paloalto NETWORKS | CYBERSECURITY PARTNER OF CHOICE

2023 Palo Alto Networks Canada Ransomware Barometer

Executive Summary

To evaluate the current state of the ransomware threat landscape in Canada, Palo Alto Networks commissioned the Angus

Reid Group to analyze the impact that ransomware has had on Canadian organizations with 100+ employees.

Since the 2021 report, the threat landscape in Canada has evolved as more and more businesses recognize the need to be proactive and have the right security strategy in place to prevent attacks, or to lessen the impact of a successful attack.

Today's threat actors do not discriminate against specific industries and sizes of businesses, so businesses across Canada cannot take a "wait and see" approach.

The study found that while the volume of ransomware attacks has remained relatively consistent among mid-market companies (100-1,000 employees), the average ransom paid has increased significantly to more than $1.130 million CAD – an increase by almost 150% in two years. Additionally, the average ransom demanded saw a steep rise by 102% to C$906,115 in 2023 up from C$449,868 in 2021.

Of the Canadian businesses hit by ransomware – 35% in 2023 compared to 37% in 2021 - only 34% of organizations paid the demand, compared to 45% in 2021. The decrease in the number of attacks may very well be the result of more organizations taking a proactive approach in modernizing and updating their security infrastructure and refusing to pay ransoms.

The long-term effects of ransomware attacks continue to be a significant challenge for Canadian organizations if they're a victim. As with the previous study, more than half (58%) say that it took more than a month to recover, however, one-quarter (24%) said that it took longer than four months, up from 17% in 2021.

Ransomware gangs continue to be a threat to Canadian organizations, but businesses are investing in the right strategies and training to improve their cybersecurity posture so they are not the next victim of cyber extortion.

Key Findings

The average ransom payment for Canadian organizations jumps to more than $1 million CAD

The study found that while the volume of ransomware attacks has slightly decreased, the average ransom paid has increased significantly to more than $1.130 million CAD – an increase by almost 150% in two years. Additionally, the average ransom demanded saw a steep rise by 102% to C $906,115 up from C$449,868 in 2021. A majority of businesses that paid ransoms (53%) paid more than $500,000 CAD, up from 29% in 2021.

While the amount demanded and paid has increased dramatically, there has been a slight decrease in the percentage of organizations impacted by a ransomware attack – 35% in 2023 compared to 37% in 2021.

Organizations in Quebec appear to be the most targeted in Canada with 43% of respondents saying they were hit with a ransomware attack. Organizations in British Columbia are most likely to pay ransoms as 42% of those hit with ransomware paid, followed by Quebec (35%) and Alberta (31%). Conversely, organizations in Atlantic Canada (5%) and Manitoba (8%) were least likely to pay ransoms.

Businesses in the manufacturing sector appear to be targeted significantly more than other sectors with 47% of respondents saying they have been hit with an attack; followed by construction (38%) and healthcare + pharma (35%) sectors. Interestingly, only 18% of organizations in the public sector have been impacted by ransomware.

