A GUIDE TO CYBERCRIME IN 2021

and how to protect your small business

WHAT'S INSIDE

3
The future of work after COVID-19
Understanding how small businesses perceive their risks 4
Cyber breaches: The byte-sized basics 4
What is a cyber breach? 5
What are some examples of cyber breach threats? 5
Are small businesses really prone to cyber breaches? 6
How much could a cyber breach cost your business? 6

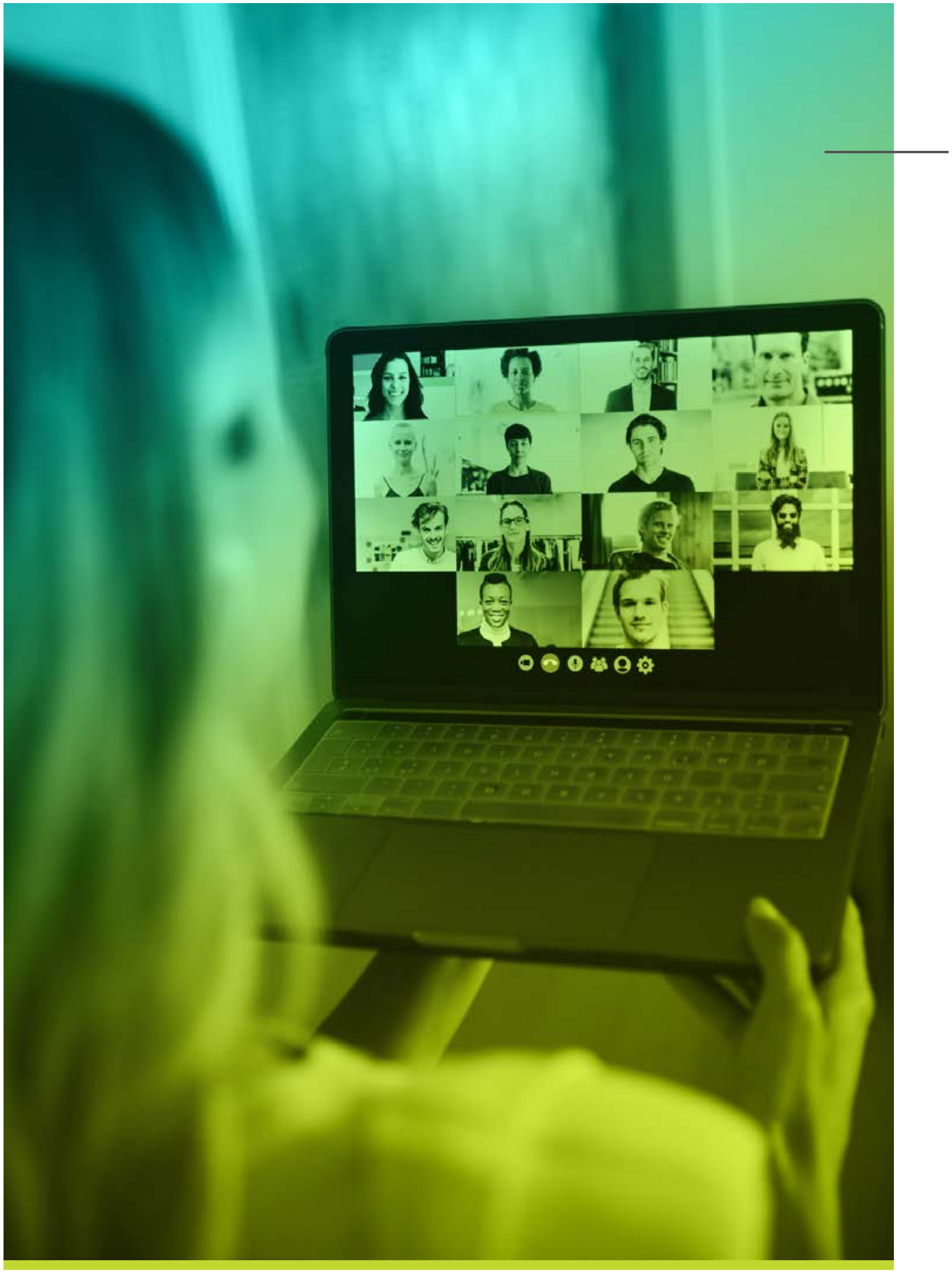
7
How cyber breaches can impact your business
Viruses are venomous 7
Your business could be a target 8
Hackers excel at extortion 8
Breaches can interrupt your business 8

