CDW PEOPLE WHO GET IT®

MANAGING SECURITY IN CANADA

How the pandemic has shifted our perceptions of the workplace and its security.

The ongoing pandemic created an air of uncertainty across Canada and globally as organizations of all sizes had to rapidly adapt their operations for much longer than they originally anticipated. Amid the evolving workplace landscape, the cybersecurity posture of organizations has similarly transitioned from office-centric to location-agnostic.

Recently, CDW commissioned a survey with Angus Reid to examine the sentiment of IT professionals regarding the cybersecurity posture at their organizations. The survey looked at organizations of all sizes and the various security solutions or tools they used before and during the pandemic, as well as their thoughts on the future of cybersecurity.

While working from home is by no means a new trend, the pandemic acted as a forced accelerant for Canadian organizations. Business continuity may have been the focus in the early stages of this transition, but security quickly became top of mind as IT professionals realized that network infrastructure needed to change to meet the new demands of an expanded threat landscape. Canadians' home lives became a simultaneous combination of work, childcare and free time — often on the same network. Unsurprisingly, Canadians' home routers were not designed to support constant professional and personal day-to-day activity.

To address remote work, many organizations adopted new tools to enable employee communication and ensure business continuity. While positive, these new tools exposed organizations to new cybersecurity threats that existing infrastructure was often not prepared to address. The pandemic served as a wakeup call for many organizations and IT professionals, who realized the workplace they were accustomed to before the pandemic is unlikely to return in the near-term. Relying on the infrastructure, cybersecurity tools and policies of the past is no longer an option as Canadian organizations look to safeguard critical data in an increasingly virtual future.

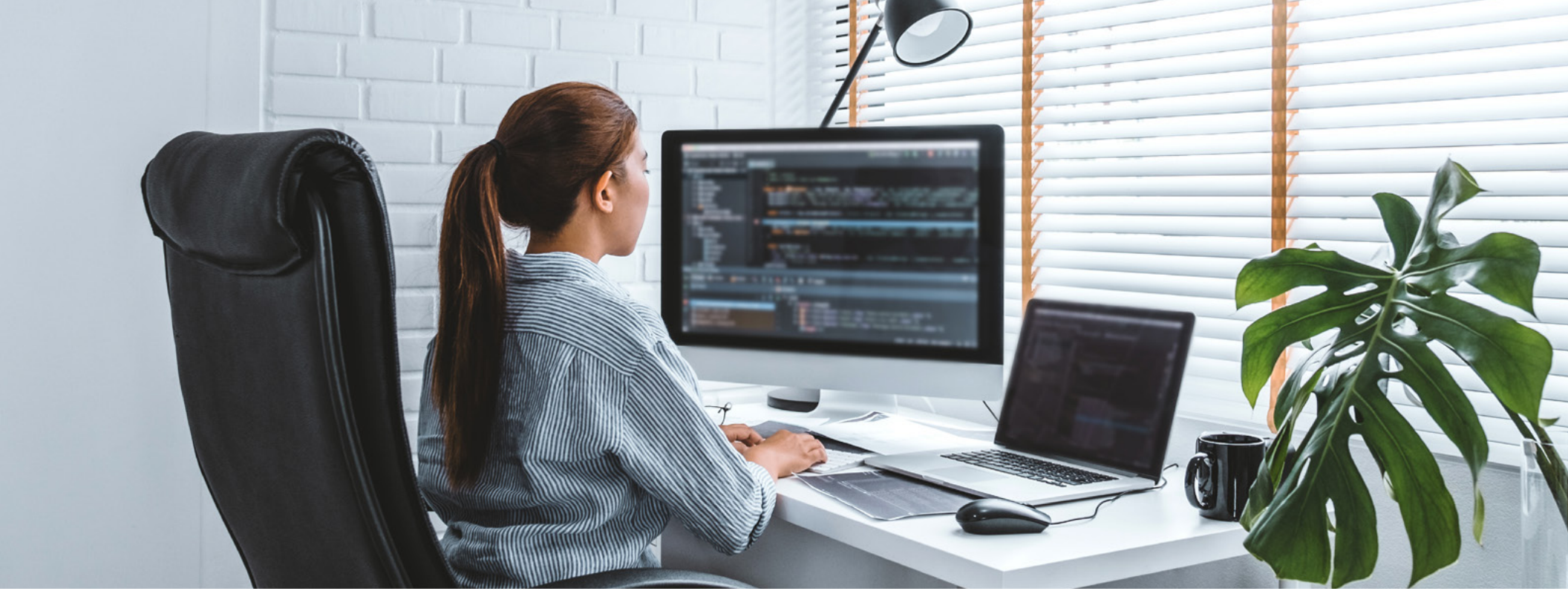
CDW's Key Findings:

