ESET CYBERSECURITY BAROMETER

CANADA 2018

"More than 80 percent of Canadians surveyed believe that the risk of becoming a victim of cybercrime is increasing."

"Nine out of ten Canadians now identify cybercrime as a serious challenge to the country's security, bigger than terrorism, corruption, and other criminal activity."

PREFACE

The ESET Cybersecurity Barometer Canada is a survey of public opinion about cybersecurity and cybercrime. The survey was conducted because there is a dearth of contemporary research quantifying public attitudes toward, and experience of, cybercrime. Yet public support for cybersecurity efforts, including cybercrime deterrence, is critical to preserving the benefits of the digital technologies upon which we now rely.

As a security software company with three decades of experience fighting criminal abuse of information systems, ESET understands that people are one of the three key factors involved in containing cybercrime, the other two being process and technology. People are victimized by cybercrime. People elect the politicians who determine cybercrime policy. People foot much of the tax bill for law enforcement efforts to reduce cybercrime. Knowing what the public thinks about cybercrime and cybersecurity is essential for successful cybercrime policy development and critical to success in society's cybersecurity efforts. (For more on this, see "Why ask the public about cybercrime and cybersecurity?" by ESET security researcher Stephen Cobb.)

For ESET Cybersecurity Barometer 2018, a survey sample of 3,500 people was used (1,000 in Canada and 2,500 in the US). The US report will appear separately. A report focusing on inter-country comparisons – encompassing North America and the 28 nations of the EU – will also be published. Repeating the surveys in 2019 will produce longitudinal data across both continents.

The ESET Cybersecurity Barometer is modelled on prior studies conducted by the European Union (EU) and published as the "Special Eurobarometer: Cyber Security." The EU has conducted four of these studies – the most recent was published in 2017 – and they provide longitudinal research across 28 countries based on a 1,000-person sample from each country. This research has the potential to help a wide range of cybersecurity stakeholders, including policymakers, consumers, companies, and government agencies. The ESET Cybersecurity Barometer extends the potential benefits of this type of research to North America.

METHODOLOGY

The survey reported here polled 1,000 Canadian adults using standard CAWI methodology with random sampling based on age, gender, and place of residence. It was conducted for ESET in September of 2018 by MNFORCE using the Research Now SSI panel.

CONTENTS

1. EXECUTIVE SUMMARY

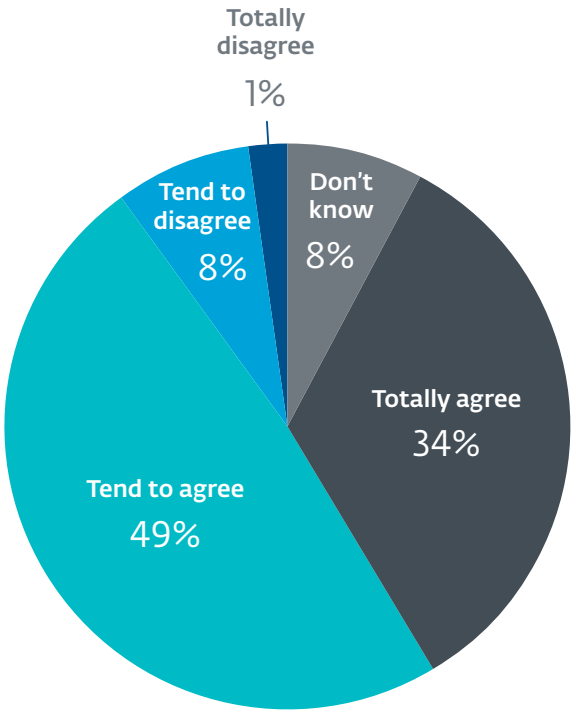
The survey findings show that Canadians are very concerned about cybersecurity, with more than eight out of ten believing that the risk of becoming a victim of cybercrime is increasing.

While the number of people expressing concern about cybercrimes was found to be considerably higher than the number of people reporting that they had experienced cybercrimes, these levels of concern should still be taken very seriously by companies that rely on consumer trust in the internet.

