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 2021

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.
- 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=510 cybersecurity decision-makers (employees or owners) completed a 12-minute online survey in July-August, 2021. 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 2021 findings are compared to the results from 2019 and 2020.

2

RESOURCES AND TRAINING

INCIDENCE OF CONDUCTING CYBERSECURITY AWARENESS TRAINING

Most organizations (93%) conduct cybersecurity awareness training, and it is mandatory for 43% of employees.

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended		
	2021	2021	2021	2021	2019	2020	2021
	510	287	181	80	502	500	510
	%	%	%	%	%	%	%
TOTAL YES	93	93	93	91	87	94	93
Yes, mandatory training for some employees	41	47	30	28	32	34	41
Yes, mandatory training for all employees	43	42	46	40	41	48	43
Yes, optional training (some or all employees)	9	4	16	24	15	12	9
No	7	7	7	9	11	6	7
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 create training material and promote it internally (61%, up from 54% in 2019). More than 4-in-10 (44%) indicate that they conduct phishing simulations.

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended		
	2021	2021	2021	2021	2019	2020	2021
	474	267	168	73	439	467	474
	%	%	%	%	%	%	%
We create training material and promote it internally	61	57	71	63	54	57	61
We conduct phishing simulations*	44	41	51	44	21	37	44
Lunch-and-learns/workshops	39	38	39	37	36	35	39
We license/provide access to a library of courses	38	37	44	41	-	31	38
We hire a third-party to conduct seminar-style training programs	35	37	29	38	32	31	35
Other	2	1	2	3	2	1	2
Don't know	<1	<1	-	-	1	<1	<1

Q7. In what ways does your organization conduct cybersecurity awareness training? Select all that apply.
Base: Have cyber security training at Q6
C Caution, small base size
* Previous phrasing: "We conduct standalone phishing simulations"

FREQUENCY OF CONDUCTING CYBERSECURITY AWARENESS TRAINING

Most organizations do not conduct cybersecurity awareness training on a frequent basis (41% annually or less – unchanged from 2019).

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended		
	2021	2021	2021	2021	2019	2020	2021
	474	267	168	73	439	467	474
	%	%	%	%	%	%	%
Annually or less	41	39	43	45	40	40	41
Quarterly	46	49	40	40	36	49	46
Monthly	11	10	12	11	12	9	11
More than monthly/ongoing	--	-	-	-	10	-	-
Don't know	2	1	5	4	2	1	2

Q8. About how often does your organization conduct cybersecurity awareness training?
Base: Have 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 is monitoring results and risk scores over time. Mentions of reduced costs and saved time remain higher than in 2019.

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended		
	2021	2021	2021	2021	2019	2020	2021
	474	267	168	73	439	467	474
	%	%	%	%	%	%	%
Monitoring training results and risk scores over time	53	52	55	42	46	46	53
Conducting end-user perception/knowledge assessments	48	46	55	56	42	38	48
Reduced costs on security incidents	44	44	43	41	25	42	44
Saved time on security incidents	42	42	43	41	27	42	42
Comparing training results to industry peers	37	38	38	34	33	25	37
Other	1	1	2	3	1	1	1
None/no ability to measure the impact/don't know	7	4	9	14	11	9	7

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

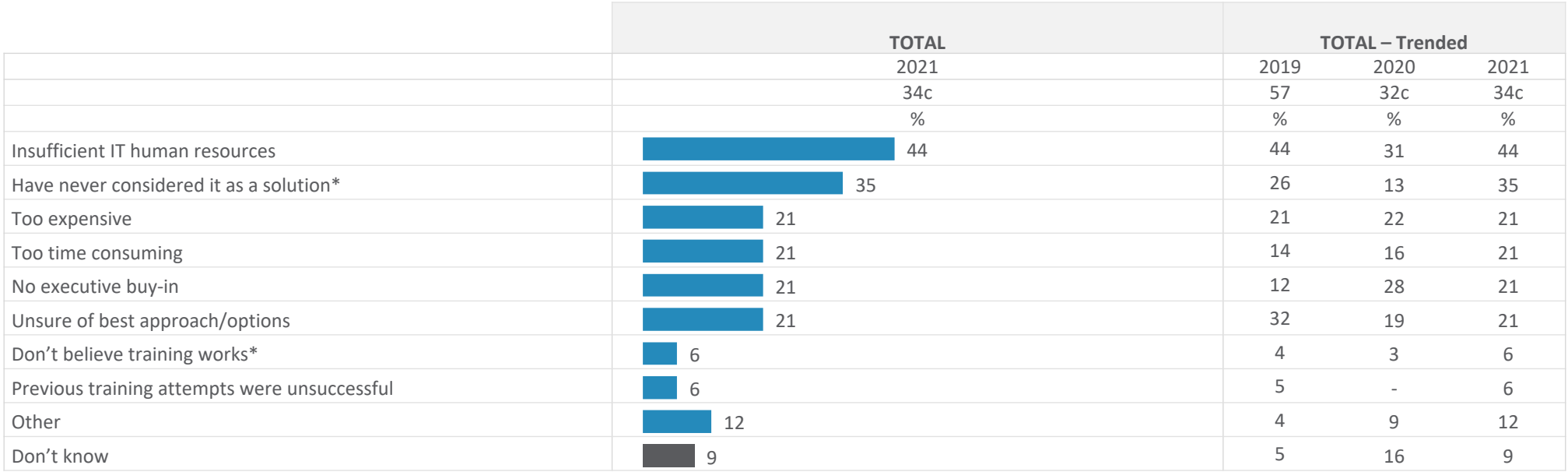
Most continue to indicate that end-user training is effective in reducing incidents and/or risky online behavior.

