cira

BUILDING A BETTER ONLINE CANADA

2018 CIRA CANADIAN INTERNET SECURITY SURVEY

While there is a wealth of published survey data available that provides insight into various aspects of cybersecurity, most of it has been collected in countries outside of Canada or aggregates Canadian data as part of the North American geographic market. As a result, there is limited data available in the public domain that specifically captures the Canadian perspective in this dynamic and rapidly evolving area.

To close this information gap, we launched the first CIRA Canadian Internet Security Survey in late 2017, and are pleased to publish the results in this report. We invited owners of .CA domains to take part in the survey and give us their perspectives on a wide range of topics related to cybersecurity.

Methodology

Between November 2017 and January 2018, we surveyed 1,985 Canadians who own at least one .CA domain registered to either a business or an institution (this includes non-profit organizations and government). The survey respondents were streamed into three main groups, based on how they use their .CA domain name. About 18 per cent of survey respondents use their domain for a personal website, usually a sole proprietor business; 74 per cent use it for a small business website, and the other 8 per cent use it for the website for an organization with more than 100 employees.

The vast majority of business professionals we surveyed report playing a significant role in their organization's IT and security-related decision making. In the case of small business respondents 72 per cent indicated they are primarily responsible for the security and IT operations for their business, while 90 per cent of those working for larger organizations said they are involved in the security and IT decision-making process.

And finally, the online survey invitation was sent via an email with participation voluntary.

Breakdown of survey respondents based on how they are using their domain name

Key Findings

- **Awareness of cyber threats is high among all respondents** - Awareness of the scope and type of cyber threats is high across all respondents. For example, 77 per cent of personal domain owners and 68 per cent of small business respondents report being either aware or very aware of the scope of the cyber threats they face today.

- **All respondents express concerns about cyberattacks** – Sixty-eight per cent of personal domain owners and 77 per cent of small business domain owners report being either concerned or very concerned about being the victim of an attack.

- **Cyberattacks are having an impact across the board** – All groups surveyed are feeling the effects of various kinds of cyberattacks. Forty-one per cent of those with personal websites indicated that they knew someone who has experienced a virus or ransomware attack; 10 per cent of small business report having their website brought down by an attack within the past 24 months; and 22 per cent of larger organizations have been victimized by a DDOS attack in the past 12 months.

- **Businesses are deploying a range security solutions to protect themselves** - Both small and large businesses are deploying multiple technology solutions to protect themselves from evolving cyber threats. These include antivirus software, hardware- and software-based firewalls, email encryption, as well as solutions that block malicious queries at the DNS level.

- **Despite investments in security the bad guys are still getting in** - In the last year 19 per cent of companies report being hit by ransomware and 32 per cent report that their users had unwittingly divulged information to phishing tactics.

- **Individuals/homeowners are not adequately protected** - As a group, when we asked about their personal experience, people are underinvesting in security solutions to protect their home networks. More than a third of respondents from this group do not pay for any security protection for their computers and mobile devices, despite reporting they are aware of the risks.

22% of organizations with greater than 100 employees have experienced a user-impacting DDoS attack in the last 12 months.

SURVEY FINDINGS: PERSONAL DOMAIN OWNERS

Thirteen per cent of the people we surveyed are using their .CA domains for one or more personal websites. We asked them a range of questions designed to gauge their awareness all types of online threats, the degree to which they have been affected personally by cyberattacks to date, and what steps they are taking to protect their computers and mobile devices.

