	20
A little more common	**44**	47	33	27	34	36	44
No change	**33**	33	38	43	35	35	33
A little less common	**1**	1	-	-	1	1	1
Much less common	**1**	1	1	-	-	-	1
TOTAL LESS COMMON	**1**	1	1	-	1	1	1
Don't know	**2**	1	8	3	8	3	2

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 (Added 2023: or buyers)? Would you say that such requirements are…?
Base: Total sample
C Caution, small base size

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

Most (72%) indicate their organization stores the personal information of customers, employees, suppliers, vendors or partners.

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended					
	2023	2023	2023	2023	2018	2019	2020	2021	2022	2023
	500	381	87	37c	500	502	500	510	500	500
	%	%	%	%	%	%	%	%	%	%
Yes	**72**	72	78	84	59	64	66	66	66	72
No	**24**	26	15	11	27	18	22	20	24	24
Prefer not to answer	**3**	2	3	3	10	13	9	10	7	3
Don't know	**1**	<1	3	3	5	5	3	4	3	1

Q41. Does your organization store any personal information of customers, employees, suppliers, vendors or partners?
Base: Total sample
C Caution, small base size

ESTIMATED NUMBER OF BREACHES IN LAST YEAR

Four-in ten (40%) organizations experienced a breach of customer and/or employee data last year (up from 29% in 2022).

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended				
	2023	2023	2023	2023	2019	2020	2021	2022	2023
	500	381	87	37c	502	500	510	500	500
	%	%	%	%	%	%	%	%	%
0	36	37	33	41	42	38	36	32	36
1	13	14	6	-	4	7	7	7	13
2	11	12	7	11	4	5	5	8	11
3 to 4	6	6	2	3	3	4	3	4	6
5 to 9	4	4	3	3	3	4	5	4	4
10 or more	7	6	6	8	4	5	5	5	7
Don't know	24	20	43	35	40	38	39	39	24

40%

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
C Caution, small base size

WHO WAS INFORMED ABOUT DATA BREACHES

Among organizations that experienced a data breach, over half informed management/senior leadership (63%) and the Board (52%), and 44% informed customers.

	TOTAL	TOTAL – Trended				
	2023	2019	2020	2021	2022	2023
	202	90	122	127	144	202
	%	%	%	%	%	%
Management/senior leadership	63	40	50	50	53	63
Board of Directors	52	21	34	43	49	52
Customers	44	48	44	41	44	44
Regulatory body	42	58	36	39	35	42
Law enforcement	38	37	31	29	35	38
Other	<1	-	2	2	-	<1
None of the above	1	-	2	4	1	1
Prefer not to answer	<1	2	1	2	1	<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

CYBER INCIDENT RESPONSE PLAN

Most (84%) indicate that their organization has a cyber incident response plan.

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended	
	2023	2023	2023	2023	2022	2023
	500	381	87	37c	500	500
	%	%	%	%	%	%
TOTAL YES	**84**	85	82	78	82	84
Yes, a comprehensive plan	**44**	43	45	30	37	44
Yes, a basic plan	**40**	42	37	49	45	40
No, but currently developing one	**9**	9	5	11	9	9
No plan	**5**	5	6	5	5	5
Don't know	**2**	1	8	5	4	2

Q2022-51E Does your organization have a cyber incident response plan?
Base: Total sample
C Caution, small base size

USE OF CYBER INCIDENT RESPONSE PLAN

More than 6-in-10 (64%) of organizations have used their cyber incident response plan in the last 12 months.

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended	
	2023	2023	2023	2023	2022	2023
	421	324	71	29c	411	421
	%	%	%	%	%	%
None	29	29	37	45	33	29
1-5	41	43	28	21	36	41
6-10	16	17	14	10	15	16
11-15	5	6	3	3	6	5
More than 15	2	1	6	7	2	2
Prefer not to answer	2	2	4	-	-	2
Don’t know	3	2	8	14	7	3

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

Half (49%) indicate that their organization is part of a group or partnership aimed at improving cybersecurity.

	TOTAL	PRIVATE	PUBLIC	MUSH
	2023	2023	2023	2023
	500	381	87	37c
	%	%	%	%
Yes	49	47	52	41
No	44	46	37	46
Prefer not to answer	1	1	-	-
Don’t know	6	5	11	14

Q2023-14G Is your organization part of any groups/partnerships aimed at improving cybersecurity (e.g., municipal or regional partnership, industry-threat sharing group, etc.)?
Base: Total answering
C Caution, small base size

Four-in-ten (39%) believe there are dormant threats on their organization's network.