	TOTAL	TOTAL – Trended		
	2021	2019	2020	2021
	474	439	467	474
	%	%	%	%
TOTAL EFFECTIVE	95	92	93	95
Very effective	32	35	32	32
Somewhat effective	63	57	61	63
Not very effective	4	6	6	4
Not effective at all	<1	<1	<1	<1
TOTAL NOT EFFECTIVE	4	6	6	4
Don't know	1	2	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 few organizations that don't conduct training tend to cite insufficient resources as the main reason (44%). Never considering it as a solution is also a top mention in 2021 (35%).



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

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

Risk advisory/recommendations, high-quality training courses and phishing simulations are most likely to be rated as critically important features when considering a training platform.

	TOTAL	% IMPORTANT		
	2021	2019	2020	2021
	510	502	500	510
	%	%	%	%
Risk advisory and recommendations	45 / 44 / 8 / 2 / 2	91	87	89
Modern, high-quality training courses	45 / 43 / 9 / 1 / 2	87	86	88
Automated phishing simulations	40 / 45 / 12 / 2 / 2	83	84	84
Pre-built training curriculum	32 / 51 / 12 / 3 / 3	84	81	82
End-to-end reporting	35 / 46 / 14 / 2 / 4	84	82	80
End-user-facing risk scores and dashboards	31 / 49 / 14 / 3 / 3	84	81	80
Off-the-shelf deployment	28 / 51 / 16 / 2 / 4	74	76	79

Q12. How important is each of the following features when considering software for delivering computer-based 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

TRAINING TOPICS

Training on both working remotely and using video conferencing software securely is common. Training on COVID-19 related cyber threats is less common, but still provided by more than half of organizations.

% Yes

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended	
	2021	2021	2021	2021	2020	2021
	510	287	181	80	500	510
	%	%	%	%	%	%
Working remotely securely	80	78	83	79	78	80
Using video conferencing software securely (e.g., Zoom)	79	78	80	80	74	79
COVID-19 related cyber threats	57	59	57	54	56	57

Q13A. Does your organization provide training on the following topics?
Base: Total sample

3

CYBERSECURITY: EXPERIENCE AND RESPONSE

INCIDENCE OF USING A CLOUD DNS FIREWALL

73% of organizations currently have a cloud DNS firewall, up from 42% in 2018 and up from 62% from 2020.

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended			
	2021	2021	2021	2021	2018	2019	2020	2021
	510	287	181	80	500	502	500	510
	%	%	%	%	%	%	%	%
Yes	73	71	78	79	42	63	62	73
No	17	21	10	11	23	14	19	17
Prefer not to answer	2	1	4	4	2	5	3	2
Don't know	7	7	8	6	32	18	15	7

Q15. 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?

Base: Total sample

ESTIMATED NUMBER OF CYBER ATTACKS IN THE LAST YEAR

2-in-10 (21%) organizations believe they didn't face any cyber attacks last year, and just 2-in-10 (19%) say they faced more than 10.

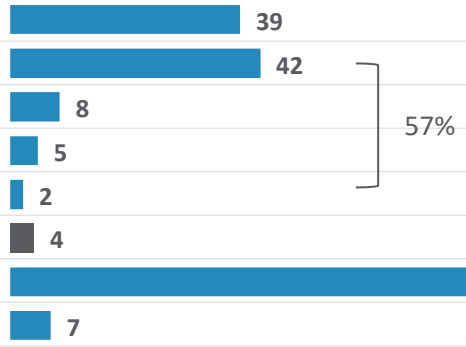
	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended	
	2021	2021	2021	2021	2020	2021
	510	287	181	80	500	510
	%	%	%	%	%	%
None	21	27	11	14	20	21
1-5	27	28	23	21	29	27
6-10	17	20	13	13	13	17
11-25	6	6	5	3	9	6
More than 25	13	9	22	15	12	13
Don't know	16	10	27	35	17	16
10 OR FEWER	65	75	47	48	62	65
MORE THAN 10	19	15	27	18	21	19

Q16. Approximately how many cyber attacks did your organization face last year?
Base: Total sample

ESTIMATED NUMBER OF ATTACKS THAT IMPACTED ORGANIZATION

Among those that faced attacks, 57% indicate that the attacks had a negative impact on their organization.

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended	
	2021	2021	2021	2021	2020	2021
	323	180	113	41	315	323
	%	%	%	%	%	%
None	39	39	31	34	43	39
1-5	42	43	44	46	40	42
6-10	8	9	9	5	7	8
11-25	5	4	6	-	3	5
More than 25	2	2	3	5	2	2
Don't know	4	3	7	10	5	4
10 OR FEWER	89	92	84	85	91	89
MORE THAN 10	7	6	9	5	4	7



Q17. Approximately how many of those cyber attacks had a negative impact on your organization (e.g., financial, time or data losses, etc.)?
Base: Organizations that experienced attacks

ESTIMATED PROPORTION OF ATTACKS THAT IMPACTED NETWORK INFRASTRUCTURE AND DATABASES

Successful attacks are likely to affect network infrastructure and databases.