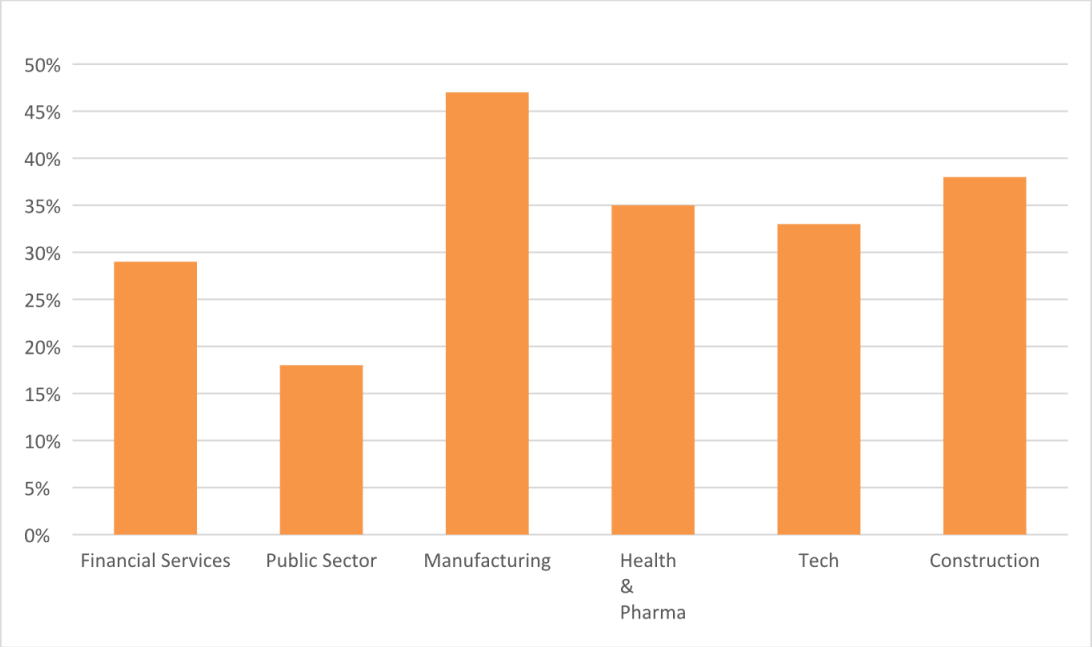

Figure 1: Percentage of organizations hit by ransomware by sector (2023 data from the Angus Reid Group)

The long-term effects of ransomware attacks continue to be a significant challenge for Canadian organizations if they're a victim. As with the previous study, more than half (58%) of affected mid-market companies say that it took more than a month to recover, however, one-quarter (24%) said that it took longer than four months, up from 17% in 2021.

The long-term effects of ransomware attacks continue to be a significant challenge for Canadian organizations if they're a victim. As with the previous study, more than half (58%) of affected mid-market companies say that it took more than a month to recover, however, one-quarter (24%) said that it took longer than four months, up from 17% in 2021.

AI technologies have increased the threat level for many organizations

The study found that Canadian IT decision-makers are concerned with the potential threat artificial intelligence (AI) poses to their organizations. More than two-thirds of respondents (69%) believe the emergence of more AI technologies has increased the threat level to their organizations. Conversely, only 2% of respondents believe AI will decrease the threat to organizations.

The top perceived threats that AI technologies pose to organizations' cybersecurity include automated phishing (21%), data privacy risks (21%) and advanced cyberattacks (19%).
In addition to AI, the survey found that the cyber threats that respondents are most concerned about have remained relatively consistent since 2021 with data breaches (68%), phishing attacks (60%) and ransomware (53%) remaining the top three.

Top AI threats to organizations

- Automated phishing 21%
- Data privacy risks 21%
- Advanced cyberattacks 19%
- More bad threat actors 12%
- Dependency on AI 8%
- Algorithm bias 7%
- False positives / negatives 7%
- Insider threat detection 5%

