ANGUS REID INSTITUTE

Canada's Non-Profit Foundation Committed to Independent Research

Cyber concerns: Canadians show little confidence in ability of several key institutions to fend off cyberattacks

Two-thirds (65%) prefer to fight the hackers rather than pay ransom if their local hospital was targeted

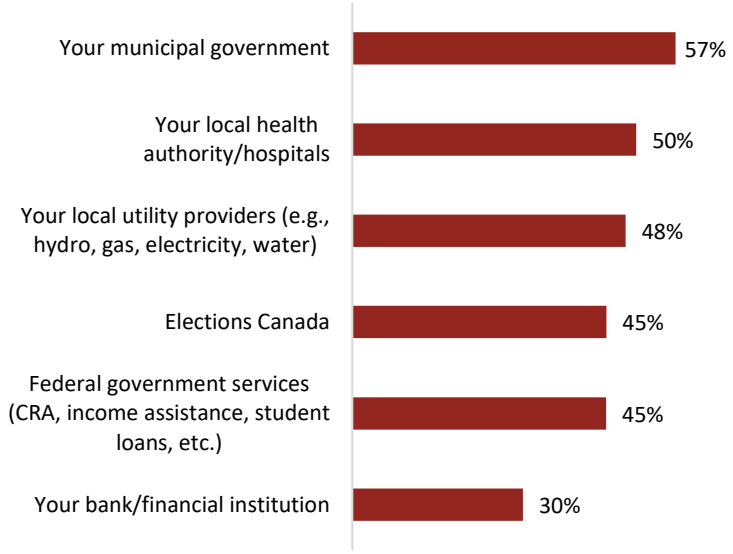
December 9, 2021 – Critical Canadian infrastructure was the target of more than 100 ransomware attacks in 2021 and new data from the non-profit Angus Reid Institute finds many Canadians lacking confidence in the ability of key institutions to defend themselves from cyber threats.

Canadian targets of ransomware attacks range from Rideau Hall, where an office connected to the governor general was recently targeted, to hospitals, including one that crippled Newfoundland and Labrador's healthcare system in October.

In the wake of the latter attack, which resulted in cancelled appointments and procedures throughout the province, half (50%) say they aren't confident their local health authority has up-to-date, high-quality cybersecurity, while two-in-five (43%) say they believe those institutions have the right defensive tools to fight cyberattacks.

Two-in-five lack confidence in Elections Canada (45%) and other federal government services such as the Canada Revenue Agency (45%) to fight hackers. Of all the institutions surveyed, Canadians had the most confidence in the cybersecurity of banks (65%).

How confident are you in each of the following to defend against cyberattacks, by having have up-to-date, high-quality cybersecurity? (All respondents, n=1,611; percentage picking 'not confident' shown)



METHODOLOGY:

The Angus Reid Institute conducted an online survey from Nov. 3-7, 2021, among a representative randomized sample of 1,611 Canadian adults who are members of Angus Reid Forum. For comparison purposes only, a probability sample of this size would carry a margin of error of +/- 2.5 percentage points, 19 times out of 20. Discrepancies in or between totals are due to rounding. The survey was self-commissioned and paid for by ARI. Detailed tables are found at the end of this release.

The threat isn't hypothetical for many Canadians; three-in-ten say they have been affected by a cyberattack and one-in-ten say their personal account or computer was compromised.

CONTACT:
Shachi Kurl, President: 604.908.1693 shachi.kurl@angusreid.org @shachikurl
Dave Korzinski, Research Director: 250.899.0821 dave.korzinski@angusreid.org
Jon Roe, Research Associate: 825.437.1147 jon.roe@angusreid.org

More Key Findings:

- Canadians would much rather prefer to fight than give in. In the case of a ransomware attack on a hospital, two-thirds (65%) would live with service disruptions and fight the hackers rather than pay the ransom while one-third (35%) prefer to pay up.

- Men aged 55 and older say they are the most likely to have been affected personally by a cyberattack – 14 per cent report having a personal account or computer compromised.

- Half (47%) of Canadians support legislation to ban the payment of ransoms to hackers in the event of ransomware attacks.