Network infrastructure and databases

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended	
	2021	2021	2021	2021	2020	2021
	185	104	70	23	162	185
	%	%	%	%	%	%
None	12	8	19	17	14	12
Few (1%-10%)	25	21	33	43	27	25
Some (11%-49%)	21	24	11	17	25	21
Many (50% - 99%)	30	35	27	13	22	30
All	9	11	7	4	9	9
Don’t know	2	2	3	4	2	2

Q18. Approximately what proportion of the successful cyber attacks impacted the following services?
Base: Organizations that experienced successful attacks

Successful attacks are also likely to affect desktops and individual devices.

Desktops and Individual Devices

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended	
	2021	2021	2021	2021	2020	2021
	185	104	70	23	162	185
	%	%	%	%	%	%
None	5	2	9	9	6	5
Few (1%-10%)	24	23	24	22	31	24
Some (11%-49%)	27	25	30	35	27	27
Many (50% - 99%)	31	38	23	26	21	31
All	10	10	11	4	14	10
Don’t know	2	2	3	4	1	2

Q18. Approximately what proportion of the successful cyber attacks impacted the following services?
Base: Total sample

PROPORTION OF ATTACKS THAT IMPACTED USER OR CUSTOMER DATA

Successful attacks are less likely to affect user or customer data.

User/Customer Data

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended	
	2021	2021	2021	2021	2020	2021
	185	104	70	23	162	185
	%	%	%	%	%	%
None	14	13	16	9	20	14
Few (1%-10%)	28	22	31	30	27	28
Some (11%-49%)	23	26	21	39	25	23
Many (50% - 99%)	21	26	16	9	19	21
All	12	11	13	9	7	12
Don't know	3	3	3	4	1	3

Q18. Approximately what proportion of the successful cyber attacks impacted the following services?
Base: Total sample

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

The most common impacts of cyberattacks are: tying up employees' time and/or preventing them from working. Mentions of reputational damage are up over time (19% in 2021, up from 6% in 2018).

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

17% indicate that their organization has been a victim of a successful ransomware attack in the last 12 months.

	TOTAL	PRIVATE	PUBLIC	MUSH
	2021	2021	2021	2021
	510	287	181	80
	%	%	%	%
Yes	17	21	14	13
No	75	75	70	74
Don't know	8	4	16	14

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, 59% indicate that data was exfiltrated.

	TOTAL	PRIVATE	PUBLIC	MUSH
	2021	2021	2021	2021
	87	60	25c	10
	%	%	%	%
Yes	 59	63	52	Base size too small to report.
No	 36	33	36	
Don't know	 6	3	12	

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
C Caution, small base size

INCIDENCE OF PAYING RANSOM DEMANDS

Among those that experienced a ransomware attack, 69% indicate that the organization paid ransom demands.

	TOTAL	PRIVATE	PUBLIC	MUSH
	2021	2021	2021	2021
	87	60	25c	10
	%	%	%	%
Yes	 69	75	52	Base size too small to report.
No	 26	23	36	
Don't know	 5	2	12	

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
C Caution, small base size

AMOUNT OF RANSOM PAID

Many (40%) don’t know how much ransom was paid. Among those who provide an estimate, amounts vary widely and no single category dominates.

	TOTAL	PRIVATE	PUBLIC	MUSH
	2021	2021	2021	2021
	60	45	13	4
	%	%	%	%
Less than $100	15	13	Base size too small to report.	
$100-$2,000	13	11		
$2,001-$25,000	17	18		
More than $25,000	15	16		
Don't know	40	42		

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

WAYS IN WHICH ORGANIZATION WAS DAMAGED BY RANSOMWARE ATTACK

One-quarter or more of organizations that suffered a ransomware attack were damaged in terms of recovery costs, loss of revenue and/or customers, or reputational damage.

	TOTAL	PRIVATE	PUBLIC	MUSH
	2021	2021	2021	2021
	87	60	25c	10
	%	%	%	%
Recovery costs/fees	32	32	36	Base size too small to report.
Loss of revenue	30	32	24	
Loss of customers	30	35	20	
Providing customer support and communication	30	30	32	
Need for external consulting	30	28	32	
Reputational damage	26	25	28	
Ransomware payment	25	30	12	
Other	2	2	4	
No answer	5	3	8	

Q20E. In which of the following ways was your organization damaged most by the ransomware attack?
Base: Organization has been the victim of a ransomware attack in the last 12 months
C Caution, small base size

SUPPORT FOR LEGISLATION THAT PROHIBITS RANSOM PAYMENTS

Almost two-thirds (64%) support legislation that would prohibit ransom payments.

	TOTAL	PRIVATE	PUBLIC	MUSH
	2021	2021	2021	2021
	510	287	181	80
	%	%	%	%
TOTAL SUPPORT	**64**	62	69	74
Strongly support	**38**	38	39	43
Somewhat support	**26**	24	30	31
Neither	**22**	24	18	11
Somewhat oppose	**5**	6	3	4
Strongly oppose	**3**	2	2	4
TOTAL OPPOSE	**7**	8	6	8
Don't know	**6**	6	8	8

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

ACTIONS TAKEN TO PREVENT FUTURE CYBER ATTACKS

The most common measures taken to prevent future cyberattacks include employee training, security audits and installation of new software. The likelihood of taking action has increased over time for all measures.