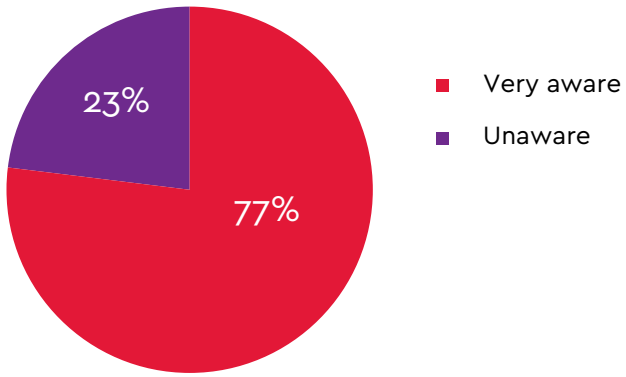
Three quarters of domain owners attuned to cyber threat risk

Overall, this group reports a high level of awareness of the scope of the online threats they are facing, with 77 per cent rating their awareness as a 7 or more on a ten-point scale, with 1 being "not aware" and 10 being "very aware". This level of awareness aligns with the findings of Canada's Internet Factbook 2017 which found that 75 per cent of Canadians were concerned about the threat of a cyberattack against organizations they know.

Nearly a quarter of respondents (24 per cent) chose 10 on the scale, indicating that they consider themselves to be "very aware" of threats posed to their computers and digital devices.

In contrast, only seven per cent of personal domain owners said they had limited awareness of the scope and type of security threats they are facing, rating their awareness level between 1 and 4 on the ten-point scale.

77% report being very aware of the types of cyber-threats they face



In addition to being generally aware of the nature of online security threats, respondents in this category also report being highly familiar with the most common types of security threats and their impacts. These include viruses, phishing scams, ransomware, and identify theft.

Scale and breadth of cybersecurity threats a significant concern among domain owners

Not surprisingly, given the generally high level of awareness about the range of security risks among this group, a significant majority of those surveyed are very concerned about being victimized by a cyberattack.

Overall, 68 per cent of respondents in this category report being concerned about the possibility of being targeted personally and financially, while 25 per cent of this total say they are "very concerned."

Indeed this concern is justified, as the number of those surveyed who report being the victim of a cyberattack is significant, particularly where it concerns computer viruses.

For example, 24 per cent of those surveyed said they were aware that a computer or mobile device belonging to themselves or a family member had been infected by a virus within the last year (excluding those asking for payment of ransom).

And when asked if they had been the victim of a ransomware attack on their computers or mobile devices in the last year, only three per cent of respondents said their device had been locked down and they had been forced to pay ransom to get it unlocked. However, when you ask them if they are aware of others who have been hit with a virus or ransomware that number jumps to 41 per cent!

In terms of phishing attacks, a large proportion of those surveyed—85 per cent—said they received phishing emails in the past year. A total of six per cent of all respondents said that this resulted in their online banking or other credentials being compromised, although 17 per cent of those surveyed in this category said they had to fix fraudulent transactions on a bank account or credit card within the last year, suggesting that hackers used other methods to steal their online banking credentials.

> 68% of individuals report being concerned about the possibility of being targeted personally and financially.

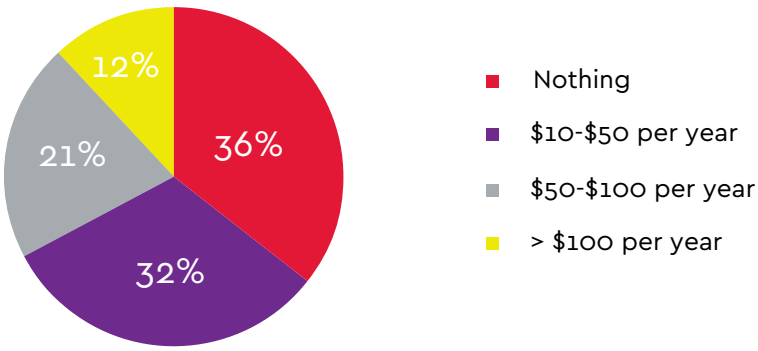
Significant gap between cybersecurity awareness and personal protection

Despite the high level of awareness of the potential impacts of security threats reported by the majority of personal domain owners, a surprisingly small number of those surveyed are making a significant investment in solutions designed to protect their personal devices and data from the growing array of potential threats.