Government agencies, such as law enforcement, should also take note and align their resources toward the reduction of cybercrime whenever possible.

The finding that nine out of ten Canadians now see cybercrime as a serious challenge to the internal security of Canada is striking. Furthermore, the level of concern about cybercrime was found to exceed that related to terrorism, corruption, and other serious criminal activities. This suggests that a realignment of resources may be needed. Indeed, less than half of the Canadians surveyed thought that the authorities were doing enough to fight cybercrime (the government received higher marks for its efforts fighting terrorism and arms trafficking).

The ESET Cybersecurity Barometer makes it clear that Canadians think there is too much cybercrime, and not enough cybersecurity, to justify a full embrace of online technology. To the extent that this situation impedes progress and threatens the promised benefits of digital transformation, concerted action by government agencies and corporate entities to improve this situation would seem to be urgently needed.



Do you agree with this statement:
"I believe the risk of becoming a victim of cybercrime is increasing"?

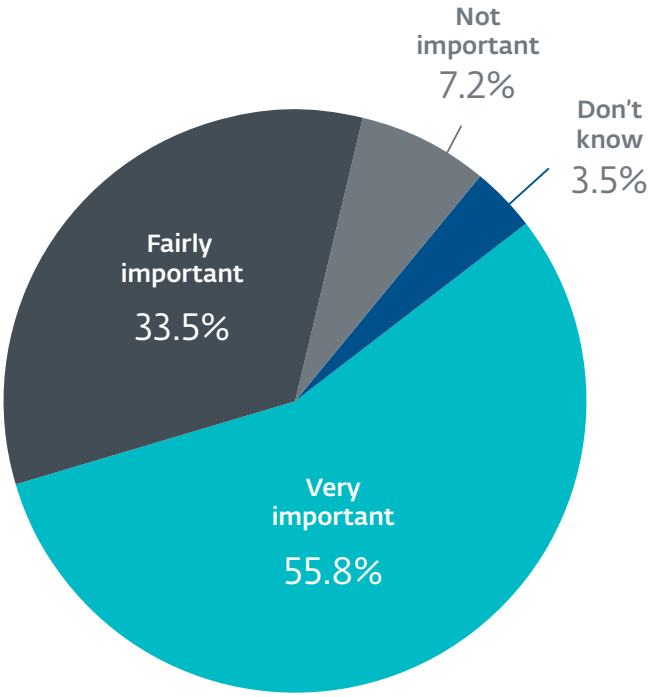
2. CYBERCRIME AS A THREAT TO SECURITY

The ESET Cybersecurity Barometer reveals that most Canadians now consider cybercrime to be an important challenge to the internal security of Canada, with nine out of ten saying it is either very important (55.8%) or fairly important (33.5%).

To place this in perspective, Canadians consider cybercrime to pose more of a challenge to internal security than a number of other serious criminal activities, like terrorism, human trafficking, or money laundering.

This perception of cybercrime appears to be widely shared across Canada, although the Atlantic region expressed the greatest concern (the number of respondents in that region who said that cybercrime was not very important was zero).

Two factors contributing to this high level of concern about cybercrime are personal experiences of cybercrime and the perceptions that people have about the government's response to the problem, or lack thereof. The survey data speaks to both of these factors.