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended			
	2021	2021	2021	2021	2018	2019	2020	2021
	510	287	181	80	194	502	500	510
	%	%	%	%	%	%	%	%
Employee training	63	63	67	70	40	57	61	63
Security audit	54	51	59	61	30	48	45	54
Installation of new software	52	48	56	51	45	46	47	52
Addition of new cloud-based security	45	44	48	46	21	29	31	45
Installation of new hardware	36	30	45	49	27	31	32	36
Hiring of new IT staff	27	23	35	29	12	24	24	27
Hiring of new IT contractor or service providers	27	23	30	26	16	21	22	27
Other	1	1	1	1	2	1	1	1
No actions taken	2	2	3	4	9	3	4	2
No answer	2	1	3	-	3	4	4	2

Q21. Which of the following actions, if any, has your organization taken to prevent future cyberattacks?
Base: Among those who say their organization has experienced a cyberattack in the last 12 months

LEVEL OF CONCERN ABOUT DAMAGE FROM FUTURE CYBER ATTACKS

There continues to be growing concern about possible damage from future cyber attacks.

	TOTAL	TOTAL – Trended		
	2021	2019	2020	2021
	510	502	500	510
	%	%	%	%
TOTAL MORE CONCERNED	61	56	54	61
Much more concerned	24	23	18	24
Somewhat more concerned	37	34	36	37
About the same	35	35	40	35
Somewhat less concerned	3	5	4	3
Much less concerned	1	1	<1	1
TOTAL LESS CONCERNED	4	6	4	4
Don't know	1	2	2	1

Q22. Compared to the last year, are you more concerned or less concerned about possible damage from cyber attacks against your organization in the next year?
Base: Total sample

A range of reasons are mentioned for devoting resources to cybersecurity measures.

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended			
	2021	2021	2021	2021	2018	2019	2020	2021
	510	287	181	80	500	502	500	510
	%	%	%	%	%	%	%	%
To secure continuity of operations	57	52	62	65	49	59	52	57
To protect personal information of employees, suppliers or partners	55	49	64	60	53	56	52	55
To prevent fraud and theft	55	54	55	58	53	56	55	55
To protect personal information of customers	55	54	58	60	55	59	52	55
To protect the reputation of the organization	53	47	61	58	43	53	53	53
To prevent downtime and outages of website or e-commerce	49	47	50	51	44	46	45	49
To comply with laws, regulations or contracts	44	40	51	51	34	43	40	44
To protect trade secrets and intellectual property	41	42	36	30	29	40	38	41
Our organization has suffered a cybersecurity incidence previously	16	14	19	19	10	20	19	16
Other	<1	1	-	-	<1	<1	<1	<1
We don’t devote any resources to cybersecurity measures	1	1	2	3	4	2	<1	1
Don’t know	2	1	3	3	4	2	2	2

Q23. What are the main reasons that your organization devotes resources to cybersecurity measures? Select all that apply.
Base: Total sample

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

More than 4-in10 (43%) anticipate an increase in human resources devoted to cybersecurity in the next 12 months (up from 2020 but on par with 2019).

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended			
	2021	2021	2021	2021	2018	2019	2020	2021
	510	287	181	80	500	502	500	510
	%	%	%	%	%	%	%	%
Decrease	7	9	6	5	3	5	9	7
Stay the same	44	45	39	41	66	45	53	44
Increase	43	42	47	45	28	45	34	43
Don't know	5	4	9	9	4	5	4	5

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

More than 4-in-10 (47%) anticipate that the amount of financial resources devoted to cybersecurity will increase in the next 12 months.

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended			
	2021	2021	2021	2021	2018	2019	2020	2021
	510	287	181	80	500	502	500	510
	%	%	%	%	%	%	%	%
Decrease	10	12	7	6	3	6	10	10
Stay the same	40	40	37	41	60	35	44	40
Increase	47	45	51	48	30	54	43	47
Don't know	3	3	5	5	6	5	3	3

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

CYBERSECURITY RISKS/THREATS THAT COULD HAVE GREATEST NEGATIVE IMPACT

Malicious software, scams/frauds, and unauthorized access are the top perceived threats in 2021.

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended			
	2021	2021	2021	2021	2018	2019	2020	2021
	510	287	181	80	500	502	500	510
	%	%	%	%	%	%	%	%
Malicious software	60	58	61	61	61	57	57	60
Scams and fraud	51	47	60	68	44	49	55	51
Unauthorized access, manipulation, or theft of data	50	45	56	56	56	55	55	50
Identity theft	44	41	46	50	41	40	42	44
Denial of service	39	39	40	39	23	34	33	39
Theft or compromise of software or hardware	37	40	33	26	30	33	30	37
Disruption or defacing of web presence	30	33	28	23	28	32	30	30
Other	<1	<1	1	-	<1	<1	-	<1
None of the above	2	3	1	1	3	2	2	2
Don’t know	3	2	4	4	4	4	3	3

Q26. 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

ACTIVITIES UNDERTAKEN TO IDENTIFY CYBERSECURITY RISKS

The most common activity undertaken to identify cybersecurity risks is monitoring of the firewall. Organizations are increasingly likely to undertake formal risk assessments (47% in 2021, up from 38% in 2020).