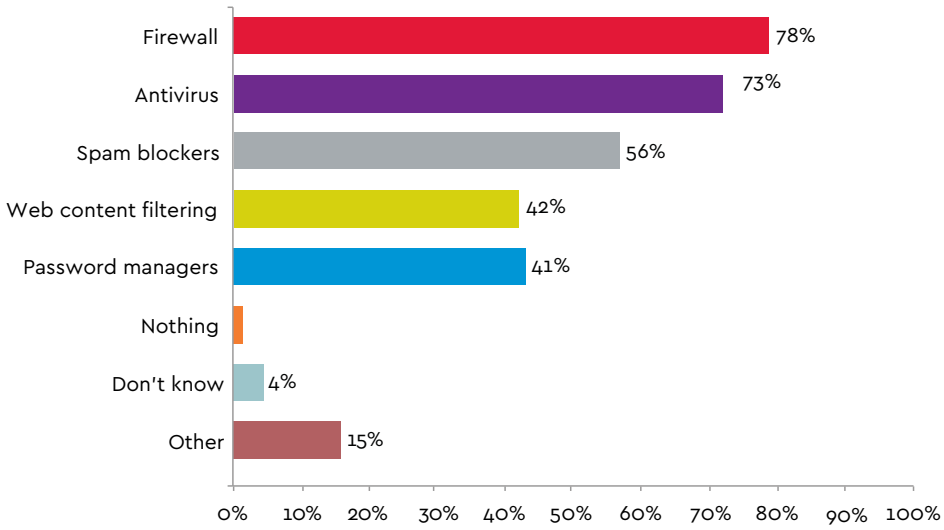
For example, 36 per cent of respondents say they are not currently investing in any form of protection for their personal computers and mobile devices.

Among those that are spending money on antivirus, firewall, and other security technology to protect their systems, the level of investment is relatively small. For example, 32 per cent of those surveyed are spending between $10 and $50 annually, 21 per cent are spending between $50 and $100, and only 12 per cent are spending over $100 annually.

How much money do you estimate you spend on antivirus, firewall, and other security technology for your home security?



What types of security software are you currently using to protect your home computers and devices (select all that apply)?



For those who have invested in security software for their home devices, the top three types of software being used by those surveyed are firewalls (78 per cent), antivirus protection (73 per cent), and spam blockers (56 per cent). Other types of security software solutions used by those surveyed includes web content filtering (41 per cent) and password managers (42 per cent).

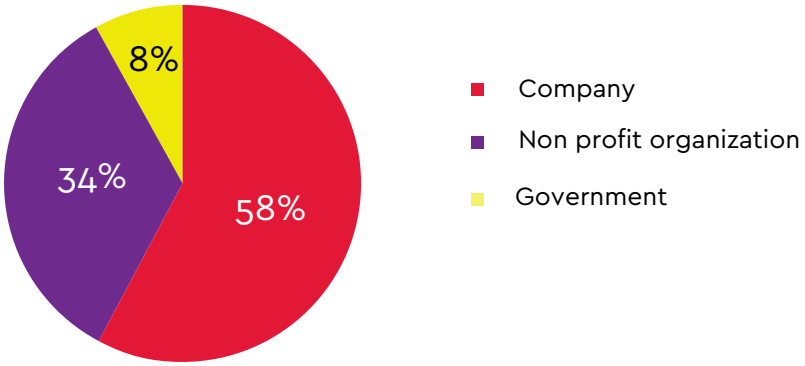
SURVEY FINDINGS: CANADIAN ORGANIZATIONS

We asked these groups a range of questions, tailored to their organization size. These questions sought their perspectives on their level of awareness of current threats, the impact they are seeing from these threats, and the steps they are taking to deal with them.

