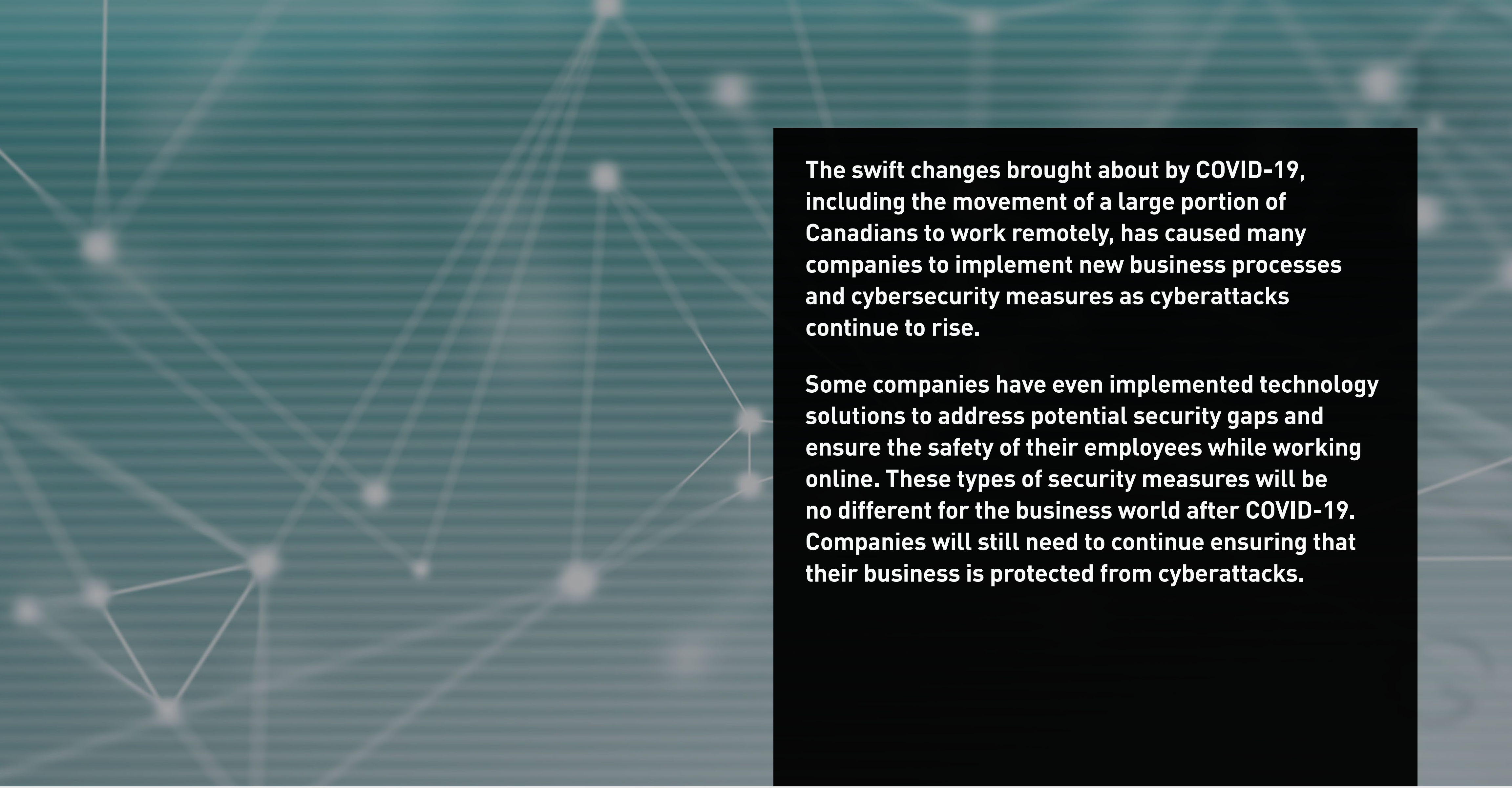
Cybersecurity tips

How to protect your business as cyberattacks increase amid COVID-19

VICTOR



The swift changes brought about by COVID-19, including the movement of a large portion of Canadians to work remotely, has caused many companies to implement new business processes and cybersecurity measures as cyberattacks continue to rise.

Some companies have even implemented technology solutions to address potential security gaps and ensure the safety of their employees while working online. These types of security measures will be no different for the business world after COVID-19. Companies will still need to continue ensuring that their business is protected from cyberattacks.

Preparing for the post-pandemic world

As social distancing measures become less widespread, organizations will need to adapt operations to this "new normal."

This will require a thorough evaluation of cybersecurity controls and business processes. In the pandemic rebuilding period, changes made to address the pandemic may need to be replaced with more secure and permanent solutions.

We can anticipate that as Canadians recover from the pandemic, on the technology front, the post-COVID-19 business world could look something like this:

- Increased and institutionalized remote working
- A significant growth in the use of online collaborative tools
- Expanded cyberattacks due to increased remote working
- A move towards "cloud" managed services and applications
- More attention given to risk management practices

Companies and their employees will need to keep these factors in mind when working in the post-COVID 19 business world. Here are five key areas to consider when developing a new cybersecurity plan.