9
5 tips on how to recover from a cyber breach

11
Your safeguard: cyber risk and data breach insurance
What is cyber risk and data breach insurance? 12
What is e-commerce insurance? 12
What is business interruption insurance? 12

13
The Trushield difference
Legal Assist* 14
Risk Management Assist** 14
Trauma Assist*** 14
24/7 Claims Service 14

15
Your next steps to fight back against cyber breaches



THE FUTURE OF WORK AFTER COVID-19

As a result of the COVID-19 pandemic, the traditional workplace has moved online. To help curb the spread of the virus, many businesses have implemented work from home environments. In a survey released by Statistics Canada in July 2020, nearly one-quarter of Canadian businesses expect that 10 per cent or more of their workforce will continue to telework or work remotely post-pandemic. It also found that 40 per cent of Canadians found themselves working from home as lockdowns were enforced, compared to less than 10 per cent in 2018.

While there are many benefits to working and doing business from home, there are also risks that come with this new future of work. The Canadian Centre of Cybersecurity notes that Canadian organizations and businesses have become more vulnerable to cyber attacks. Your small business may be an attractive target to hackers, who work to exploit your vulnerability during a challenging time and gain access to customer data and other sensitive information.

Fortunately, you're not alone! We've created a detailed resource to help you navigate the world of cybercrime, including the most common types of cyberattacks, practical ways to prevent and respond to them, and the importance of cyber risk insurance. You can use this guide as part of your small business risk management and business continuity planning.

Are small business owners at risk?

To better understand the way small businesses perceive their cybersecurity risks, we partnered with Leger, a Canadian market research and analytics company, to conduct a survey of 422 businesses representing different industries in September 2020. We learned that:

- The COVID-19 pandemic hasn't changed the way small and medium-sized businesses (SMBs) perceive their cybersecurity risks, despite findings from the Canadian Centre for Cybersecurity that show cybercrime has been frequent – 77 per cent of SMBs feel that their risks are the same as compared to 6 months ago.
- Only 29 per cent of SMBs surveyed believe they are at a high risk of a cyber-attack.
- Only 15 per cent have implemented preventative IT and employee training.
- Only 11 per cent have purchased cyber risk or data breach insurance.
- In comparison to other risks, such as financial security, employee/labour and health and safety, SMBs ranked cybersecurity as low risk.

Based on these findings, cybersecurity is often not a priority in risk management and business continuity planning for many small business owners. Throughout this guide, you'll find that we reference this study and compare it with national and international data.

Cyber breaches: The byte-sized basics

Picture this: you're checking your email account, and you open an email that appears to be from a recent customer. You don't recognize the email address, but you open the email anyway. The sender has attached a digital receipt and wants you to take a look at it. Thinking nothing of it, you decide to open the attachment. That's when disaster strikes. The attachment contains a malicious virus that gives an unknown hacker remote access to your computer. In just a few quick minutes, they're able to steal your personal information, financial records, and customer data. Just like that, you and your small business have been hit by a cyber breach.

Nearly one-quarter of Canadian businesses expect that 10 per cent or more of their workforce will continue to telework or work remotely post-pandemic.

What is a cyber breach?

A cyber breach is when an unauthorized individual or organization gains the ability to view, access, or retrieve data from another individual or organization. Cyber breaches typically involve stealing data to share with others, or stealing data and holding it for ransom. Cyber breaches are also known as data breaches, leaks, or spills.