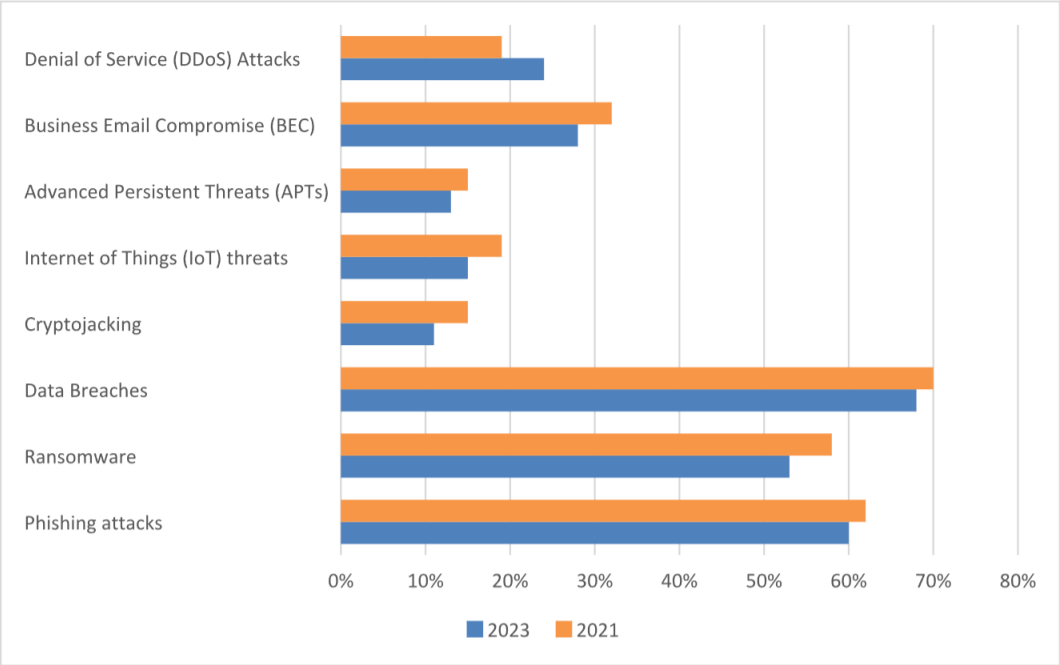

Figure 2: Year-to-year comparison of top cyber threats (2023 and 2021 data from the Angus Reid Group)

For the public sector, more than three quarters of respondents (80%) believe data breaches to be their top threat, while 78% of healthcare and pharma decision makers considered phishing attacks the top threat to the sector.

Top cyber threats by sector

- Financial Services – Data Breaches 69%
- Public Sector – Data Breaches 80%
- Manufacturing – Phishing Attacks 64%
- Health & Pharma – Phishing Attacks 78%
- Technology – Data Breaches 71%
- Construction – Data Breaches 60%

Companies are investing in technology and their workforce to stay protected

In the past two years, the research found that organizations are taking a more proactive approach to improving their cybersecurity posture. In addition to the high-profile breaches and ransomware attacks, the vast majority of IT decision makers (81%) are also concerned about an increased difficulty in staying protected against cyberattacks by adopting a hybrid / remote work model.

To improve security, one-in-five organizations (20%) have increased their spending on cybersecurity software significantly for better protection, while a majority (51%) have increased spending somewhat. Organizations are planning on taking significant actions to improve their organizations cybersecurity posture in the coming year compared to 2021.