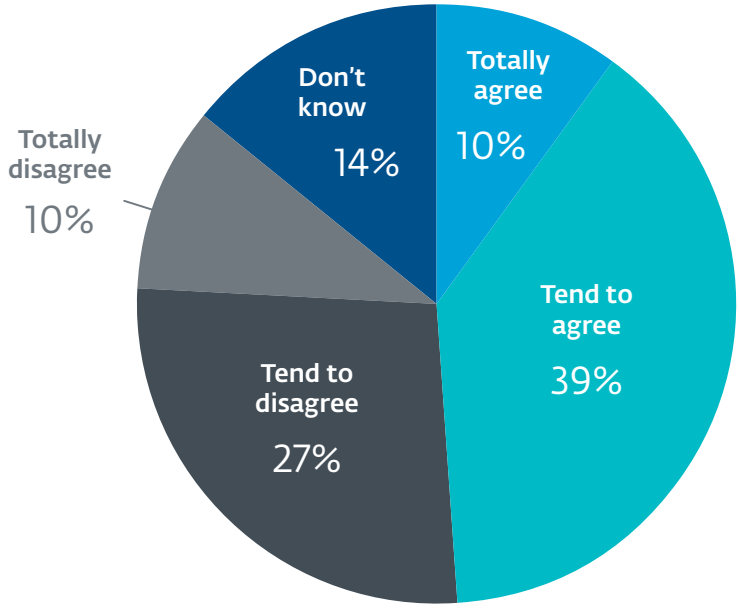


How important is cybercrime as a challenge to the internal security of Canada?

Slightly less than half of Canadian respondents think that the police and other law enforcement authorities are doing enough to fight cybercrime.

While this is disappointing – and may well contribute to the high levels of concern about cybercrime – it is nevertheless better than the perception south of the border.

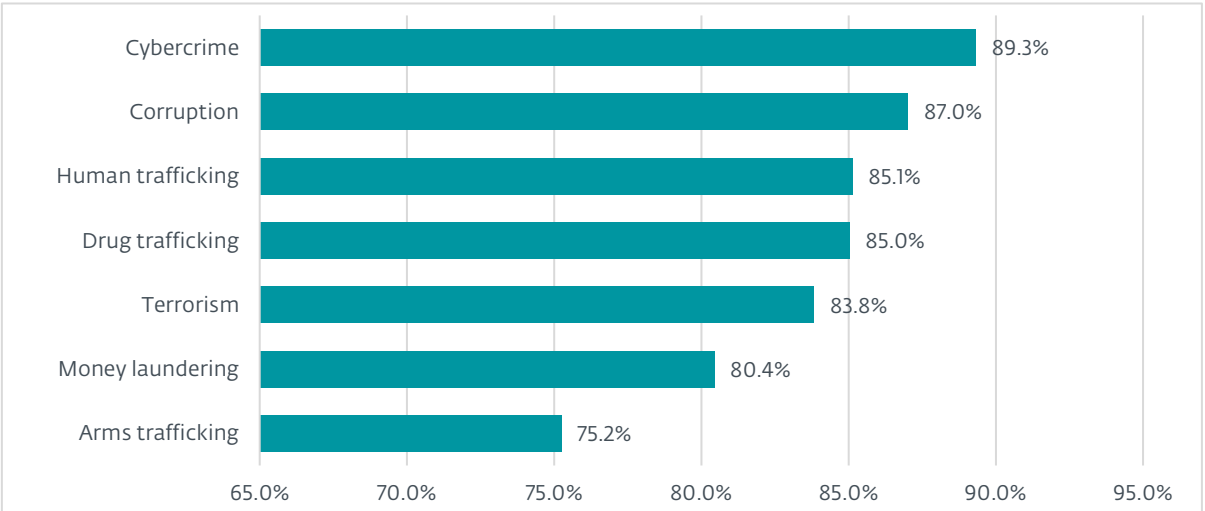
Only 44% of US respondents surveyed agreed that the authorities in their country were doing enough to fight cybercrime.



Are the police and other law enforcement authorities in Canada doing enough to fight cybercrime?