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended			
	2021	2021	2021	2021	2018	2019	2020	2021
	510	287	181	80	500	502	500	510
	%	%	%	%	%	%	%	%
Monitoring firewall	58	54	62	59	61	63	64	58
Formal risk assessment of cyber security practices	47	46	46	35	29	39	38	47
Monitoring employees' use of computers and the internet	46	47	41	35	41	48	44	46
Security framework/certification	42	44	40	33	-	35	30	42
Penetration testing	40	37	46	43	23	39	41	40
Complete external audit of IT systems	38	36	36	33	24	40	35	38
Use of a SIEM	24	23	26	20	-	21	18	24
Other	1	<1	2	1	-	-	<1	1
None	2	2	1	3	8	1	2	2
Prefer not to answer	3	3	5	5	4	4	4	3
Don't know	3	2	6	8	10	5	4	3

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

Just over half (53%) of organizations maintain a formal patching policy.

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended			
	2021	2021	2021	2021	2018	2019	2020	2021
	510	287	181	80	500	502	500	510
	%	%	%	%	%	%	%	%
Yes	53	52	60	49	29	56	49	53
No	25	29	17	23	36	19	24	25
Prefer not to answer	9	8	8	10	8	11	11	9
Don’t know	13	11	15	19	27	14	16	13

Q31. Does your organization maintain a formal patching policy?
Base: Total sample

CYBERSECURITY INSURANCE COVERAGE

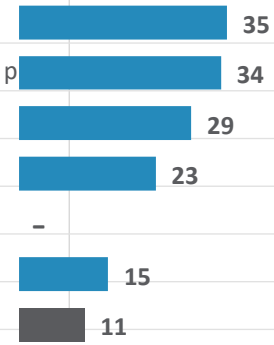
Six-in-ten (59%) of organizations have cybersecurity insurance coverage. Three-in-ten (29%) have a cybersecurity-specific policy.

	TOTAL	PRIVATE	PUBLIC	MUSH
	2021	2021	2021	2021
	510	287	181	80
	%	%	%	%
Yes, a cybersecurity-specific policy	29	31	26	21
Yes, as part of a business insurance policy	30	36	19	21
No	17	15	17	18
Prefer not to answer	7	6	8	9
Don’t know	18	13	30	31

Q31A. 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 increased premiums and proof/verification of security measures in place.



	TOTAL	PRIVATE	PUBLIC	MUSH
	2021	2021	2021	2021
	300	191	82	34
	%	%	%	%
Increased premiums	35	36	37	35
Requested new forms of proof/verification of cybersecurity measures in p	34	37	28	21
Changed eligibility criteria for obtaining/renewing coverage	29	30	27	21
Reduced reimbursement amounts for ransomware attacks	23	25	23	29
Other	–	-	-	-
None/no changes	15	14	15	6
Don’t know	11	8	20	29

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

CHANGE IN MEASURES/AUDIT CONTROL WITH THIRD PARTY VENDORS

Over half (56%) indicate that cybersecurity measures or audit controls are more common requirements in contracts with third party vendors.

	TOTAL	PRIVATE	PUBLIC	MUSH
	2021	2021	2021	2021
	510	287	181	80
	%	%	%	%
TOTAL MORE COMMON	**56**	61	52	49
Much more common	**22**	22	23	21
A little more common	**34**	38	29	28
No change	**35**	33	33	35
A little less common	**1**	2	-	-
Much less common	**–**	-	-	-
TOTAL LESS COMMON	**1**	2	-	-
Don't know	**8**	4	15	16

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

LEVEL OF FAMILIARITY WITH CANADA'S PERSONAL INFORMATION PROTECTION OF ELECTRONIC DOCUMENTS ACT (PIPEDA)

About two-thirds (65%) are familiar with PIPEDA (relatively unchanged over time).

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended			
	2021	2021	2021	2021	2018	2019	2020	2021
	510	287	181	80	500	502	500	510
	%	%	%	%	%	%	%	%
TOTAL FAMILIAR	**65**	66	69	66	58	69	69	65
Very familiar	**18**	18	21	25	17	26	19	18
Somewhat familiar	**47**	48	48	41	41	43	50	47
Not very familiar	**21**	21	17	13	22	18	19	21
Not familiar at all	**10**	10	10	14	16	9	8	10
TOTAL NOT FAMILIAR	**31**	31	27	26	38	26	27	31
Don't know	**4**	3	5	8	4	5	4	4

Q38. How familiar are you Canada's Personal Information Protection of Electronic Documents Act (PIPEDA)?
Base: Total sample

AWARENESS THAT CHANGES TO PIPEDA WILL REQUIRE DISCLOSURE OF DATA BREACHES

More than half (59%) are aware that PIPEDA requires commercial organizations to disclose data breaches.