- In the transition to remote work, 50 percent of organizations experienced a minor service interruption for employees, while 17 percent had some interruption but adapted to working from home.
- When it comes to cybersecurity solutions and/or tools, our survey found that 48 percent of respondents are reaping most of the benefits, while 22 percent said they are benefiting from some, but not all.
- Software as a service (SaaS) increased in usage: 29 percent of organizations used these tools for all of their work prior to the pandemic, increasing to 35 percent during. This adoption is expected to continue, as 37 percent of respondents said their organization plans to leverage SaaS for all of their work in the future
- The pandemic resulted in a growing number of organizations using multi-factor authentication (MFA) to secure their devices, as 61 percent of respondents adopted this method amid the pandemic, compared to 54 percent who used it prior
- IT professionals' confidence in their cybersecurity posture has and is anticipated to remain positive: 75 percent of IT professionals noted they were confident or very confident in their organization's cybersecurity posture prior to COVID-19, compared to 72 percent amid the pandemic and 74 percent looking ahead
- IT professionals and the organizations with whom they work are appreciating the value of reviewing their cybersecurity posture on a more regular basis. According to our survey, only 20 percent of organizations examined, tested and fixed any gaps in their cybersecurity framework every two weeks. During the pandemic, 25 percent of respondents indicated the same
- Concerningly, 14 percent of IT professionals said their organization does not plan on conducting any cybersecurity training in the future to help employees identity potential threats. Thankfully, 12 percent plan to conduct monthly training, while 21 percent plan to quarterly.

What is driving the change?

Many of today's organizations are stuck in a limbo between the way we worked before the pandemic and what office landscapes will demand when COVID-19 eventually subsides. Amid the new reality, many may reconsider the need for a physical office at all, while some long for the office landscape of the past to return. Our survey found that only nine percent of respondents believe employees at their organization will be expected to return to work full time when it is deemed safe to do so, while a net 69 percent will remain either entirely remote or have a mix of in-office and remote.

Organizations need to realize that employees have grown accustomed to working from home and may not want to go back to always being in one physical location. Our survey found that the investment in cybersecurity tools or solutions when looking at pre-pandemic versus during remained largely flat or increased. Additionally, IT professionals anticipate their spend on solutions and tools to increase when looking to the future compared to their spend prior to the pandemic to improve security posture. For example, multifactor authentication (MFA) saw a 10 percent increase in anticipated spend, followed by cloud security (8 percent) and artificial intelligence (AI) and machine learning (ML) (7 percent). These figures indicate that IT professionals are seeing the benefit of the solutions they're using and recognize the growing importance of investing in appropriate cybersecurity tools or solutions.



The challenging transition to working from home

It's no surprise that the shift to remote work was widespread due to COVID-19. However, prior to the pandemic, a net 86 percent of all respondents were already permitted to work from home in some capacity on an exclusive, regular or intermittent basis. Enterprises had the highest proportion of employees with the ability to work from home in some capacity, with 90 percent indicating this was an option. This was followed by large organizations at 87 percent, medium sized businesses at 83 percent and small businesses at 80 percent. During the pandemic, 58 percent of survey respondents cited having the option to work from home most or all of the time. This transition has not been entirely smooth for most organizations however, as nearly three-quarters (70 percent) of organizations experienced some kind of service interruption for employees.

While organizations of all sizes and sectors had a service interruption, severity varied by business size. The survey found that 54 percent of business and professional services organizations had a minor interruption of service but quickly enabled their employees to work from home, compared to only 33 percent in healthcare who said the same. Compare this to 36 percent in business and professional services who had no interruption of service for employees, while only 16 percent in government said the same.