Most cyber breaches involve accessing and stealing data that's vulnerable and exposed, whether they're files, documents, or other sensitive information. Here are some examples of types of data that could be stolen from you (and your customers):

- **Financial information**, such as credit card or bank details
- **Confidential business information**, such as login credentials and passwords
- **Personal health records**, such as medication requirements
- **Sensitive personal information**, such as addresses and phone numbers
- **Intellectual property**, such as copyrighted materials, patents, and trademarks

What are some examples of cyber breach threats?

During the COVID-19 pandemic, Statistics Canada reported that just over four in ten Canadians experienced at least one type of cybersecurity incident since the beginning of the pandemic, including malware, phishing attacks, fraud and hacked accounts. Here are is a list of common cyber breach threats that could impact you, your business, and your customers:

Malware – This is a general term that refers to any type of harmful computer virus. Worms, spyware, and adware are all examples of malware. In April, the Canadian Centre for Cyber Security (CCCS) reported a large number of COVID-19 themed domains that were found to be malicious or related to fraudulent activity. Many hackers have developed COVID-19 related content, including statistics on infection rates and geographic spread, public health updates, knowledge of cures or treatments, and access to medical supplies, to try and trick victims into clicking on malicious links or attachments. For example, SMS messages were sent from imposters claiming to be from the Government of Canada, directing individuals to visit a malicious website and download an application.

Phishing – This refers to cyber criminals attempting to extract sensitive information by disguising as a trustworthy contact or online entity. Phishing lures are often hidden in the form of hyperlinks, websites, or emails from questionable sources. Essentially, phishing involves cyber criminals placing bait online in hopes that someone unsuspecting will "bite" and share sensitive information. Some phishing attacks can be quite sophisticated. For example, in late April, the CCCS reported a phishing campaign targeting individuals waiting for their Canadian Emergency Response Benefit (CERB) deposit with a link where they could access their benefits, but only once they revealed personal financial information.

Password Attacks – This refers to cyber criminals using programs or applications to try cracking your passwords in order to obtain your online credentials and access your data. They may be looking to hack into your email, your website, your bank account, or other systems. Cyber criminals can be relentless, and they often employ different password attacking techniques to get the job done.

Ransomware – This is an increasingly popular type of cyber breach where cyber criminals steal data and hold it for ransom. Using a virus or similar type of malware, a cyber criminal will gain access to a victim's data and lock it. Once locked, they will threaten to publish the victim's data, delete the data, or continue blocking access to it unless a ransom is paid. The ransom instructions are often intimidating and will usually be included in the virus itself. Here are a couple of examples:

- "Your computer was used to visit websites with illegal content. You must pay a $10,000 fine in order to unlock your computer."
- "You only have 96 hours to submit the payment. If you do not send the money within 96 hours, all your files will be permanently encrypted and you won't be able to recover them. Choose wisely."

Ransomware attacks are becoming more popular and more prevalent across the globe. In the spring, the CCCS reported a Canadian university engaged in COVID-19 research and a provincial government health agency were targeted by COVID-19-themed phishing attacks attempting to deliver ransomware.

Are small businesses really prone to cyber breaches?

Based on the sophisticated examples above, you might think that cyber criminals only target large organizations. In a recent study released by the Insurance Bureau of Canada (IBC) on the impact of COVID-19 on cybercrime, 99 per cent of Canadian organizations reported an increase in cyber attacks. But what are the chances that small businesses like yours could ever be targeted by hackers? Well, they're higher than you might think.

As a small business you may think that you're insignificant to cybercriminals. However, according to the IBC, SMBs are often targeted as entry points to gain access to larger businesses, with 89 per cent experiencing an increase in phishing attacks since the beginning of the COVID-19 pandemic.

Many small business owners are reluctant to invest in cyber training or protection because of limited resources. In the same IBC survey mentioned above, less than half of SMEs had implemented defenses against cyberattacks (47 per cent).