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended			
	2021	2021	2021	2021	2018	2019	2020	2021
	510	287	181	80	500	502	500	510
	%	%	%	%	%	%	%	%
Yes	59	61	57	51	42	57	59	59
No	29	26	29	31	41	29	30	29
Prefer not to answer	4	4	3	4	5	5	3	4
Don't know	9	8	11	14	12	10	8	9

Q39. Are you aware that changes to PIPEDA in 2019 now require commercial organizations to disclose data breaches to affected individuals and the federal government 'in a timely manner'? (Previous phrasing) Are you aware that recent (previous phrasing: upcoming) changes to PIPEDA now (previous phrasing: will) require commercial organizations to disclose data breaches to affected individuals and the federal government 'in a timely manner'?

Base: Total sample

LEVEL OF CONCERN ABOUT PIPEDA CHANGES AND/OR IMPACT ON ORGANIZATION

Decision-makers are divided in their level of concern about the changes to PIPEDA, but are more likely than not to be concerned.

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended			
	2021	2021	2021	2021	2018	2019	2020	2021
	510	287	181	80	500	502	500	510
	%	%	%	%	%	%	%	%
TOTAL CONCERNED	**53**	57	46	44	38	53	54	53
Very concerned	**12**	13	9	9	8	14	14	12
Somewhat concerned	**41**	45	36	35	30	39	40	41
Not very concerned	**31**	30	31	35	36	27	31	31
Not concerned at all	**7**	6	10	5	10	8	10	7
TOTAL NOT CONCERNED	**38**	36	41	40	46	35	40	38
Don't know	**8**	6	13	16	16	12	6	8

Q40. How concerned are you about the potential impact of these changes to PIPEDA on your organization? (Previous phrasing) How concerned are you about the recent (previous phrasing: upcoming) changes to PIPEDA and/or the potential impact of these changes on your organization?

Base: Total sample

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

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

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended			
	2021	2021	2021	2021	2018	2019	2020	2021
	510	287	181	80	500	502	500	510
	%	%	%	%	%	%	%	%
Yes	**66**	64	71	74	59	64	66	66
No	**20**	23	12	9	27	18	22	20
Prefer not to answer	**10**	9	12	13	10	13	9	10
Don't know	**4**	3	5	5	5	5	3	4

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

One-quarter of organizations experienced a breach of customer and/or employee data last year.

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended		
	2021	2021	2021	2021	2019	2020	2021
	510	287	181	80	502	500	510
	%	%	%	%	%	%	%
0	36	38	30	28	42	38	36
1	7	7	6	8	4	7	7
2	5	6	3	3	4	5	5
3 to 4	3	5	1	-	3	4	3
5 to 9	5	6	4	1	3	4	5
10 or more	5	5	6	3	4	5	5
Don't know	39	33	50	59	40	38	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, half informed management/senior leadership, 43% informed the Board, and 41% informed customers.

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

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 (74%) have a formal data retention policy. More than 4-in-10 say they use a mobile app and/or have made policy or process changes in how data is handled.

% Yes

	TOTAL	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended	
	2021	2021	2021	2021	2021	2020	2021
	510	510	287	181	80	500	510
	%	%	%	%	%	%	%
Formal data retention policy	74 / 19 / 8	74	72	79	74	70	74
Use a mobile app for customers/suppliers/partners	44 / 51 / 6	44	48	38	33	44	44
Have made policy/process changes re: handling customer data	42 / 39 / 20	42	44	40	35	43	42

Q41C. 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. User location and device identifiers are also commonly tracked. Organizations are less likely than in 2020 to indicate that clipboard data is tracked.

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended	
	2021	2021	2021	2021	2020	2021
	222	138	69	26	219	222
	%	%	%	%	%	%
Contact information (email or phone number)	56	55	59	50	51	56
User location (GPS or other methods)	46	44	48	42	42	46
Device identifiers (UDID or IMEI)	43	43	42	23	39	43
Clipboard data	23	23	22	19	34	23
Other	–	-	-	-	1	-
None of the above	6	7	6	8	5	6
Don't know	6	4	10	19	7	6

Q41F. What does the mobile app track?
Base: Total sample

4

COVID-19

Seven-in-ten (69%) say they were required to work from home as a result of COVID-19.

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended	
	2021	2021	2021	2021	2020	2021
	510	287	181	80	500	510
	%	%	%	%	%	%
Yes	**69**	66	76	73	66	69
No, I was already working from home some or all of the time	**15**	16	13	9	16	15
No, my job cannot be performed remotely	**15**	17	9	16	16	15
No answer	**1**	1	2	3	2	1

Q49. Were you required to work from home as a result of the COVID-19 pandemic?
Base: Total sample

SOURCE OF DEVICES FOR WORKING FROM HOME

Seven-in-ten (71%) are working on employer-provided devices at home.

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended	
	2021	2021	2021	2021	2020	2021
	428	236	161	65	408	428
	%	%	%	%	%	%
Employer-provided devices	**71**	72	73	68	65	71
Personal devices	**12**	14	11	9	17	12
Both	**16**	14	16	23	16	16
No answer	**1**	1	-	-	1	1

Q50. Are you using employer-provided or personal devices to work from home during the COVID-19 pandemic?
Base: Those who work from home

OTHERS IN ORGANIZATION REQUIRED TO WORK AT HOME

Half (52%) of those not working at home indicate that others in their organization were required to as a result of the pandemic.