Cybersecurity and cloud, today and tomorrow

With the shift to remote came the need for additional cybersecurity measures. Choosing the correct solutions to suit the needs of the organization was, and continues to be, crucial in optimizing security in a virtual landscape and ensuring business continuity. Nearly half (48 percent) of respondents said their organization is reaping most of the benefits of the cybersecurity solutions and/or tools it's currently using, while 27 percent say they are fully benefiting. This is promising but reveals that one quarter (25 percent) of Canadian organizations have room to improve in realizing the potential of their cybersecurity tools or solutions.

The adoption of cloud-based technology was prevalent in most organizations both before and during the pandemic. Nearly three-quarters (73 percent) of respondents indicated that the use of cloud-based technology has improved their organization's cybersecurity posture. SaaS cloud technology experienced a renaissance during the course of the pandemic and is showing a clear value-add to organizations of all sizes. Prior to the pandemic, roughly one third of organizations all sizes used SaaS for all work (28 percent of small organizations, 29 percent of medium, 31 percent of large and 30 percent of enterprise). Looking to the future, the usage of SaaS for all workloads increased significantly across the board, with 35 percent of small organizations indicating they will use SaaS holistically, 35 percent of medium, 42 percent of large and 38 percent of enterprise-level organizations.

Similarly, infrastructure as a service (IaaS), saw slight growth among Canadian organizations. Prior to the pandemic, 18 percent of organizations used IaaS for all work (14 percent of small organizations, 17 percent medium, 18 percent large and 20 percent enterprise). Looking to the future, IaaS adoption is expected to continue as 22 percent of small organizations anticipate using it for all work, while 21 percent of medium organizations, 24 percent of large and 25 percent of enterprise organizations said the same.

The use of artificial intelligence (AI) and machine learning (ML) for cybersecurity purposes also saw adoption during the pandemic. Our survey found that 19 percent of respondents indicated their organization leverages AI/ML during the pandemic – a slight increase from the 17 percent who utilized it pre-pandemic. AI and ML for security purposes and penetration testing are both expected to increase in adoption in the future compared to pre-pandemic levels, as both tools saw an 8 percent jump in anticipated use. MFA also saw growth in adoption as 61 percent of organizations use this security measure during the pandemic, compared to 54 percent of organizations before COVID-19. In addition, the prevalence of password managers grew three percent amid the pandemic, while managed detection services grew four percent and software, such as email, anti-spyware and antivirus, saw a decrease of one percent.

Organizations are expected to continue leveraging these tools in the future as one quarter of respondents (25 percent) will continue using AI/ML for security purposes, while just over two thirds (64 percent) will continue using MFA, 41 percent will leverage penetration testing and 80 percent will use firewalls. While this growth does appear gradual, it highlights that today's organizations appreciate the improved security that these cybersecurity and cloud-based tools can bring to organizations. This will help ensure business continuity while providing employees a secure and flexible landscape to collaborate in – no matter where they are.

Familiar barriers will continue

Organizations of all sizes face the same challenges when looking to invest in their cybersecurity infrastructure. The different forms of resistance faced by IT professionals from within their organization when exploring investment in cybersecurity tools or technology remained largely flat when comparing organizations' experiences before and during the pandemic.

Budget constraints remain the most common form of resistance (46 percent pre-pandemic, 45 percent during). The perceived complexity of projects similarly continues to be a factor, as 27 percent of respondents noted this as a barrier both before and during COVID-19. In the future, nearly half of respondents (48 percent) anticipate budget constraints will be the top barrier, followed by perceived complexity of projects (24 percent) and scale of data (17 percent). The consistency of budget as a barrier is concerning, particularly amid the pandemic as organizational security needs rapidly changed and will continue to in the future. Organizations need to recognize that security is a necessary expense to ensure business continuity and the safety of its critical information.

Don't forget employee training

While the majority of IT professionals maintain similar levels of confidence in their organizations' cybersecurity posture today compared to prior to the pandemic, there is always room to improve. Thankfully, one quarter (25 percent) of respondents now review their cybersecurity posture every two weeks to assess cybersecurity gaps – a five percent increase in frequency compared to before the pandemic. Concerningly, despite the shift in organizational infrastructure and increase of cybersecurity incidents broadly, seven percent of Canadian organizations admitted to reviewing their cybersecurity posture less than once per year.