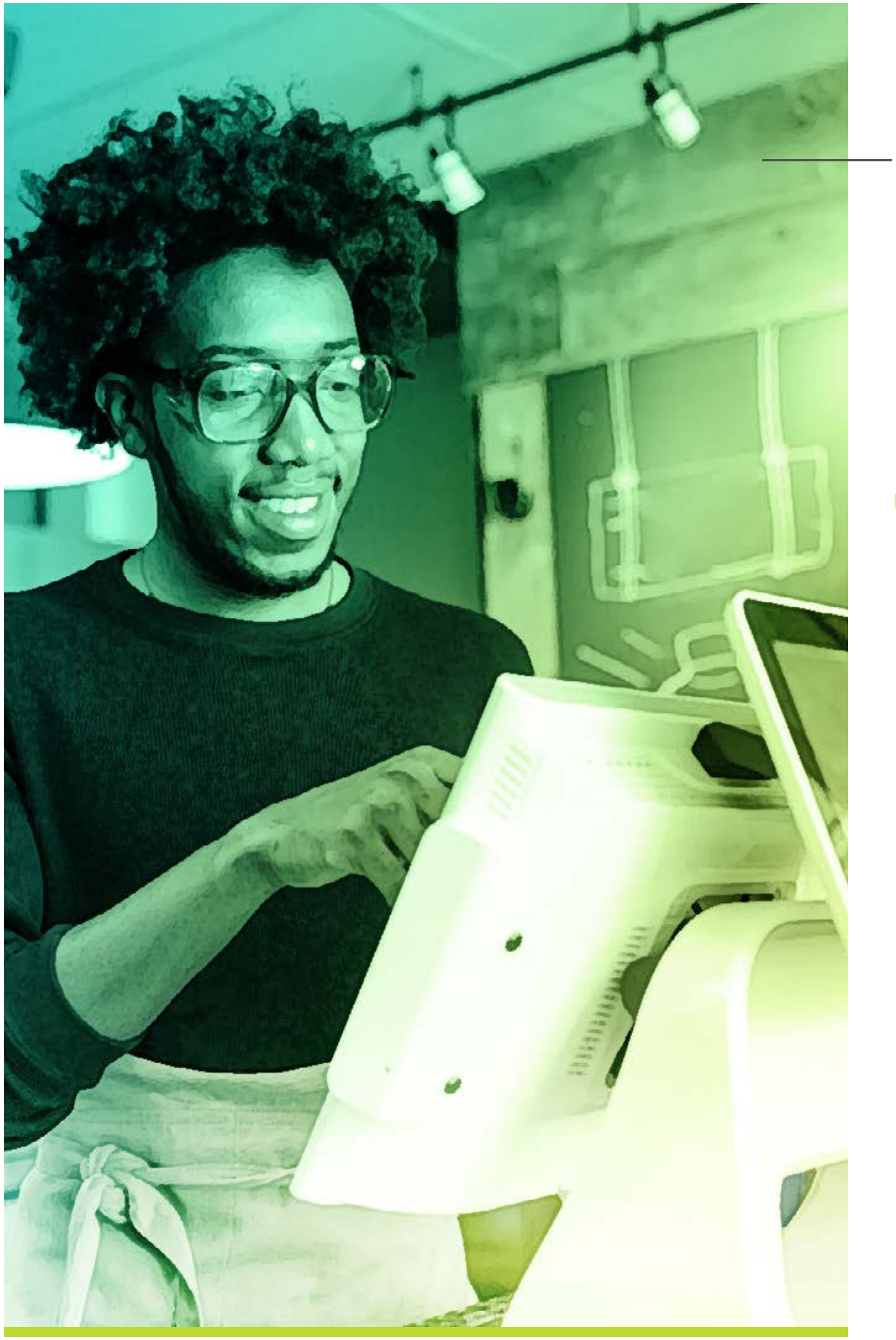
Large corporations invest millions of dollars in state-of-the-art technology and IT resources to defend themselves from cyber breaches. Most small businesses do not have the budget to invest in protective barriers and IT infrastructure like large corporations do. Because of this, small businesses tend to be easier to hack.