Survey findings: Canadian organizations

In addition to collecting responses from personal domain owners, we also surveyed people who own one or more .CA domains that they use exclusively for business purposes. This includes small businesses with 100 or fewer employees and larger organizations with more than 100 employees. Among the larger organizations, 58 per cent were companies, 34 per cent were not-for-profit organizations, and eight per cent were government organizations.

Types of organizations with 100 employees responding to survey



We asked these groups a range of questions, tailored to their organization size. These questions sought their perspectives on their level of awareness of current threats, the impact they are seeing from these threats, and the steps they are taking to deal with them, including the IT security solutions they currently use and their level of investment in these solutions.

Of those surveyed in the small business category, the majority of respondents (72 per cent) report that they have primary responsibility for IT operations and security for their business, while 11 per cent say they rely on internal technical resources, and 17 per cent use an external managed service provider or IT contractor.

Among those working for larger organizations, which include private sector, not-for-profit and government organizations, 90 per cent say they are involved in the IT security decision-making process.

Cyber threats a major concern for Canadian businesses

Like their counterparts operating personal websites on their .CA domains, business domain owners likewise express high levels of concern about the potential impact of cyberattacks on their operations.

Overall, 77 per cent of small businesses respondents rate their level of concern as a 7 or higher on a ten-point scale, with 1 being "not concerned" and 10 being "very concerned".

A significant proportion of respondents—about one fifth of the total—rated their concern at the highest level on the ten point scale, indicating that they consider themselves to "very concerned" about threats cyberattacks pose to their business.

Among larger organizations, respondents say they are worried about the impact of phishing and ransomware in their organizations, with 16 per cent saying they are "somewhat worried" about ransomware, and another 57 per cent saying they are worried or very worried about it, rating it between 7 and 10 on the ten point scale.

Phishing is also a significant concern among larger organizations, with 18 per cent saying they are "somewhat worried" about it, and another 55 per cent saying they are worried or very worried about it.

The level of concern among Canadian businesses is justified by the research conducted in Canada's Internet Factbook 2017 which found that 44 per cent of Canadians were unlikely to continue making purchases from an online business following a major cyberattack.

> Despite all the headlines, only 57% of organizations rank themselves as worried about ransomware.

Impact and frequency of cyberattacks is increasing in Canada

As is the case with personal websites, the impact of cyberattacks in a Canadian business context is a major cause for concern. Among larger organizations in particular, these attacks are increasing in frequency daily.

Twenty-two per cent of respondents from organizations with greater than 100 employees—nearly a quarter of those surveyed in this category—said theey had been the victim of a DDoS attack in the past year that negatively impacted business performance.

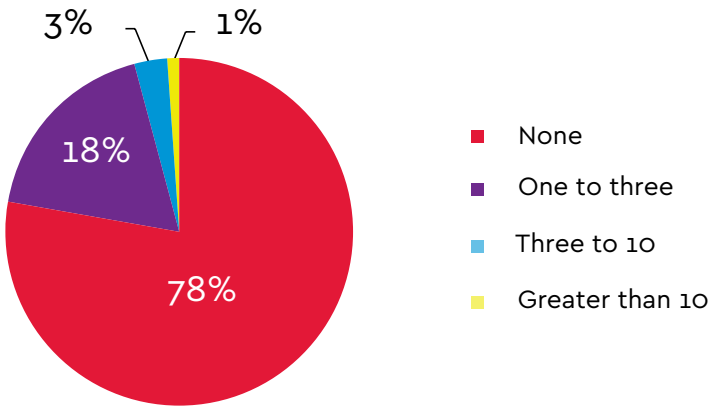
Overall, 17 per cent said their organization had experienced between one and three DDoS attacks, three per cent had experienced between three and ten attacks, and two per cent had experienced more than ten attacks.

It's a similar story for ransomware, with 19 per cent of those surveyed in this category saying their organization had been the victim of a ransomware attack. Seventeen per cent of organizations report being victimized in this manner between one and three times, while another two per cent reported a breach between three and ten times.