	TOTAL	PRIVATE	PUBLIC	MUSH
	2023	2023	2023	2023
	500	381	87	37c
	%	%	%	%
Yes	39	38	39	49
No	44	45	41	35
Prefer not to answer	1	1	1	-
Don't know	16	15	18	16

Q2023-20C A dormant threat is malicious software, like a botnet, that has not yet been activated and so is not visibly disrupting your organization's IT systems. Do you believe there are dormant threats on your organization's network?
Base: Total answering
C Caution, small base size

Six-in-ten (61%) sought external help for incident response and recovery in connection to cyberattacks or incidents in the last 12 months.

	TOTAL	PRIVATE	PUBLIC	MUSH
	2023	2023	2023	2023
	205	152	37c	14c
	%	%	%	%
Yes	61	63	54	64
No	36	36	35	29
Prefer not to answer	<1	1	-	-
Don’t know	2	1	11	7

Q2023-21A Did your organization seek external help for incident response and recovery in connection to any of the cyber attacks or incidents experienced in the last 12 months?
Base: Yes at Q16A
C Caution, small base size

Most commonly, organizations sought help from a cybersecurity firm/consultancy.

	TOTAL	PRIVATE	PUBLIC	MUSH
	2023	2023	2023	2023
	126	95	20c	9c
	%	%	%	%
Cybersecurity firm/consultancy	63	65	60	44
Government agency/department (with cybersecurity expertise)	36	35	30	33
Private negotiators	34	34	35	44
Law enforcement	33	29	45	33
Data breach coach	33	34	25	44
Public relations firm/consultancy	32	35	10	11

Q2023-21B From which of the following did your organization seek help? Select all that apply.
Base: Yes at Q21A
C Caution, small base size

TIME NEEDED TO RECOVER IT SYSTEMS

Most say it took under a month to recover their organization's IT systems to pre-incident capacity, and just under half (47%) say it took less than a week.

	TOTAL	PRIVATE	PUBLIC	MUSH
	2023	2023	2023	2023
	192	143	35c	14c
	%	%	%	%
Less than 1 day	14	15	11	7
1 day to less than a week	33	36	17	21
1 week to just under a month	31	31	31	36
1 month to just under 6 months	14	11	20	29
More than 6 months	5	3	11	7
Have not recovered	1	1	-	-
Prefer not to answer	–	-	-	-
Doesn't apply/no recovery needed	2	1	6	-
Don't know	1	-	3	-

Q2023-21C About how long did it take to recover your organization's IT systems to pre-incident capacity (excluding data theft)?
Base: Yes at Q16A, excluding No impact at Q20
C Caution, small base size

Most say it took under a month to recover compromised or stolen data, and 44% say it took less than a week.

	TOTAL	PRIVATE	PUBLIC	MUSH
	2023	2023	2023	2023
	187	141	32c	14c
	%	%	%	%
Less than 1 day	12	13	13	-
1 day to less than a week	32	35	16	14
1 week to just under a month	35	38	28	29
1 month to just under 6 months	10	7	28	50
More than 6 months	7	4	13	7
Have not recovered	1	1	-	-
Prefer not to answer	–	-	-	-
Doesn't apply/no data compromised	4	4	3	-
Don't know	–	-	-	-

Q2023-21D About how long did it take to recover data that was compromised or stolen?
Base: Answer given at Q21c
C Caution, small base size

Almost 4-in-10 (38%) say their organization has made changes to its cybersecurity approaches in response to news about major cyber attacks.

	TOTAL	PRIVATE	PUBLIC	MUSH
	2023	2023	2023	2023
	500	381	87	37c
	%	%	%	%
Yes	38	37	34	35
No	53	56	44	43
Prefer not to answer	2	2	7	5
Don't know	7	6	15	16

Q2023-51G Has your organization made any changes to its cybersecurity approaches in response to news about major cyber attacks on organizations such as Indigo, SickKids, and Empire Company?
Base: Total answering
C Caution, small base size