About ARI

*The **Angus Reid Institute (ARI)** was founded in October 2014 by pollster and sociologist, Dr. Angus Reid. ARI is a national, not-for-profit, non-partisan public opinion research foundation established to advance education by commissioning, conducting and disseminating to the public accessible and impartial statistical data, research and policy analysis on economics, political science, philanthropy, public administration, domestic and international affairs and other socio-economic issues of importance to Canada and its world.*

INDEX

Part One: Three-in-ten Canadians have been affected by a cyberattack

Part Two: Low confidence in cyber-resilience of Canadian institutions

Part Three: Canadians prefer to fight hackers instead of paying ransoms

Part One: Three-in-ten Canadians have been affected by a cyberattack

The issue of cybersecurity has come to the forefront after several high-profile Canadian institutions were targeted by hackers in recent months. Most recently, Rideau Hall experienced a "breach" in early December. The target was the internal network of the office that supports the work of the governor general, but details of who exactly was affected, and what information was accessed, have yet to be released.

The attack affecting the governor general's office follows what has been called the "worst cyberattack in Canadian history", when Newfoundland and Labrador's healthcare system was disrupted provincewide by an October ransomware attack targeting "the brain of the data centre". Thousands of appointments were delayed, including nearly all non-emergency procedures in one of the province's four health authorities.

Ransomware attacks – caused by hackers who gain control of and lock computer systems until a ransom is paid – have increased by 151 per cent in the first six months of 2021 when compared to 2020, according to the Communication Security Establishment's Canadian Centre for Cyber Security. The centre believes that is the tip of the iceberg and many more go unreported. Of the 235 known attacks, more than half targeted critical infrastructure, including electrical grids and hospitals. In response to the

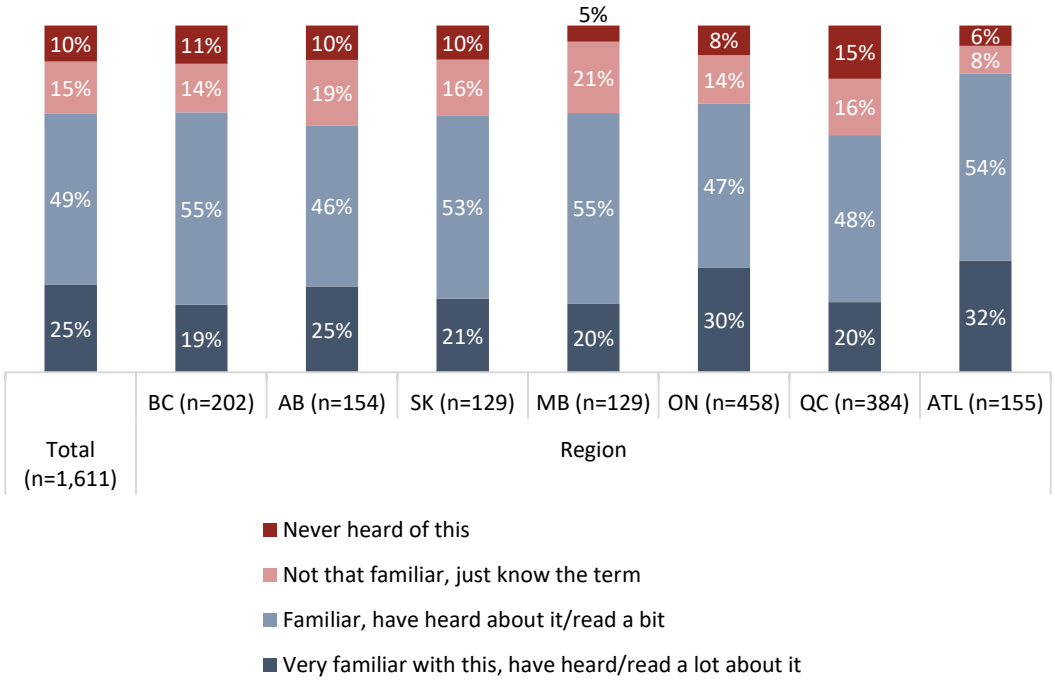
CONTACT:
Shachi Kurl, President: 604.908.1693 shachi.kurl@angusreid.org @shachikurl
Dave Korzinski, Research Director: 250.899.0821 dave.korzinski@angusreid.org
Jon Roe, Research Associate: 825.437.1147 jon.roe@angusreid.org

increasing threat, the Cyber Centre posted a playbook, advising Canadian organizations on how to best protect themselves from ransomware attacks – and what to do if they are targeted by hackers.