Phishing attacks are also a major cause for concern among large organizations, with 32 per cent reporting that users within their organization had unwittingly divulged important information to hackers within the last year.

> 19% of organization report having experienced a ransomware attack.

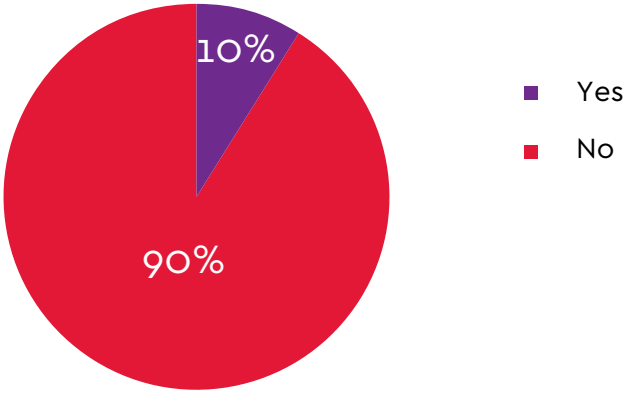
In the last 12 months how many times have you experienced a DDoS attack that impacted performance?



The results among the Canadian small businesses we surveyed were similar. The number of small businesses impacted by cyberattacks, while less than half the rate reported by large organizations, is nonetheless significant and a cause for serious concern.

Ten per cent of those surveyed in the small business category report having their website brought down by a website hack or cyberattack within the past 24 months.

In the last 24 months, has your website been hacked or otherwise brought down through an actual or suspected cyberattack?