Remote working solutions

Anticipate a permanent increase in remote working. With this in mind, consider the following:

- Establish secure connectivity processes for employees at their workstations (such as multi-factor authentication for VPN and critical information systems)
- Manage access for your remote workforce that meets company security requirements and employees' ease-of-use needs
- Implement mobile device management solutions to address the use of company-issued, and approved personal, technology devices (i.e., mobile phone, laptop, etc.) for business purposes
- Enforce software updates to employees' company-issued technology devices
- Closely examine remote desktop protocols, which allow remote access of Windows systems and servers and can entice hackers to try and gain unauthorized access to company files
- Implement network access controls to authenticate and validate employee access when using company technology devices, and enforce technology security policies before permitting them to connect to your company's corporate in-office or remote networks

1

2

Cloud services

Cloud services can offer significant cost, efficiency, resilience and potential security benefits over hosted digital platforms for the storage and application of business information. However, cloud services should be strategically adopted and managed.

- Adopt formal strategies for the use of cloud services
- Develop an inventory of cloud usage in your company
- Define policies for the storage of business information and outline the conditions required for the use of cloud services, data storage and local storage, particularly for sensitive and/or confidential information
- Ensure your cloud-based service provider has strong security protocols to protect your company's sensitive and/or confidential information
- Ensure you have installed cloud-based software that monitors access activity and enforces security policies
- Monitor cloud usage within your company and enforce related cybersecurity policies to guard against technology viruses, malware or any suspicious activity

Secure collaboration tools

While email communication, office productivity tools and video conferencing have been vital during the pandemic, companies may choose to innovate by adopting and using additional secure collaboration tools. Here are some basic safety measures to consider when doing this:

- Implement safe email protocols and encryption to protect against unauthorized access
- Don't send work-related information to your personal technology devices (i.e., mobile phone, tablet, laptop, etc.) as this may compromise sensitive/confidential information and expose it to cybercriminals (i.e., bad actors)
- When using video conferencing tools such as Zoom or WebEx, protect your privacy by making the meeting private and apply a passcode to prevent unwanted parties from hijacking your meeting
- Limit sharing capabilities during video conferencing to protect sensitive/confidential information and to prevent the accidental disclosure of content not intended for public sharing
- Avoid sharing your video conference meeting website link publicly, which may invite potential hackers or unwanted guests to your meeting
- Use a service provider that prioritizes encryption and cybersecurity measures to protect your privacy and safeguard your company's information

3

“Bring Your Own Device” policy

4

Many organizations have allowed employees to use their personal technology devices, including laptops, mobile phones and tablets, for business purposes because of the COVID-19 crisis. Phone calls were routed to personal mobile phones, email was made available on personal devices and employees were permitted to access cloud-based applications from personal devices.

However, in order to protect and mitigate potential cyberrisks to your company and your employees, consider the following:

- Ensure that your company has established a policy on the implementation and use of personal technology devices for business purposes (i.e., “Bring Your Own Device” - BYOD)
- Verify that your company’s insurance policy supports BYOD as some insurers may reject BYOD use unless the personal device is tied to your company’s network
- Review implemented measures taken during COVID-19 to ensure the continued protection of your company’s business networks and sensitive information
- Ensure that BYOD devices are well protected with updated security software and encryption
- Review and update VPN profiles and firewall rules so employees receive appropriate role-dependent privileges
- Educate employees on safe technology practices while using their personal technology devices to guard against the potential of cyberattacks in light of BYOD use

5

Cyberbreach assessment and response plan

Companies will need to implement a strong and current breach response plan. This is important to address the potential impact of a cyberbreach on business continuity.

- Conduct a risk assessment and implement security mechanisms, such as multi-factor authentication, single sign-on and automatic logout from unattended devices
- Conduct regular cybersecurity audits and vulnerability tests of your computer systems and technology devices to assess, identify and correct security weaknesses and gaps
- Incorporate lessons learned from the contingency operations brought about by COVID-19
  - If there was no pre-existing breach response plan, the need for one should be apparent
- Refresh and update your breach response and disaster recovery plans to address your company's current situation and the "new normal"
- Provide regular employee security training and awareness against cyberthreats
  - Well-trained staff are your best line of defense against attacks
- Obtain a cyber insurance policy or review your existing policy to protect yourself against new cybersecurity challenges, and ensure that the policy meets your company's needs

A new focus on resilience

COVID-19 has reinforced the need for companies to revisit their cyber strategy to align with "new normal" requirements. This recent crisis has highlighted the need to prepare for serious business disruption and establish sound contingency plans. The post-COVID-19 recovery and preparation period presents the opportunity for companies to rebuild and improve their organizations' resilience and build strong business practices going forward.

For more information and insights, visit victorinsurance.ca
or view the following additional resources:

- Victor Cyber Insurance
- COVID-19 Resources
- Infographic: "Typical day in the life of a business owner"
- Animated video: "A day in the life of a business owner in a cyberworld"

#COVID-19 #CyberAttacks #TheThreatIsReal #StaySafe

Visit us at victorinsurance.ca to learn more.

This document is for illustrative purposes only and is not a contract. It is intended to provide a general overview of the program described. Please remember only the insurance policy can give actual terms, coverage, amounts, conditions and exclusions. Program availability and coverage are subject to individual underwriting criteria.