The problem is also growing south of the border. This year, hackers disrupted a major fuel supply pipeline in the United States in May and targeted meat-packing company JBS for an US$11-million ransom. The U.S. is meeting the threat head-on, according to the U.S. Cyber Command, which said the military has "imposed costs" on ransomware groups.

The threat of cyberattacks is on the minds of Canadians: three-quarters (75%) say they are familiar with this form of digital sabotage. In the wake of the incident in Canada's eastern-most province – which required Newfoundland and Labrador to go back in time to a paper-based system from the 1980s to keep clinics running – awareness is highest in Atlantic Canada:

Prior to reading the information we've just shared above, how familiar have you been with this type of event – have you seen or heard of cyberattacks happening in Canada?

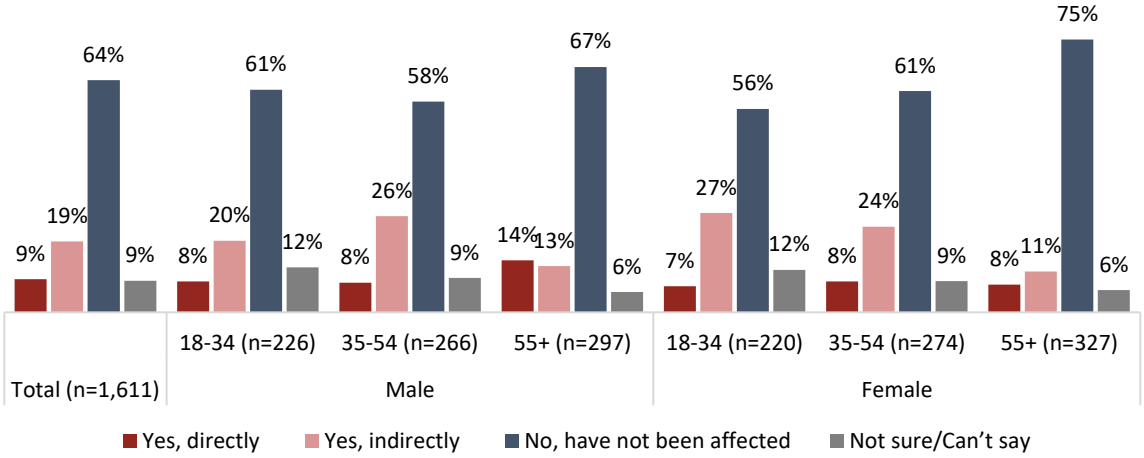


Three-in-ten Canadians say they have been indirectly affected by a cyberattack – instances where their data held by a third-party was illegally accessed – and one-in-ten say their personal account was compromised or their own computer was infected.

Men aged 55 and older are the most likely demographic to report being directly affected by a cyberattack – 14 per cent say that's the case – while those under 55 are much more likely to report being affected indirectly:

CONTACT:
Shachi Kurl, President: 604.908.1693 shachi.kurl@angusreid.org @shachikurl
Dave Korzinski, Research Director: 250.899.0821 dave.korzinski@angusreid.org
Jon Roe, Research Associate: 825.437.1147 jon.roe@angusreid.org

Have you been personally affected by a cyberattack?