	TOTAL	PRIVATE	PUBLIC	MUSH
	2021	2021	2021	2021
	82	51	20	15
	%	%	%	%
Yes	**52**	51	60	53
No	**40**	43	25	33
Don't know	**7**	6	15	13

Q50A. Were other people in your organization required to work from home as a result of the COVID-19 pandemic?
Base: Among those not working at home

WAYS IN WHICH ORGANIZATION EQUIPS EMPLOYEES TO WORK FROM HOME

Most organizations provide tools and/or financial supports for employees working from home. The most common supports are tools – portable (45%) and/or additional (40%). However, one-third (34%) reimbursed employees for home office upgrades.

	TOTAL	PRIVATE	PUBLIC	MUSH
	2021	2021	2021	2021
	395	216	149	66
	%	%	%	%
Provide portable tools that can be moved between the organization and home office	45	45	48	45
Purchase additional tools for home offices	40	44	37	35
Reimburse employees for home office upgrades	34	38	29	23
Reimburse employees for mobile phone costs	29	35	19	20
Reimburse employees for home internet costs	29	31	24	21
Use employee monitoring software	25	28	19	17
Other, please specify	1	-	3	5
None/no additional investments or reimbursements	15	11	21	20
None/employees will not continue working remotely	3	3	2	3
No answer	2	2	1	2

Q50B. In which of the following ways, if any, will your organization equip employees so that they are able to continue to work remotely all or some of the time?
Base: Was required to work from home (personally or others in organization) as a result of the pandemic

PROTECTIONS IN RESPONSE TO COVID-19

In 2021, just under half (45%) say their organization implemented new cybersecurity protections in response to COVID-19.

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended	
	2021	2021	2021	2021	2020	2021
	510	287	181	80	500	510
	%	%	%	%	%	%
Yes	**45**	48	45	39	52	45
No	**45**	45	37	41	42	45
Don't know	**10**	6	18	20	6	10

Q51. Did your organization implement any new cybersecurity protections in response to COVID-19?
Base: Total sample

The most common new protections are for devices (71%) and new policies (54%).

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended	
	2021	2021	2021	2021	2020	2021
	231	139	82	31	260	231
	%	%	%	%	%	%
Protections to protect the devices of employees working from home	71	74	67	71	60	71
New policies	54	54	55	52	63	54
New platform(s)	41	40	43	29	38	41
Other	2	1	4	3	2	2
Don’t know	3	-	9	13	3	3

Q51B. Which of the following kinds of new cybersecurity protections did your organization implement in response to COVID-19?
Base: Organizations that have implemented new cybersecurity protections in response to COVID-19

Almost all (95%) indicate that at least some of the new protections will be permanent.

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended	
	2021	2021	2021	2021	2020	2021
	231	139	82	31	260	231
	%	%	%	%	%	%
NET YES	95	99	87	77	91	95
Yes, all	58	58	55	55	50	58
Yes, some	37	42	32	23	41	37
No	–	-	-	-	1	-
Don't know	5	1	13	23	8	5

Q51C. Will the new cybersecurity protections be permanent?
Base: Organizations that have implemented protections to protect the devices of employees working from home

INCIDENCE OF COVID-19 THEMED THREATS

One-quarter (26%) indicate that their organization has been targeted by a COVID-19 themed cybersecurity incident.

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended	
	2021	2021	2021	2021	2020	2021
	510	287	181	80	500	510
	%	%	%	%	%	%
Yes	 26	28	27	23	28	26
No	 59	62	47	50	60	59
Don't know	 15	9	26	28	12	15

Q51D. In recent months there have been media reports about cyber criminals using COVID-19 as a theme for their cyber attacks (e.g., phishing attempts that ask users to click to see test results, fake COVID-19 tracing apps, etc.). Has your organization been targeted by a COVID-19 themed cybersecurity incident?

Base: Total sample

Over 3-in-10 (36%) indicate that the volume of cyber attacks has increased during the pandemic.

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended	
	2021	2021	2021	2021	2020	2021
	510	287	181	80	500	510
	%	%	%	%	%	%
TOTAL INCREASED	**36**	38	38	35	29	36
Increased a lot	**7**	6	9	6	6	7
Increased somewhat	**29**	32	29	29	23	29
Stayed the same	**48**	47	42	45	49	48
Decreased somewhat	**3**	4	1	3	4	3
Decreased a lot	**<1**	<1	-	-	1	<1
TOTAL DECREASED	**3**	4	1	3	5	3
Don't know	**14**	11	19	18	16	14

Q51E. Has the volume of cyber attacks against your organization increased or decreased during the COVID-19 pandemic?
Base: Total sample

MONITORING FOR CHANGES IN NUMBER OF ATTACKS

More than 4-in-10 (47%) indicate that their organization is actively measuring for changes in the number of cyber attacks since the start of the pandemic.

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended	
	2021	2021	2021	2021	2020	2021
	510	287	181	80	500	510
	%	%	%	%	%	%
Yes	 47	51	45	34	45	47
No	 37	37	30	36	41	37
Don't know	 16	12	25	30	15	16

Q51F. Has your organization actively measured for changes in the number of cyber attacks since the start of the COVID-19 pandemic?
Base: Total sample??

LEVEL OF CONCERN ABOUT SECURITY FOOTPRINT

More than 4-in-10 (47%) are more worried about their organization's IT security footprint and policies in light of the COVID-19 pandemic.