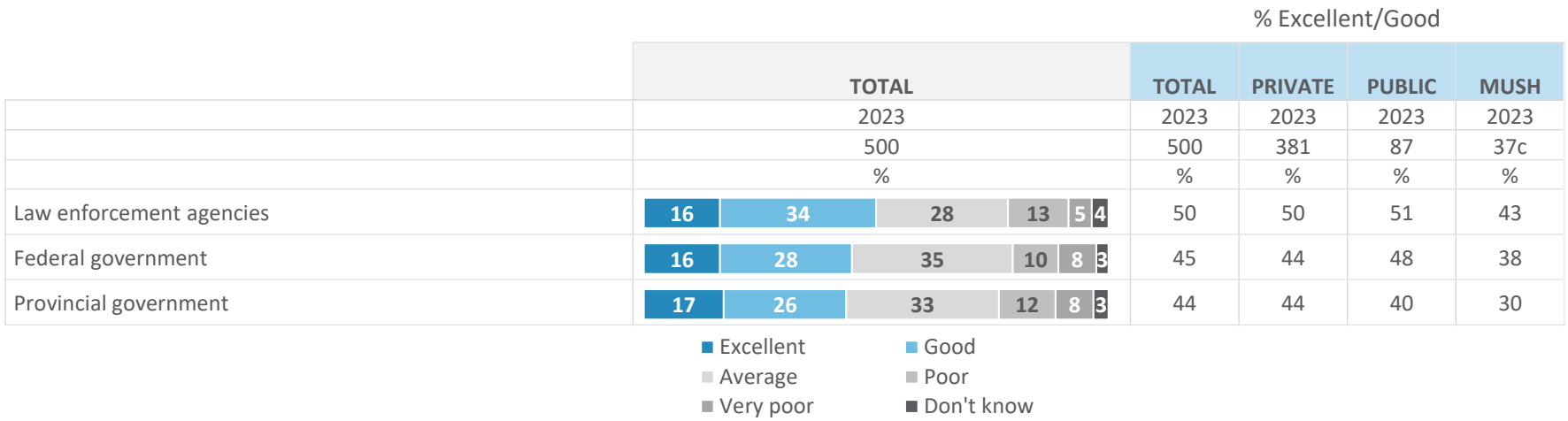
Organizations are most likely to perceive profit-motivated cyber criminals as the biggest potential threat.

	TOTAL	PRIVATE	PUBLIC	MUSH
	2023	2023	2023	2023
	500	381	87	37c
	%	%	%	%
Cyber criminals motivated by profit	63	66	54	65
Foreign state actors (e.g., Russia, China, North Korea, etc.)	33	32	39	35
Hacktivists	28	29	22	22
Insider threats	28	27	28	22
Cyber criminals motivated by nationalist beliefs	27	26	28	19
Other	1	<1	3	3
Don't know	4	3	8	8
Prefer not to answer	1	1	-	-

Q2023-51H In general, which of the following would you say pose the biggest potential cyber threat to your organization?
Base: Total answering
C Caution, small base size

RATING OF SUPPORT FROM LAW ENFORCEMENT AND GOVERNMENT

Half or slightly fewer rate the level of support from law enforcement agencies, federal government and provincial government as excellent or good for organizations taking actions to prepare against cyberthreats. Comparatively, about 2-in-10 rate the support from each as poor.



Q2023-51P How would you rate the level of support from each of the following for organizations taking actions to prepare against cyber threats?
Base: Total answering
C Caution, small base size

There is broad support for the objectives of Bill C-26.

	TOTAL	PRIVATE	PUBLIC	MUSH
	2023	2023	2023	2023
	500	381	87	37c
	%	%	%	%
TOTAL SUPPORT	**78**	77	82	86
Strongly support	**36**	34	45	43
Somewhat support	**42**	43	37	43
Neutral	**17**	18	13	8
Somewhat oppose	**1**	1	1	3
Strongly oppose	**2**	2	1	-
TOTAL OPPOSE	**3**	3	2	3
Don't know	**2**	2	3	3

Q2023-51Q In 2022, the federal government introduced Bill C-26, An Act Respecting Cybersecurity. This Bill aims to increase baseline levels of cybersecurity in the following critical infrastructure sectors: telecommunications, finance, energy, and transportation. Operators in these sectors will be required to establish protocols to prevent cyber incidents and increase reporting of incidents. To what extent do you support or oppose the objectives of Bill C-26?

Base: Total answering

C Caution, small base size

4

GENERATIVE AI

Almost 7-in-10 (68%) are worried about potential cyber threats from generative AI.

	TOTAL	PRIVATE	PUBLIC	MUSH
	2023	2023	2023	2023
	500	381	87	37c
	%	%	%	%
TOTAL WORRIED	**68**	67	74	78
Very worried	**15**	15	9	16
Somewhat worried	**53**	51	64	62
Not very worried	**26**	29	18	22
Not at all worried	**5**	4	6	-
TOTAL NOT WORRIED	**31**	33	24	22
Don't know	**1**	1	2	-

Q2023-51J How worried are you about potential cyber threats to your organization from generative artificial intelligence (e.g., ChatGPT)?
Base: Total answering
C Caution, small base size

Organizations are most concerned about data gathered by AI tools and improved phishing emails and texts.

	TOTAL	PRIVATE	PUBLIC	MUSH
	2023	2023	2023	2023
	341	255	64	29c
	%	%	%	%
Data gathered by AI tools	61	61	58	55
Improved phishing emails and texts	58	60	56	62
Deepfake images and videos	40	40	34	31
Deepfake voices	33	35	27	28
Other	<1	-	-	-
Don't know	3	3	3	-

Q2023-51K Which of the following types of generative AI threats are you most concerned about?
Base: Worried at Q51J
C Caution, small base size

POTENTIAL NEGATIVE IMPACTS OF MOST CONCERN

Among those worried about generative AI threats, privacy breaches, AI-powered cyber attacks, and data poisoning tend to be of greatest concern.