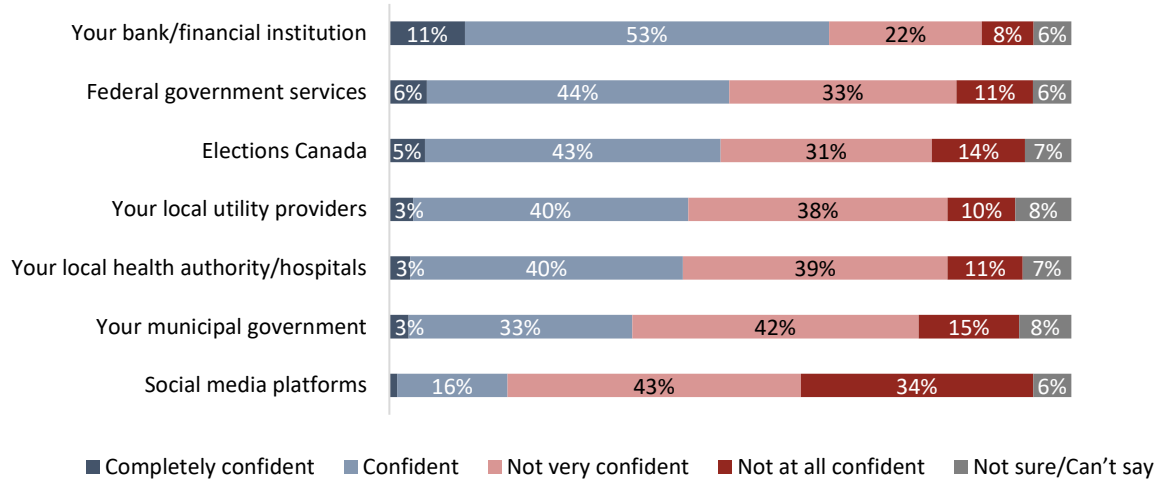


For the one-in-ten who have been personally affected by a cyberattack, awareness of the problem is much higher. Two-in-five (41%) say they are very familiar and are well versed in the subject (see detailed tables).

Part Two: Low confidence in cyber-resilience of Canadian institutions

Further, Canadians aren't confident key institutions are well insulated against the threat posed by hackers. Canadians have the highest levels of assurance in financial institutions, with two-thirds (65%) saying they are confident that banks have high-quality cybersecurity. But only half say the same of the federal government and its services, while it drops even lower for local governments and health systems:

How confident are you in each of the following to defend against cyberattacks, by having have up-to-date, high-quality cybersecurity? (All respondents, n=1,611)



CONTACT:
Shachi Kurl, President: 604.908.1693 shachi.kurl@angusreid.org @shachikurl
Dave Korzinski, Research Director: 250.899.0821 dave.korzinski@angusreid.org
Jon Roe, Research Associate: 825.437.1147 jon.roe@angusreid.org

There are demographic divides when it comes to confidence in federal government services' cybersecurity. Men aged 18 to 34 are the least confident in the federal government while women the same age are the most confident.

Meanwhile, three-in-ten (28%) 18- to 34-year-old men are confident social media platforms are secure against cyberattacks, double the rate of men aged 55-plus – notably the group most likely to have experienced a cyberattack personally:

How confident are you in each of the following to defend against cyberattacks, by having have up-to-date, high-quality cybersecurity? (Percentage choosing 'completely confident' or 'confident' shown)							
(Weighted sample sizes)	Total (n=1,611)	Age and Gender					
		Male			Female		
		18-34 (n=226)	35-54 (n=266)	55+ (n=297)	18-34 (n=220)	35-54 (n=274)	55+ (n=327)
Your bank/financial institution	65%	67%	64%	67%	67%	61%	62%
Federal government services	50%	44%	48%	53%	57%	51%	46%
Elections Canada	49%	51%	46%	48%	51%	48%	49%
Your local utility provider	44%	43%	35%	52%	42%	44%	46%
Your local health authority/ hospitals	43%	36%	38%	48%	45%	45%	44%
Your municipal government	36%	31%	30%	34%	40%	38%	40%
Social media platforms	17%	28%	18%	14%	18%	15%	13%

Confidence varies across the country. Notably, confidence in the ability of Elections Canada to defend itself against cyberattacks ranges from a high of 53 per cent of British Columbians, to a low of one-third (35%) of Albertans. With the disruption in Newfoundland and Labrador's health system fresh in mind, Atlantic Canadians have the lowest confidence in the cybersecurity of their local health authority and hospitals (see detailed tables).