Beyond increasing regular monitoring, Canadian organizations are also leveraging focused testing to identify and address gaps in cybersecurity posture. Prior to the pandemic, one third (33 percent) of organizations leveraged penetration testing to optimize their perimeter. As a result of the pandemic, penetration testing will be used by two fifths (41 percent) of organizations across all sizes.

While having the appropriate cybersecurity solutions or tools in place and scheduling regular network reviews and testing is important, employees remain an organization's first line of defence in preventing a cyberattack. Our survey found that organizations increased their regular employee training across the board. One tenth (12 percent) of organizations now train employees on a monthly basis (compared to 10 percent prior to COVID-19), while one fifth train on a quarterly basis (compared to 19 percent). Concerningly, 17 percent of respondents said their organization still only conducts cybersecurity training during the onboarding process, while 14 percent noted their organization does not plan on holding employee training in the future at all. Not only is regular training important as solutions and technology advance, but training should be reflective of our new environment and the unique cybersecurity risks facing employees at their organization.

WHAT WE'RE SEEING IN DIFFERENT INDUSTRIES

Government

Nearly two thirds (61 percent) of IT professionals indicated government employees rarely worked from home prior to the pandemic. This is significantly higher than the average of 46 percent among all industries. In addition, 24 percent were very concerned about working with third party organizations regarding the access and availability of sensitive data prior to COVID-19, the highest among all respondents. Looking into the future, 27 percent of government organizations remain concerned about working with third party organizations, still the highest among all respondents.

IT professionals in government did note an anticipated increase in adoption of select cybersecurity tools. Our survey found that 27 percent expect to use AI/ML for security in the future — an increase of 12 percent from pre-pandemic adoption. Similarly, MFA is expected to be used by nearly two thirds (62 percent) of respondents — an increase of 9 percent compared to before the pandemic. Cloud security was only used by 30 percent of government respondents before the pandemic, the lowest among all sectors, but is expected to be used by nearly half (45 percent) of government organizations in the future. While this is still the lowest of all sectors, it marks an encouraging increase in adoption.

Healthcare

During the pandemic, 45 percent of healthcare respondents said employees worked from home most of the time which is, unsurprisingly, the lowest among all sectors. In terms of cybersecurity tools and solutions, public key infrastructure (PKI) and penetration testing are rarely used in this industry, highlighting a clear opportunity to improve as the healthcare sector has seen an unprecedented demand for its services. Both prior to and amid COVID-19, only 13 percent of healthcare organizations leveraged PKI — the lowest among all sectors for both periods. Similarly, penetration testing was leveraged by 16 percent of organizations prior to the pandemic, while 24 percent plan to leverage it in the future.

Despite underutilization of these solutions, 26 percent of healthcare organizations conducted cybersecurity posture reviews every two weeks prior to the pandemic, which is tied for second most among industries. Amid COVID-19, the number of organizations conducting biweekly testing increased to 29 percent, indicating that healthcare organizations are fairly committed to regularly assessing any vulnerabilities. However, the healthcare industry is not as proactive when it comes to training. Prior to COVID-19, no employees went through monthly cybersecurity training, while only 5 percent expect to have monthly training in the future. Concerningly, over one third (34 percent) expect cybersecurity training for employees to be conducted only during the onboarding process — the highest of all sectors.

IT professionals in healthcare have historically faced — and are expected to continue facing — a variety of barriers when looking to invest in cybersecurity infrastructure. Unfortunately, 61 percent faced budget constraints prior to the pandemic, while 66 percent expect to in the future — both of which are the highest among all industries. Nearly one third (29 percent) were unsure of their needs prior to the pandemic, while 24 percent are unsure of future cybersecurity needs — again the highest across surveyed industries.

Education

When looking at educational institutions, only 22 percent of IT professionals are very confident in their future cybersecurity posture, which is the lowest among respondents. In relation to this, over half (57 percent) of IT professionals working in education are the most concerned about future cloud security (57 percent). Given the new, virtual demands on the education sector, these combined figures are concerning and indicate that cybersecurity and cloud solutions are not being leveraged to their full advantage in the sector.