	TOTAL	PRIVATE	PUBLIC	MUSH
	2023	2023	2023	2023
	341	255	64	29c
	%	%	%	%
Privacy breaches	54	53	52	55
AI-powered cyber attacks	52	50	58	62
Data poisoning (i.e., manipulating training data to introduce biases or malicious patterns	46	44	50	48
Dependence on AI for security	35	37	22	21
Lack of transparency and explainability	34	35	34	28
Other	<1	-	2	-
Don't know	2	2	2	-

Q2023-51L Which of the following potential negative impacts of generative AI on your organization are you most concerned about? Select up to 3.
Base: Worried at Q51J
C Caution, small base size

Over 4-in-10 (44%) say their organization has integrated AI tools into its workflows and operations.

	TOTAL	PRIVATE	PUBLIC	MUSH
	2023	2023	2023	2023
	500	381	87	37c
	%	%	%	%
Yes	44	46	32	22
No	50	50	52	62
Prefer not to answer	2	2	3	5
Don’t know	4	2	13	11

Q2023-51M Has your organization integrated AI tools into its workflows and operations?
Base: Total answering
C Caution, small base size

Among those who have not integrated AI tools, 4-in-10 (39%) indicate that their organization is planning to.

	TOTAL	PRIVATE	PUBLIC	MUSH
	2023	2023	2023	2023
	249	189	45c	23c
	%	%	%	%
Yes	39	37	47	52
No	45	47	40	35
Prefer not to answer	1	1	2	-
Don’t know	16	16	11	13

Q2023-51N Is your organization planning to integrate AI tools into its workflows and operations?
Base: No at Q51M
C Caution, small base size

Just over 3-in-10 (32%) say their organization has an AI policy.

	TOTAL	PRIVATE	PUBLIC	MUSH
	2023	2023	2023	2023
	500	381	87	37c
	%	%	%	%
Yes	32	33	24	22
No, but currently developing one	41	42	36	41
No plan	22	22	25	30
Prefer not to answer	1	1	3	-
Don't know	3	2	11	8

Q2023-51O Does your organization have an AI policy?
Base: Total answering
C Caution, small base size

5

SAMPLE CHARACTERISTICS

Sample Characteristics

AGE

Total sample n=500	%
18-29	12
30-39	39
40-49	27
50-59	16
60 or older	7

PROVINCE OR TERRITORY

Total sample n=500	%
Newfoundland	1
Prince Edward Island	1
Nova Scotia	1
New Brunswick	2
Quebec	12
Ontario	50
Manitoba	3
Saskatchewan	1
Alberta	11
British Columbia	18

REGION

Total sample n=500	%
Atlantic	5
Quebec	12
Ontario	50
West	33

GENDER

Total sample n=500	%
Male	74
Female	26
Non-binary	<1
Prefer not to answer	<1

EMPLOYEE OR SELF-EMPLOYED

Total sample n=500	%
Employee/Contractor working for a single organization	94
A business owner	6

TYPE OF ORGANIZATION

Employees n=468	%
Private sector	81
Public/Not-for-profit sector	19

PUBLIC SECTOR ORGANIZATION

Public sector n=87	%
Municipal government or agency	8
Provincial government or agency	14
Federal government or agency	29
Hospital or other health care organization	9
Primary or secondary school	3
College or university	22
Public utility	5
Charity	1
Non-profit	6
Other	3
MUSH	43

COUNTRY IN WHICH ORG OPERATES

Total sample n=500	%
In Canada only	69
In countries outside of Canada	7
Both	24

Sample Characteristics

ANNUAL REVENUE

Private organization n=381	%
Under $1M	2
$1M to just under $10M	17
$10M to just under $25M	21
$25M to just under $100M	22
$100M to just under $250M	20
$250M or more	14
Prefer not to answer	2
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	12
6-10	23
11-20	23
More than 20 years	38
Prefer not to answer	<1

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

Total sample n=500	%
50-99	23
100-249	27
250-499	16
500-999	23
1000 or more (public sector only)	10

FAMILIARITY WITH ORGANIZATION'S COMPUTER SYSTEMS/IT FUNCTIONS

Total sample n=500	%
Very familiar	69
Somewhat familiar	31

IT AREAS INCLUDED WITHIN JOB

Employees n=500	%
System administration	57
Desktop IT	56
Cybersecurity	70
Networking	60
Other technical	26
Non-technical decision-making	36
Other non-technical areas (e.g., HR, finance, admin, etc.)	21
Risk evaluation	31