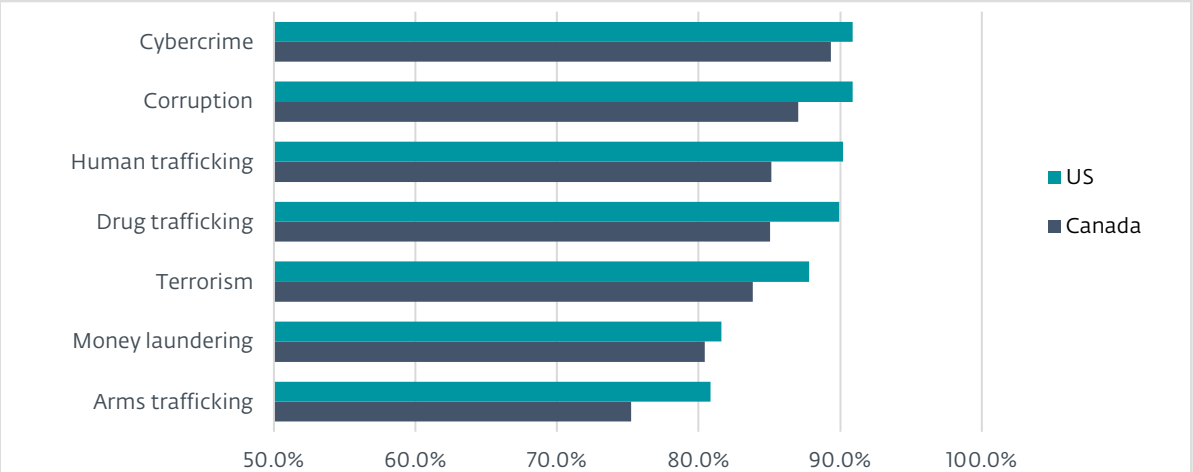
Most cybersecurity professionals concur that fighting crime in cyberspace is quite different from tackling crime in physical space, and considerably harder. For the police and other law enforcement authorities to gain ground against criminals in cyberspace requires a serious investment in skills and resources, together with a clear signal that fighting cybercrime is a priority.

According to the survey, Canadians tend to think the government is doing a better job against terrorism and arms trafficking than it is against cybercrime or corruption. This may be reflected in how Canadians responded when asked to rate the importance of seven criminal activities as challenges to internal security.



Importance of criminal activity as a challenge to the internal security of Canada (percentage of respondents who chose Fairly Important or Very Important)

Canadians are not alone in putting cybercrime at the top of the list. Respondents in the US also saw cybercrime as the most important challenge, but to an even higher degree. However, while Canadians have a lower level of concern across all of these criminal activities when compared with their neighbors to the south, it is interesting that the concern gap around cybercrime is fairly small.



Importance of criminal activity as a challenge to the internal security of your country (percentage of respondents who chose Fairly Important or Very Important)

3. CYBERSECURITY CONCERNS

The ESET Cybersecurity Barometer asked Canadians how concerned they were about experiencing or being a victim of various forms of cybercriminal activity such as the hacking of their email or social network account, discovering malware on their computer, or being asked for a payment in return for getting back control of a device (ransomware).

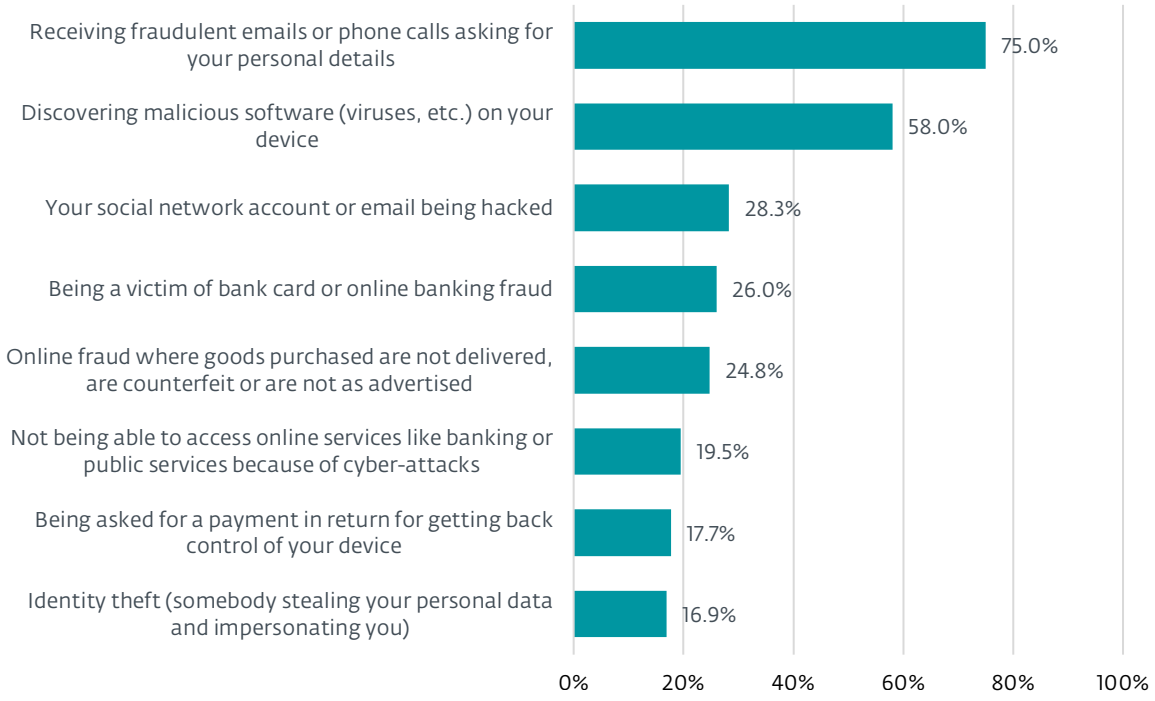
The next two charts explore this data, which indicates that the biggest concern of all is identity theft, defined in the survey as "somebody stealing your personal data and impersonating you." This is closely followed by concern about becoming a victim of bank card or online banking fraud. Malware infection rounds out the top three worries.