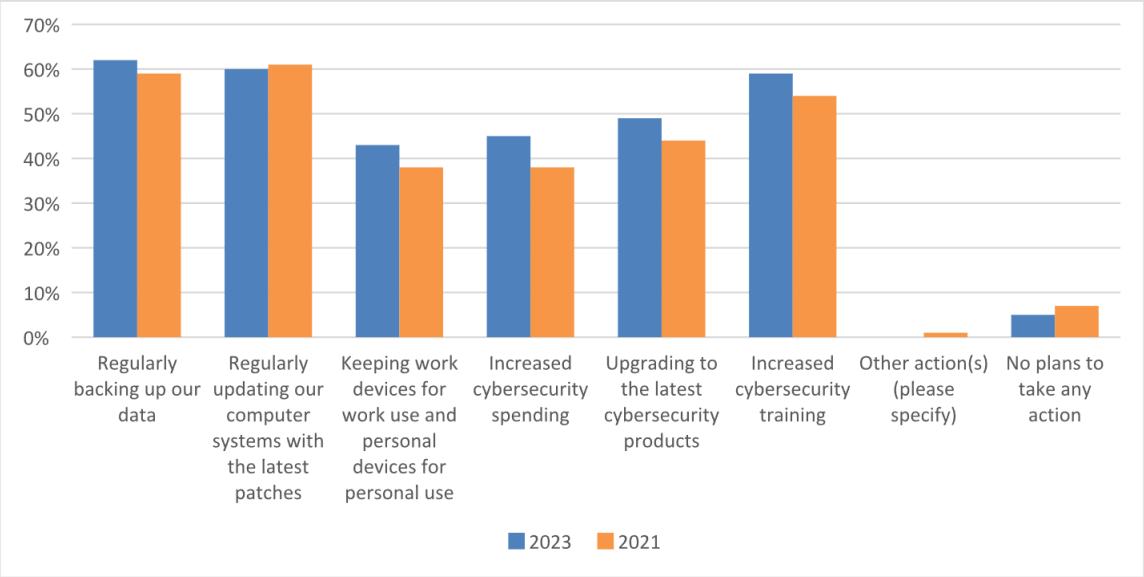

Figure 3: Year-to-year comparison of top actions organizations are taking to improve their cybersecurity posture (2023 and 2021 data from the Angus Reid Group)

In parallel, organizations who feel their employees lack adequate understanding of the issues recognize the importance of cybersecurity training with almost half (49%) updating or implementing new cybersecurity training for its workforces to better protect against the latest cyberthreats, up from 38% in 2021.

As a result of the improved training, leaders believe employees have better understanding of cybersecurity best practices to self-manage while working remotely today (76%) than two years ago (72%). The vast majority of leaders (86%) also believe cybersecurity fundamentals should be a core competency for employees going forward.

Businesses expect the Federal Government to do more to help protect businesses against the latest cyber threat

While businesses are doing their share to help protect themselves by implementing the right cybersecurity strategy and employee training, they also believe the Government has a significant role to play too.

More than two-thirds of IT decision makers (70%) believe the federal government has a responsibility help businesses protect against the latest threats. Currently, only one-quarter (25%) believe the government is doing enough to help businesses protect themselves against cybersecurity threats.

More than half of respondents in Atlantic Canada (52%) believe the government is not doing enough to help businesses protect themselves against cybersecurity threats, followed by Ontario (48%).

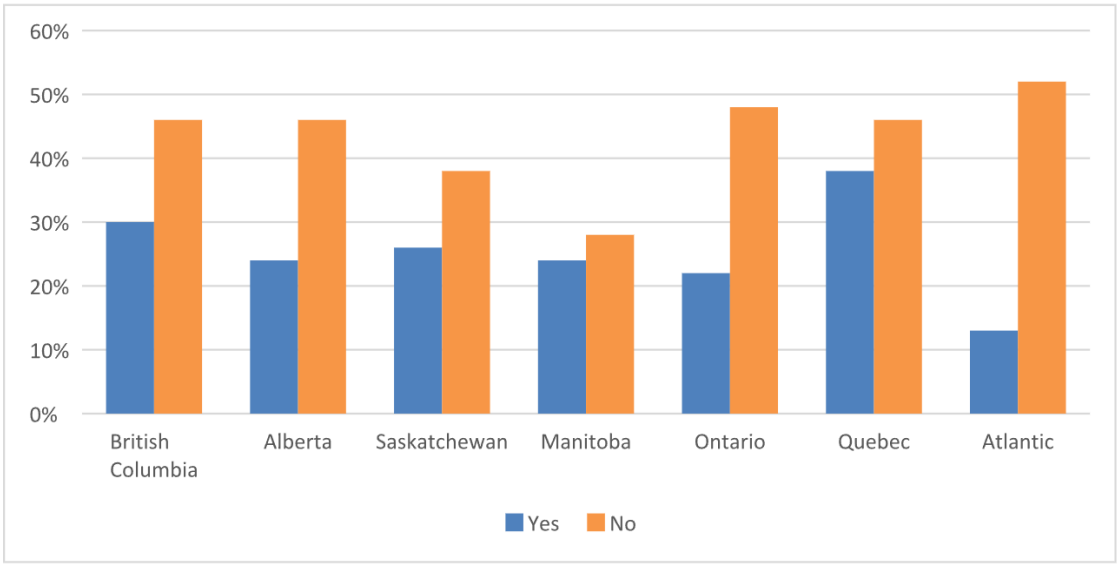

Figure 4: Provincial breakdown on whether the Federal Government is doing enough to protect businesses from latest cyber threats (2023 data from the Angus Reid Group)