Some cyber criminals even target small businesses to steal customer information. The Canadian Federation of Independent Business (CFIB) suggests that many SMBs don't have adequate cyber protection in place because they don't know they need it. A small customer database is still a hacker's goldmine – in fact, according to Symantec's 2019 Internet Security Threat report, a name or birthday can be worth up to $1.50 on the black market, while a passport or driver's license can be worth up to $35.

How much could a cyber breach cost your business?

It's difficult to pinpoint the exact amount that a cyber breach could cost your business, but we've rounded up both external and internal sources to give you an idea. According to an article in The Canadian Underwriter, North America is the most expensive location for a SMB to suffer a data breach, with the average recovery cost at $149,000 USD. In a 2019 cyber security poll conducted by IBC, 37 per cent of SMBs that suffered a cyber attack stated that the breach cost them more than $100,000. This includes costs associated with lost business, bringing in external cyber experts, repairing brand damages, and improving software and infrastructure. According to the IBC, remote work has increased the average cost of a data breach by $137,000.

Our internal insurance claims data has shown us that claims resulting from cyber incidents can range anywhere between $5,000 and just over $100,000 CAD. These claims range from email viruses to ransomware extortions, ranging in shape and size.



HOW CAN CYBER BREACHES IMPACT YOUR BUSINESS

Still not convinced that cyber breaches could put a dent in your business? Here are some cyber breach trends you should be on the lookout for:

Viruses are venomous

Like the flu, computer viruses can have long lasting implications on you and your business, whether a virus locks down your machine, steals confidential data, or damages personal documents. If you or an employee clicks a malicious link, it could infect the computer you use for your business. If you use multiple machines, it could also infect your entire system with a destructive virus that can shut down your network and wipe your hard drives.

Not only can viruses and other infections impact your small business, they could also impact your customers and other companies as well. For example, ransomware is regularly spread through phishing messages that contain harmful connections or through drive-by downloading, which occurs when a user accidentally visited a malicious site. According to the CCCS, when ransomware infects a device, it will either lock the screen or encrypt all of the files. To retrieve your data, hackers demand that you pay a ransom. A hacker may impersonate a law enforcement agency, and it say that your files were locked because your computer was used for some form of illegal activity.

As we continue to navigate the pandemic, the CCCS has found that businesses in healthcare, research and medical manufacturing are likely to be targets of ransomware attacks. When something like this occurs, it can lead to costly downtime and could do significant damage to your brand's reputation.

Your business could be a target

You may think that only careless individuals end up getting hacked. We don't doubt that you do your best to remain cautious when browsing the internet or checking emails. You might avoid visiting sketchy websites, opening unknown emails, or clicking suspicious links. With your careful behavior and overall awareness, you might think you're in the clear.

Hackers excel at extortion

In early 2020, Vanson Bourne, a global technology market research firm, conducted a global survey to gauge the impact of ransomware attacks on businesses. It found that 51 per cent of businesses were hit by ransomware in 2019, and businesses that paid a ransom to their hackers often doubled the cost of dealing with the attack.