In terms of barriers when looking to invest in cybersecurity technology, 27 percent of organizations are unsure of their current needs amid the pandemic, which is the highest among all respondents. Looking ahead, however, education seems slightly surer as only 23 percent expressed uncertainty about their needs regarding future cybersecurity investment. Additionally, budget is expected to be a growing issue in the future. Half of respondents (50 percent) indicated this as a barrier prior to the pandemic, while 53 percent feel this will be a roadblock in the future. In addition, 18 percent of organizations faced resistance from senior management prior to the pandemic – once again the highest among all respondents. Fortunately, senior management in this industry have largely seemed to change their outlook, as only eight percent of respondents see leadership decisions as a barrier looking to the future.

Financial Services

The financial services sector is one of the more adaptive sectors when it comes to leveraging and adopting cybersecurity tools, solutions and training. Looking to the future, 51 percent of respondents are confident in their organization's cybersecurity posture, which is the highest among all respondents. This is likely thanks to regular training; prior to COVID-19, 17 percent of employees in this sector received monthly training, with a further 31 percent receiving training on a quarterly basis. Both figures are the highest among all respondents.

In terms of technology, 60 percent of financial services organizations plan to continue using SaaS for all work which is the highest among all respondents. In addition, 29 percent of organizations used AI/ML for security before the pandemic, while 40 percent anticipate using it in the future — once again the highest among all sectors surveyed. Interestingly, only 40 percent of respondents anticipate budget constraints when looking to invest in cybersecurity tools or solutions, the lowest among all industries, while 31 percent anticipate no barriers at all moving forward.

Business and Professional Services

Similar to the financial services sector, business and professional services tend to be on the forefront of cybersecurity tools and solutions. Two-fifths (41 percent) of respondents are very confident in their future cybersecurity posture, the highest among all respondents. Prior to the pandemic, employees worked from home frequently, with 13 percent working remotely 3–4 times a week and 20 percent working remotely 1–2 times a week — the highest and second highest figures among all industries, respectively. Amid the pandemic, 73 percent of employees are working from home most or all the time, which is the second highest of all respondents and well above the average of 58 percent. Cybersecurity posture confidence, forward-looking investments in cybersecurity tools and solutions and the nature of work in this industry are likely what allowed and will continue to allow businesses in this sector to operate remotely with a high rate of success.

This sector also has the fewest barriers to cybersecurity investment across all sectors. Looking to the future, nine percent of respondents expect resistance from senior management, only eight percent expect they won't know where to start (lowest of all respondents) and 35 percent do not anticipate to face any barriers at all (highest of all respondents). Similarly, IT respondents in this sector anticipate leveraging various cybersecurity tools with 28 percent expecting to use AI/ML (second highest of all respondents), 77 percent for MFA, (highest of all respondents) and 67 percent for cloud security (highest of all respondents).

Where do we go from here?

The pandemic's second wave has led IT professionals to continue adapting and adjusting to serve the current environment's demands, while carefully planning for various potential challenges that the future work environment will bring to bear. As Canadian organizations reckon with their needs, the top three takeaways we recommend are:

1. **Leverage cybersecurity tools that enable agility in our remote and uncertain environment.**

   It's important that organizations recognize how the pandemic has shifted their organizational security and learn from it moving forward. Adapting to avoid previous mistakes by making the necessary adjustments through policy and technology adoption is essential.

2. **Make sure your cybersecurity infrastructure meets the needs of your organization.**

   With uncertainty around what may be required to maintain business continuity over the long-term, regularly reviewing and testing the efficacy of existing cybersecurity solutions is crucial to assess any gaps or vulnerabilities. Equally as important, but often underappreciated, is conducting regular training for employees relevant to the work environment.

3. **Adopt the appropriate cybersecurity tools to prevent data breaches.**

   While some organizations see cost as a barrier and may be hesitant to allocate budget to invest in cybersecurity, IT professionals must work to implement the appropriate solutions to ensure security today and in future work environments. It's important organizations understand why they're making the investment in these tools and that adoption doesn't reduce the need for cybersecurity expertise.

Our Featured Partners

If you're curious about improving your organization's cybersecurity posture or would like to learn more about how to get started, contact our CDW cybersecurity experts at 800.972.3922 or visit CDW.ca/cybersecurity.

PEOPLE WHO GET IT®