Currently, only one in five (20%) IT decision makers believe Canadian institutions - both public and private sector - are well prepared for a cyber threat from a nation-backed threat group, while more than a third (34%) believe we're not.

When asked what actions can be taken to help improve Canadians cybersecurity posture, almost three-quarters (74%) believe cybersecurity compliance for organizations should be mandated by the federal government.

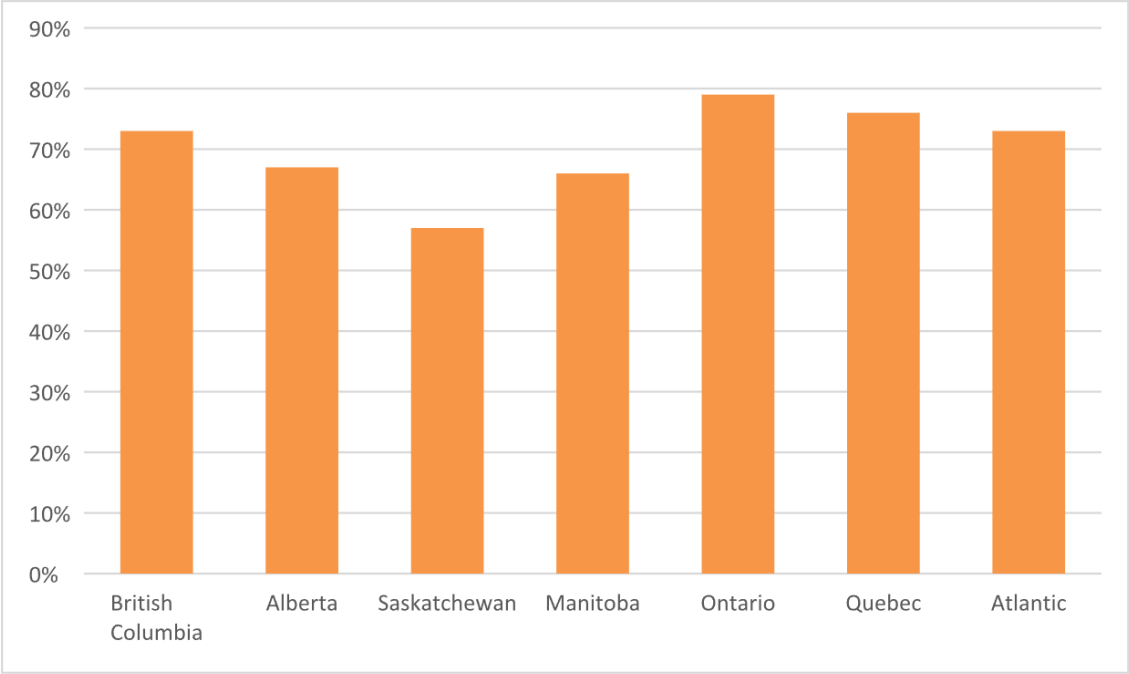

Figure 5: Provincial breakdown that agree that cybersecurity compliance should be mandated by the Federal Government (2023 data from the Angus Reid Group)

An overwhelming majority (92%) also believe cybersecurity education programs should be part of high-school curriculum to prepare young Canadians.

Security Best Practices

Ransomware continues to be a major threat to organizations in Canada and around the world. While the headlines typically focus on attacks against large organizations, small businesses are increasingly targets by threat groups, which can be especially devastating to organization's that don't have the knowledge and resources to withstand a major attack.