Those who have been victimized by hackers indirectly have much lower confidence in the digital defence systems of local health authorities (34%) and utility providers (36%) than those who have been targeted more directly:

CONTACT:
Shachi Kurl, President: 604.908.1693 shachi.kurl@angusreid.org @shachikurl
Dave Korzinski, Research Director: 250.899.0821 dave.korzinski@angusreid.org
Jon Roe, Research Associate: 825.437.1147 jon.roe@angusreid.org

How confident are you in each of the following to defend against cyberattacks, by having have up-to-date, high-quality cybersecurity? (Percentage choosing 'completely confident' or 'confident' shown)				
(Weighted sample sizes)	Total (n=1,611)	Affected by Cyberattack		
		Yes, directly (n=147)	Yes, indirectly (n=314)	No, have not been affected (n=1,028)
Your bank/financial institution	65%	65%	62%	67%
Federal government services	50%	51%	46%	52%
Elections Canada	49%	51%	48%	50%
Your local utility providers (e.g., hydro, gas, electricity, water)	44%	50%	36%	47%
Your local health authority/hospitals	43%	46%	34%	47%
Your municipal government	36%	37%	28%	39%
Social media platforms	17%	17%	15%	18%

Part Three: Canadians prefer to fight hackers instead of paying ransoms

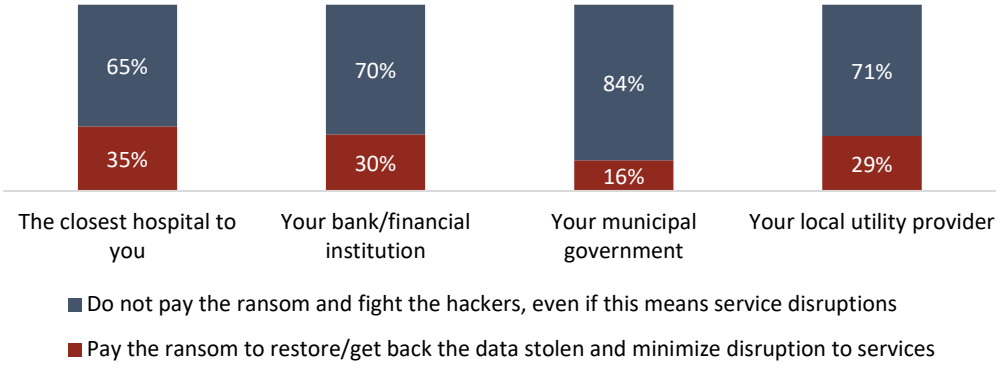
In late November INTERPOL coordinated an international crackdown on hackers which resulted in over 1,000 arrests. The U.S. military, too, has confronted the problem directly. Earlier in the year, the U.S. Cyber Command said ransomware attacks were the responsibility of law enforcement. Now, it says it is taking offensive measures against ransomware groups.

It would appear that most Canadians share a similar impulse to fight back against cyberattacks. When hypothetically placed at the helm of various institutions in the midst of a ransomware crisis, most Canadians say they would not pay up and would instead choose to fight back against the hackers – even if this meant service disruptions.

This stands in contrast with a report released earlier this year, in which 54 per cent of Canadian companies hit by such an attack said they paid the ransom (another survey this year found that 69 per cent of the companies they surveyed paid the ransom).

CONTACT:
Shachi Kurl, President: 604.908.1693 shachi.kurl@angusreid.org @shachikurl
Dave Korzinski, Research Director: 250.899.0821 dave.korzinski@angusreid.org
Jon Roe, Research Associate: 825.437.1147 jon.roe@angusreid.org

Suppose you were in charge of each of the following institutions and they were attacked by hackers demanding a ransom to restore data. For each institution, what would you do?
(All respondents, n=1,611)



There are some important differences in opinion when broken down by age and gender. On the example of a local hospital, fully four-in-five (80%) men over the age of 55 would refuse to pay the ransom – a number which falls to half (50%) of women aged 18 to 34:

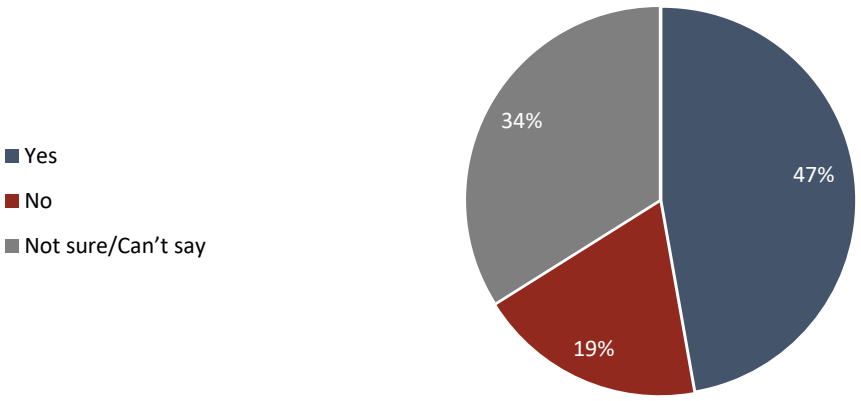
Suppose you were in charge of the local hospital, and they were attacked by hackers demanding a ransom to restore data. What would you do?							
(Weighted sample sizes)	Total (n=1,611)	Age and Gender					
		Male			Female		
		18-34 (n=216)	35-54 (n=272)	55+ (n=303)	18-34 (n=225)	35-54 (n=280)	55+ (n=315)
Pay the ransom to restore/get back the data stolen and minimize disruption to services	35%	40%	27%	20%	50%	38%	37%
Do not pay the ransom and fight the hackers, even if this means service disruptions	65%	60%	73%	80%	50%	62%	63%

CONTACT:
Shachi Kurl, President: 604.908.1693 shachi.kurl@angusreid.org @shachikurl
Dave Korzinski, Research Director: 250.899.0821 dave.korzinski@angusreid.org
Jon Roe, Research Associate: 825.437.1147 jon.roe@angusreid.org

In an effort to disincentivize ransomware attacks, lawmakers in the U.S. have recently proposed the Ransomware and Financial Stability Act which would ban companies from paying any ransoms over US$100,000 without first seeking the government's permission. At least three states – New York, North Carolina, and Pennsylvania – are also exploring this option, while a similar bill died in committee in Texas earlier this year.

Although no such legislation is being considered publicly in Canada at the moment, a plurality of Canadians (47%) say they would support a ban on ransomware payments. Another one-third (34%) said they aren't sure:

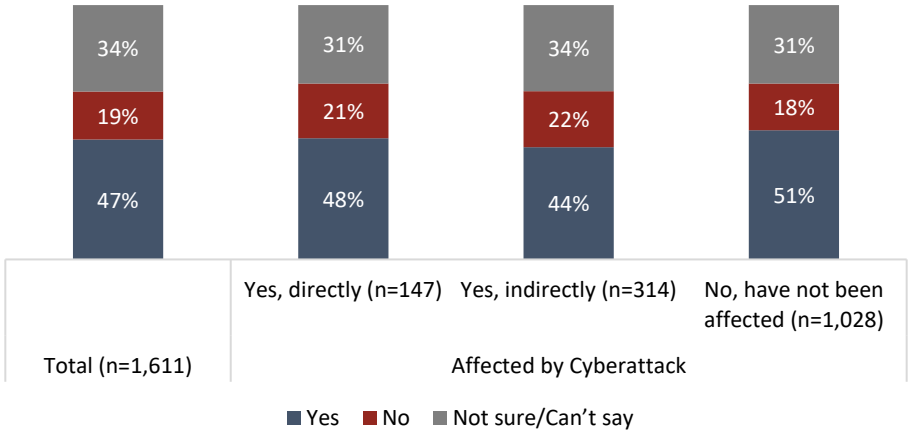
Would you support legislation that bans ransomware payments?
(All respondents, n=1,611)



Those who have been directly and indirectly affected by cyberattacks don't hold stronger opinions on the matter of a ban on ransomware payments. Half (48%) who have been directly affected believe there should be a ban, while two-in-five (44%) who were indirectly targeted by hackers say the same:

CONTACT:
Shachi Kurl, President: 604.908.1693 shachi.kurl@angusreid.org @shachikurl
Dave Korzinski, Research Director: 250.899.0821 dave.korzinski@angusreid.org
Jon Roe, Research Associate: 825.437.1147 jon.roe@angusreid.org

Would you support legislation that bans ransomware payments?



For detailed results by age, gender, region, education, and other demographics, click here.

For detailed results by whether or not respondents were affected by a cyberattack, click here.

CONTACT:
Shachi Kurl, President: 604.908.1693 shachi.kurl@angusreid.org @shachikurl
Dave Korzinski, Research Director: 250.899.0821 dave.korzinski@angusreid.org
Jon Roe, Research Associate: 825.437.1147 jon.roe@angusreid.org