Percentage of respondents registering concern about experiencing cybercriminal activity (Fairly Concerned plus Very Concerned)

Taken as a whole, these responses to questions about specific cybersecurity concerns may help to explain why Canadians think cybercrime is such a big problem: All eight issues are concerning to more than 60% of respondents, with the exception of "being asked for a payment in return for getting back control of your device," and that scored 59%.

(Note that asking for a payment "in return for getting back control of your device" is one way to describe ransomware, but the survey question was developed – and tracked in the EU – before the term ransomware was widely used. It is possible that more people would have expressed concern if the term ransomware had been used.)

Levels of concern about becoming a victim of crime may not be a direct reflection of how much crime occurs, so the survey also asks directly: "How often have you experienced or been a victim of the following situations?" The survey tracks the same categories as in the questions about levels of concern. The results show that in Canada, two categories of criminal activity had been experienced by more than half of all respondents: fraudulent requests for personal information and malware.



Respondents who had experienced cybercriminal activity (often or occasionally)

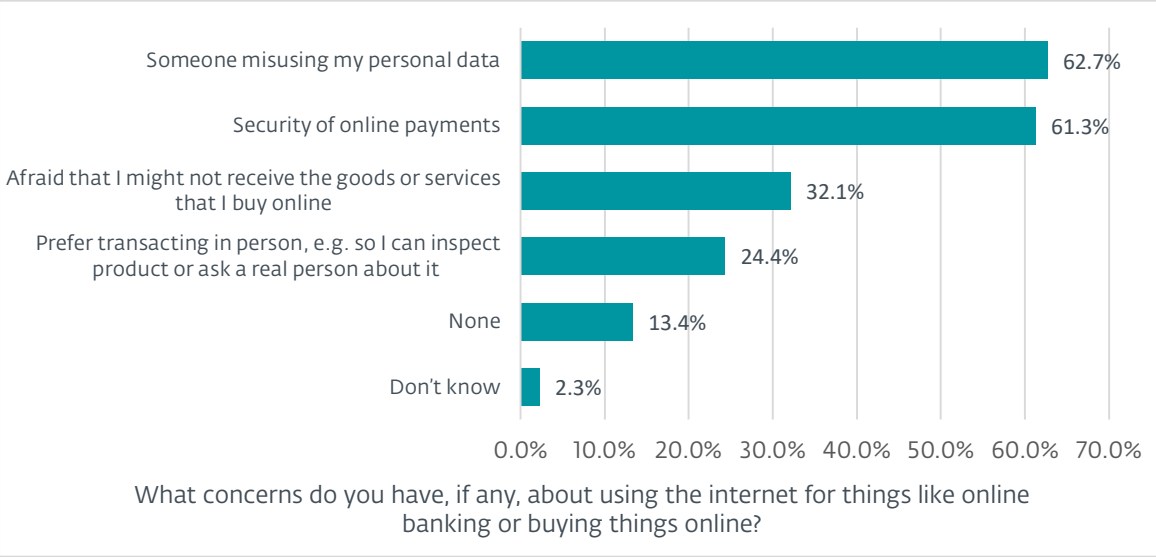
From the perspective of criminology, it is interesting that identity theft was the least experienced but most feared item among those presented. However, inverse relationships like this are not unprecedented in crime research. Fear of specific crimes may be amplified by heavy media coverage and well-intentioned victim advocacy. This can have positive effects, like attracting resources to address the problem and encouraging crime-reducing behavior among potential victims.