As hybrid work has become the new normal for many organizations, cybersecurity education and training becomes incredibly valuable.

Tips to protect against ransomware attacks

1. Beware of phishing emails — if you think you received one, report it.

Ransomware is primarily spread through phishing emails that contain malicious attachments. Disguised as legitimate communication, the fraudulent email tricks the recipient into responding by enticing them to click a link, open an attachment or directly provide sensitive information.

Phishing emails have become one of the most prevalent methods of ransomware because they're simple to deploy. Adding to the ease of deployment is the availability of low-cost phishing kits that include website development software, coding, spamming software and content that can be utilized by hackers to create convincing websites and emails.

2. Update devices with the latest software patches.

Hackers like to take advantage of software vulnerabilities to spread ransomware. Software vulnerabilities are weaknesses in a software program.

A software patch helps to solve this problem by addressing security vulnerabilities in a software program, so a hacker is unable to exploit them. Most of the time, software patches will be issued automatically by a vendor, so take advantage of them. Other times, you will need to install a software patch manually; make sure to check whether you have the latest patches. If you don't, go directly to the vendor's website and install them.

3. Restore any encrypted files with backups.

If you're the victim of a ransomware attack, don't panic. Check whether you have backed up your files. If you have, restore from your latest backup. This is the fastest way to get your files back. If you haven't backed up your files, then you may need to consider your files lost.

The most common question we get with ransomware attacks is: "Should you pay the ransom?" Unfortunately, there's not a one-size-fits-all scenario. All victims of ransomware attacks are left with difficult decisions. Seek the advice of a professional who can help you determine what to do.

What we advise is to prepare for a ransomware attack. There are security tools and technologies available that can help prevent a ransomware attack and protect you from making that difficult decision.

Methodology

In partnership with Palo Alto Networks, the Angus Reid Group conducted an online survey among a representative sample of 1,000 business and IT decision-makers in organizations with 100+ employees, in the week of November 6, 2023. The respondents are members of the Angus Reid Business Advisory Network. For comparison purposes only, this sample plan would carry a margin of error of +/- 3.1 percentage points 19 times out of 20 for business leaders.

About Angus Reid Group

Angus Reid is Canada's most well-known and respected name in opinion and market research data. Offering a variety of research solutions to organizations across North America, the Angus Reid Group team connects technologies and people to derive powerful insights that inform your decisions. Data is collected through a suite of tools utilizing the latest technologies. Prime among that is the Angus Reid Forum, an opinion community consisting of engaged residents across the country who answer surveys on topical issues that matter to everyone. Within this community sits the Business Advisory Network, a highly engaged community of B2B professionals comprised of decision makers in the financial sector, IT professionals, education, trades and other B2B sectors. This community is diverse, accurate and delivers reliable business intelligence for your organization's biggest decisions.

About Palo Alto Networks

Palo Alto Networks is the world's cybersecurity leader. We innovate to outpace cyberthreats, so organizations can embrace technology with confidence. We provide next-gen cybersecurity to thousands of customers globally, across all sectors. Our best-in-class cybersecurity platforms and services are backed by industry-leading threat intelligence and strengthened by state-of-the-art automation. Whether deploying our products to enable the Zero Trust Enterprise, responding to a security incident, or partnering to deliver better security outcomes through a world-class partner ecosystem, we're committed to helping ensure each day is safer than the one before. It's what makes us the cybersecurity partner of choice.

At Palo Alto Networks, we're committed to bringing together the very best people in service of our mission, so we're also proud to be the cybersecurity workplace of choice, recognized among Newsweek's Most Loved Workplaces (2023, 2022, 2021), with a score of 100 on the Disability Equality Index (2023, 2022), and HRC Best Places for LGBTQ Equality (2022). For more information, visit www.paloaltonetworks.com.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

parent_ds_title_date