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended	
	2021	2021	2021	2021	2020	2021
	510	287	181	80	500	510
	%	%	%	%	%	%
TOTAL MORE WORRIED	**47**	51	46	39	44	47
A lot more worried	**11**	9	13	9	13	11
Somewhat more worried	**37**	41	33	30	31	37
No change	**46**	44	46	55	51	46
Somewhat less worried	**3**	3	2	3	1	3
A lot less worried	**1**	1	1	-	1	1
TOTAL LESS WORRIED	**4**	4	3	3	2	4
Don't know	**3**	2	4	4	3	3

Q51G. To what extent are you more or less worried about your organization's IT security footprint and policies in light of the COVID-19 pandemic?
Base: Total sample

5

HOME DNS

USE OF 3rd PARTY DNS

More than 3-in-10 (36%) use a 3rd party DNS on their personal devices or home network.

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended	
	2021	2021	2021	2021	2020	2021
	510	287	181	80	500	510
	%	%	%	%	%	%
Yes	**36**	38	33	31	30	36
No	**46**	46	44	45	53	46
I run my own DNS and don't back it up with a 3rd party	**8**	7	9	9	5	8
No answer	**10**	8	14	15	12	10

Q51H. Do you use a 3rd party DNS (i.e. not your ISP) on your personal devices or home network?
Base: Total sample

USE OF CYBERSECURITY PROTECTION ON HOME DNS

Just under 9-in-10 (87%) use cybersecurity protection or content filtering on their home DNS.

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended	
	2021	2021	2021	2021	2020	2021
	222	131	76	32	172	222
	%	%	%	%	%	%
NET YES	87	89	86	88	91	87
Yes, cybersecurity protection	42	47	32	25	41	42
Yes, content filtering	19	21	21	22	26	19
Both	26	21	33	41	24	26
Neither	8	8	11	13	6	8
No answer	5	4	4	-	3	5

Q51I. Do you use cybersecurity protection or content filtering on your home DNS?
Base: Among those who use a home DNS

REASONS FOR USING A 3rd PARTY DNS SERVICE

Better privacy, performance, and malware filtering are the most common reasons for using a 3rd party DNS service.

	TOTAL	PRIVATE	PUBLIC	MUSH	TOTAL – Trended	
	2021	2021	2021	2021	2020	2021
	182	110	59	25	149	182
	%	%	%	%	%	%
Better privacy from hackers and/or cybertheft	**55**	52	56	72	44	55
Better performance	**46**	49	44	48	45	46
Malware filtering	**46**	45	49	60	53	46
Better privacy from my ISP	**42**	41	44	52	45	42
I like technology	**24**	22	25	24	29	24
Other	**1**	-	2	-	-	1
No answer	**1**	1	2	-	1	1

Q51J. What is the main reason that you use a 3rd party DNS service? **Select all that apply.**
Base: Total sample??

6

SAMPLE CHARACTERISTICS

Sample Characteristics

AGE

Total sample n=510	%
18-29	5
30-39	30
40-49	29
50-59	26
60 or older	11

PROVINCE OR TERRITORY

Total sample n=510	%
Newfoundland	1
Prince Edward Island	1
Nova Scotia	2
New Brunswick	1
Quebec	9
Ontario	56
Manitoba	2
Saskatchewan	<1
Alberta	12
British Columbia	16
Yukon/NWT/Nunavut	<1

GENDER

Total sample n=510	%
Male	80
Female	19
Prefer not to answer	1

EMPLOYMENT STATUS

Total sample n=510	%
Employed full-time	100
Employed part-time	-

EMPLOYEE OR SELF-EMPLOYED

Total sample n=510	%
Employee/Contractor working for a single organization	92
A business owner	8

TYPE OF ORGANIZATION

Employees n=468	%
Private sector	61
Public/Not-for-profit sector	39

PUBLIC SECTOR ORGANIZATION

Public sector n=181	%
Municipal government or agency	7
Provincial government or agency	20
Federal government or agency	21
Hospital or other health care organization	15
Primary or secondary school	2
College or university	13
School board	7
Public utility	4
Charity	3
Other	8
MUSH	44

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

Total sample n=510	%
50-99	26
100-249	26
250-499	16
500-999	13
1000 or more (public sector only)	19

Sample Characteristics

FAMILIARITY WITH ORGANIZATION'S COMPUTER SYSTEMS/IT FUNCTIONS

Total sample n=510	%
Very familiar	55
Somewhat familiar	45

COUNTRY IN WHICH ORG OPERATES

Total sample n=510	%
In Canada only	69
In countries outside of Canada	8
Both	21
Prefer not to answer	2

NUMBER OF YEARS IN OPERATION

Total sample n=510	%
Less than 1 year	1
1-2	3
3-5	11
6-10	15
11-20	16
More than 20 years	52
Prefer not to answer	2

IT AREAS INCLUDED WITHIN JOB

Employees n=510	%
System administration	54
Desktop IT	53
Cybersecurity	52
Networking	47
Other technical	32
Non-technical decision-making	30

ANNUAL REVENUE

Private organization n=287	%
Under $1M	3
$1M to just under $10M	20
$10M to just under $25M	20
$25M to just under $100M	19
$100M to just under $250M	13
$250M or more	7
Prefer not to answer	10
Don't know/Not sure	8