Of course, some crimes are worse than others in terms of their impact on people's lives. For example, anecdotal evidence suggests that identity theft can be very unsettling to people, causing a greater psychological impact than some other forms of digital crime.

When asked about a variety of cybersecurity concerns related to online banking and shopping, more than three out of five Canadians surveyed indicated that they are worried about the misuse of personal data supplied in online transactions.

While Canada has worked hard to be a leader in digital privacy, these findings suggest that the companies with whom Canadians do business online could do a better job of reassuring online customers from Canada about the protections they provide for personal information. It could also be argued that fewer headlines about data breaches would help improve trust.

Three out of five Canadians also indicated concern about the security of online payments. Again, this could be interpreted as a call to online merchants to improve their security posture and demonstrate that they take the security of online transactions seriously.



What concerns do you have, if any, about using the internet for things like online banking or buying things online?

Interestingly, concern about misuse of personal data involved in online transactions was much lower in Quebec (57%) than the rest of Canada. In North America generally, there is less concern about non-delivery of goods and services bought online than there is about the security of online payments, but Canadians were more concerned about non-delivery of online purchases than their US counterparts (32% to 24%).

The preference for performing transactions in person as a response to online security concerns was a lot higher in the Atlantic region (36%) than the rest of Canada. Despite that preference, the Atlantic region reported an average level of online activity in the category "buying goods and services," as can be seen from this table.

Which of the following activities do you do online?	REGION				
	Ontario	Atlantic	Western	Quebec	Canada
Online banking	89.0%	87.5%	84.3%	85.2%	86.6%
Buying goods or services (holidays, books, music, etc.)	79.5%	75.0%	74.3%	70.0%	75.4%
Selling goods or services	33.2%	40.3%	31.3%	32.1%	32.9%
Using online social networks	79.5%	87.5%	72.0%	74.7%	76.7%
Sending or receiving email	90.8%	93.1%	93.0%	89.9%	91.4%
Reading news	78.8%	80.6%	80.3%	72.6%	77.9%
Playing games	54.0%	63.9%	52.3%	52.3%	53.8%
Watching TV	48.3%	50.0%	44.3%	48.5%	47.3%
Other	2.0%	1.4%	2.7%	2.5%	2.3%
Don't know	0.5%	0.0%	0.3%	0.4%	0.4%

Concerns related to use of the internet were also assessed with a survey question that asked respondents if they agreed or disagreed with this statement: "I am concerned that my online personal information is not kept secure by websites." Sadly, one in four Canadians surveyed said that they totally agreed. Almost half tended to agree. Given the extent to which companies and government agencies have come to rely on the internet as a tool for communication and interaction with the public, these numbers should be worrying.

The survey also asked people if they agreed with this statement: "I am concerned that my online personal information is not kept secure by public authorities." A disappointing two thirds of Canadian respondents either tended to agree (45%) or totally agreed (22%). Overall concern was lowest in Quebec (64%) and highest in the Atlantic region (72%).

When it comes to improving cybersecurity and addressing the risks of cybercrime, it is helpful to know the degree of confidence that people have in their ability to understand the problem. The ESET Cybersecurity Barometer found that two thirds of the North Americans surveyed considered themselves to be well-informed about the risks of cybercrime (either fairly well or very well informed). However, confidence was higher in the US (70%) than in Canada (62%).