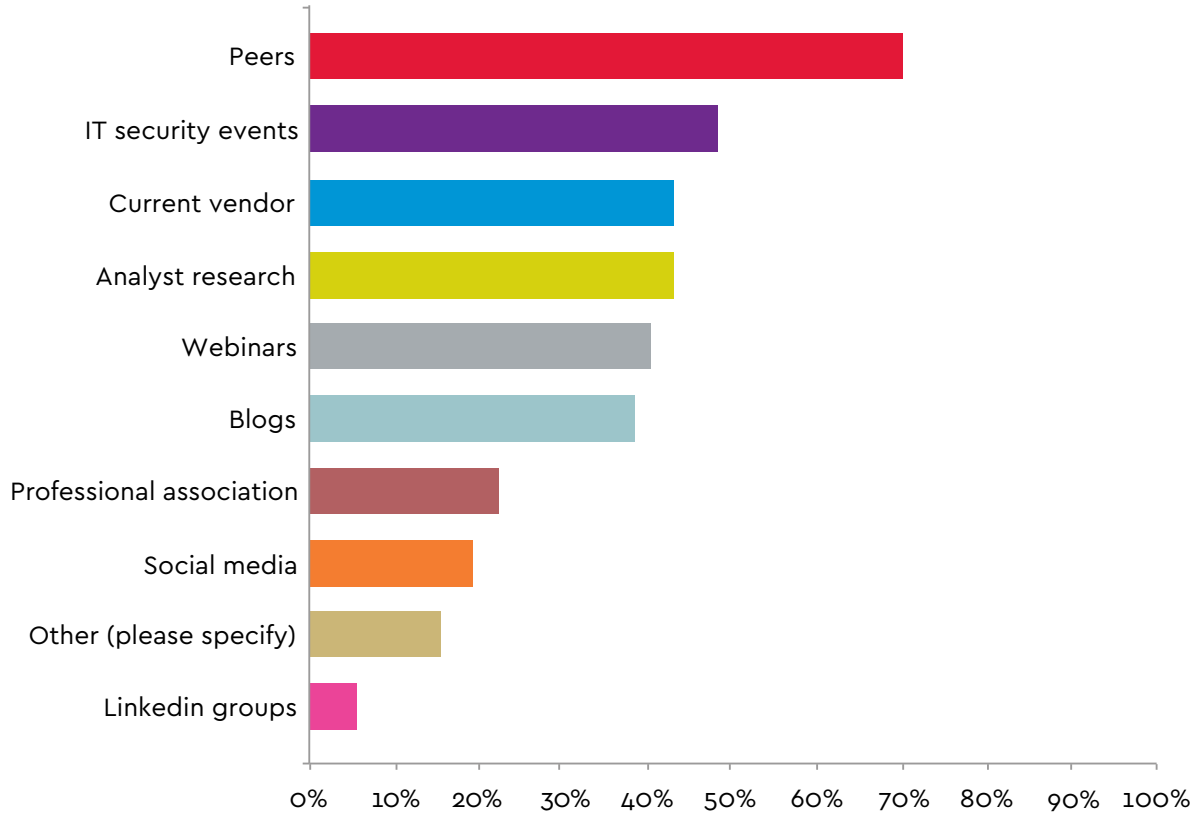


Canadian businesses see their peers in the cybersecurity community as trusted resource

In terms of where IT professionals go to educate themselves on matters related to IT security services, respondents from small businesses and larger organizations alike indicated their peers were their go-to source. We excluded general search engine research from this question to understand where else organizations typically look.

And while small businesses looked to their current vendor (35 per cent) and blogs (32 per cent) as their second and third choices, respondents from larger organizations listed IT security events (48 per cent) and their current vendor (43 per cent) as their second and third choices respectively.

Where do organizations with >100 employees go to get the information IT security services? (Select your top 3)



Canadian businesses recognize the value of defence in depth

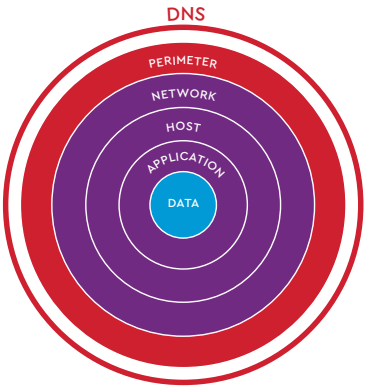
Canadian businesses, both large and small, recognize the value of layered cybersecurity protection and are investing in a variety of IT security solutions to protect themselves—a concept called defence in depth.

The term defence in depth has its origins in the military, where layers of defense—each with different capabilities—protect each other, and the core. In the case of a DNS firewall, it exists as a first layer of protection outside the organization and might be compared to air cover over a battlefield. It has a unique perspective, vital early threat detection capabilities, and can respond to a potential compromise before it even reaches your network.

At the individual device level, small businesses report they are using several different types of solutions for protection. Eighty-four per cent report using antivirus software, while 61 per cent say they are using traditional hardware-based firewalls and 54 per cent reporting using software-based firewall solutions.