In comparison, when this same question was asked of the residents of all 28 EU countries in 2017, the total "well-informed" percentage was only 46% for the region as a whole; however, there was considerable variation between countries (ranging from 27% in Bulgaria to 76% in Denmark).

As the following table shows, there were considerable regional variations within Canada. The Atlantic and Western regions considered themselves less well informed, while people in the province of Ontario appeared to be most confident.

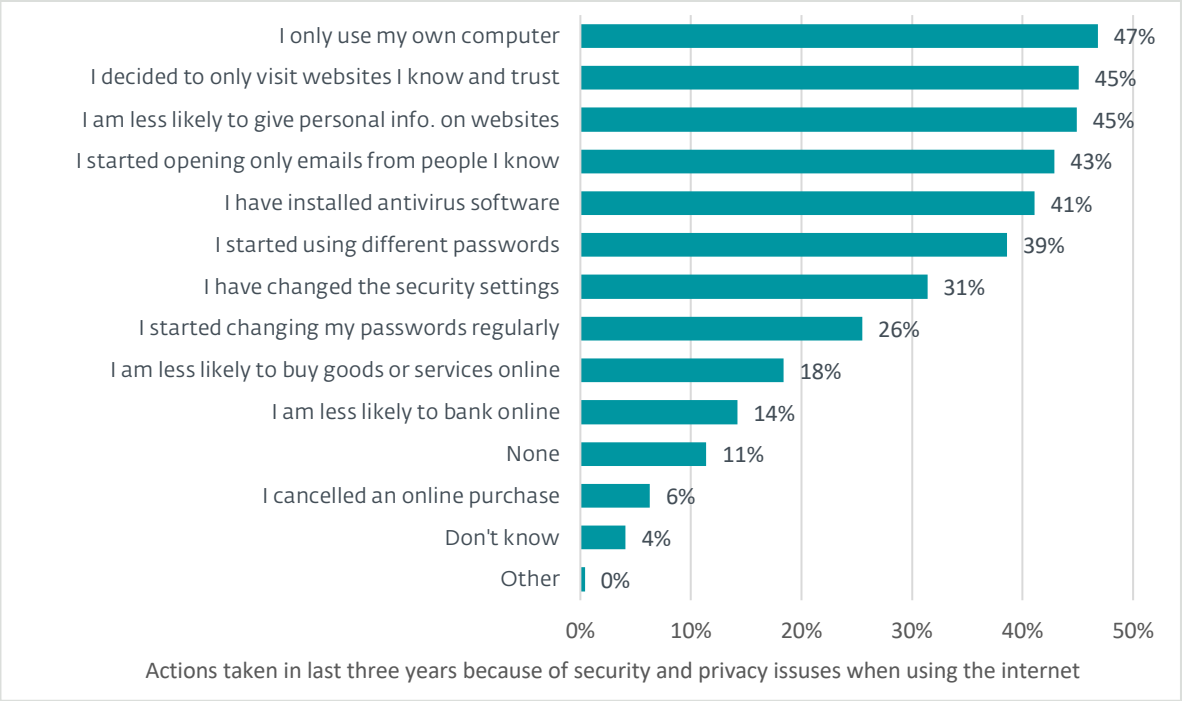
How well informed do you feel about the risks of cybercrime?		REGION				
		Ontario	Atlantic	Western	Quebec	Canada
	Very well informed	13.0%	12.5%	5.7%	13.1%	10.8%
	Fairly well informed	51.4%	44.4%	54.7%	47.7%	51.0%
	Not very well informed	29.7%	37.5%	31.7%	33.3%	31.7%
	Not at all informed	3.8%	2.8%	5.0%	3.0%	3.9%
	Don't know	2.0%	2.8%	3.0%	3.0%	2.6%

Being well-informed about cybercrime is one thing; believing that you are able to protect yourself against cybercrime is another. The survey found that two thirds of Canadians appear confident in this regard, agreeing with the following assertion: "I am able to protect myself sufficiently against cybercrime, e.g. by using antivirus software." Conversely, the other third may represent market growth potential for security vendors.