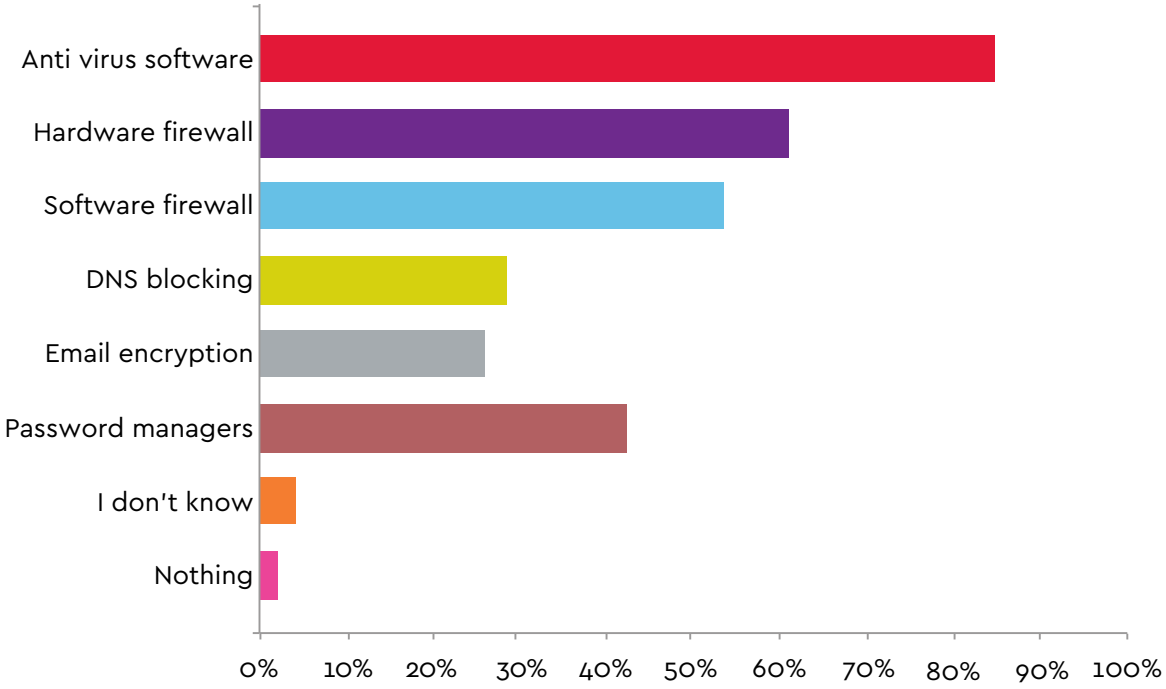
Other systems small businesses are deploying include password managers (42 per cent), email encryption (26 per cent) and cloud-based systems, which block malicious queries such as malware and phishing links (29 per cent).

A majority of larger organizations indicate that they are using security solutions that block malicious queries at the DNS level with 60 per cent of those surveyed say they are providing malware and phishing protection using this method. Of these, a surprising 55 per cent say that they are blocking content (also called web filtering) using this method as well. We expect that this type of blocking is done by a combination of on-site recursive servers, traditional firewalls and cloud-based DNS firewalls.

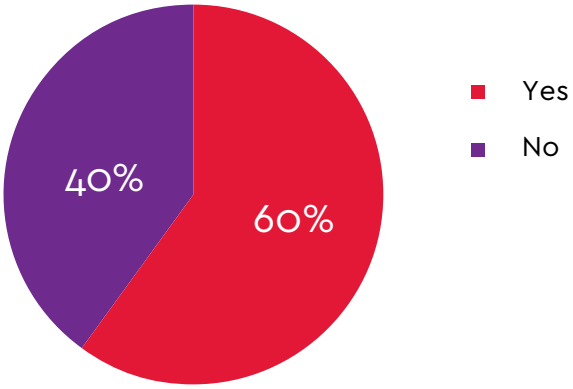


The DNS provides a layer of protection outside the organization using recursive servers in the Internet

What software or hardware do you use on your computers and devices? (Select all that apply)



Do you use any tools that provide malware and phishing protection by blocking queries at the DNS level?



Conclusion

Our first Cybersecurity survey of .CA registrants that have business-type domain name registrations shows that Canada is not immune to the cyber threats facing organizations in other countries. They are very concerned about the risk and are investing in several different solutions to help mitigate it.

Despite this, they survey shows that the bad guys keep breaking-in and so continual improvement in security is critical to any organization that relies on technology for their business.

CIRA can help you discover malware you didn't know you had with D-Zone DNS Firewall.

CIRA offers a Canadian solution to help with the growing malware problem. With nodes located inside Canada and data privacy and sovereignty built-in, it provides a simple yet effective layer of protection for Canadian organizations. The results have shocked even us, with almost every new customer discovering malware they didn't know they had as it tried to call out to its command-and-control servers. Try D-Zone DNS Firewall today and see what you have been missing.

Learn more and try today by visiting:

cira.ca/cybersecurity/firewall