I am able to protect myself sufficiently against cybercrime, e.g. by using antivirus software		REGION				
		Ontario	Atlantic	Western	Quebec	Canada
	Totally agree	16.6%	15.3%	14.3%	17.3%	16.0%
	Tend to agree	52.4%	41.7%	50.7%	47.7%	50.0%
	Tend to disagree	18.4%	25.0%	17.7%	19.4%	18.9%
	Totally disagree	4.6%	2.8%	2.7%	3.4%	3.6%
	Don't know	7.9%	15.3%	14.7%	12.2%	11.5%

4. CYBERSECURITY RESPONSES

Canadians have taken a variety of actions in the last three years because of security and privacy issues when using the internet, from only using their own computers to changing passwords. More than a third of those surveyed have adjusted their security settings and installed antivirus software.



Companies that rely heavily on internet transactions should note the percentage of people who said that they are less likely to shop or bank online due to security and privacy concerns (18% and 14%, respectively). While the percentages are not high, they surely represent lost opportunity for retailers and financial firms. Marketers should also note that almost half of Canadians chose to give out less personal information on websites.

As a means of assessing people's security priorities, the ESET Cybersecurity Barometer respondents were asked: "Have you changed your password to access your account(s) for any of the following online services during the last 12 months?" Seven categories of account were presented, and clearly email accounts were the primary concern (this assumes that a password change reflects security concern or prioritization).

	Ontario	Atlantic	Western	Quebec	Canada
Email	61.6%	73.6%	55.3%	55.3%	59.1%
Online social networks	44.0%	52.8%	35.0%	45.1%	42.2%
Shopping websites	37.1%	38.9%	32.0%	29.5%	33.9%
Online banking	54.0%	59.7%	50.7%	46.8%	51.7%
Online games	14.8%	18.1%	12.0%	13.9%	14.0%
Public services websites	18.2%	19.4%	14.7%	16.0%	16.7%
Other	2.3%	1.4%	3.0%	3.0%	2.6%
None	17.1%	5.6%	20.3%	20.7%	18.1%

5. DISCUSSION

Cybersecurity involves protecting digital technologies – upon which we are now so heavily dependent – against criminals who seek to abuse those technologies for their own ends. Public support for efforts to reduce cybercrime is critical to society's efforts to preserve the benefits of digital technologies. That is why it is so important to know what the public thinks about cybercrime and cybersecurity, something that the EU recognized when it created the EU Barometer for Cybersecurity.

The data from that project has not only helped to inform policy decisions in EU countries, but also provided valuable input for marketing projects. Academic researchers have used the data to analyze the relationship between cybercrime experience and online technology adoption.

Neither the Canadian government nor the US government appear to have felt the need to undertake similar surveys of their citizens, seemingly content to let companies be the default source of data about the cybercrime problem. There are several problems with that approach. The results of any survey about cybersecurity that was carried out by a company that sells security-related products and services is open to accusations of bias, particularly if the implications of those results conflict with the agendas of the politicians and policy makers to whom they are presented.

The same weakness can affect the private sector as well. Any CEO who does not want to believe that the public perceives cybercrime to be a serious threat may discount company-sponsored research. One motive for wanting to ignore growing evidence of a looming cybercrime crisis might be resistance to increasing the cost of a hardware or software product to make it more secure. An abundance of insufficiently secure products only adds to the incidence of cybercrime.

The main reason that the ESET Cybersecurity Barometer was fielded with the same set of questions as the EU research was to refute accusations of bias. The survey was conducted by a reputable survey firm using accepted methodology. The results are solid and should be used by policy makers working on the cybercrime problem without fear of challenge.

In conclusion, these results strongly suggest that, unless cybersecurity and cybercrime deterrence are treated as priorities by government agencies and corporations, the rate at which systems and data are abused will continue to rise, further undermining the public's trust in technology. That trust is vital to Canada's economic well-being, now and in the future.

Author: Stephen Cobb, CISSP