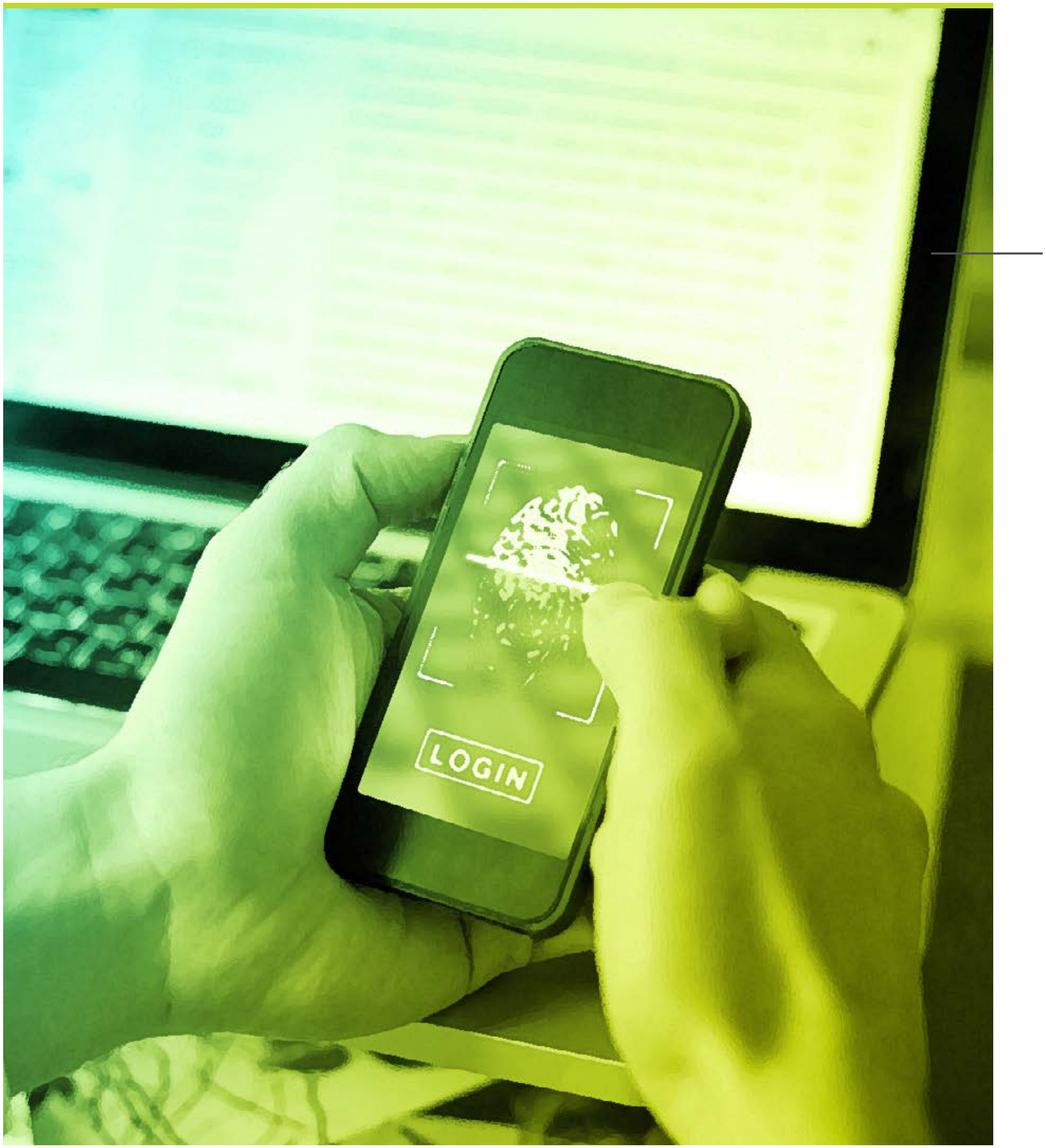
In 2020, the risks have increased. Hackers are deploying server-based attacks that are more sophisticated and far more devastating because of the higher value of assets that are stolen. According to the CCCS, Canada is one of the top countries impacted by ransomware, and these attacks are set to increase as cybercriminals scale their operations.

Breaches can interrupt your business

Cyber criminals work in the shadows and will go under the radar to breach businesses. During the pandemic, your team may have shifted to working remotely, which could expose your data to new and unexpected cyber risks. For example, many hackers are creating illegitimate sites to unleash malware by pretending to be a credible source, such as a university. An article by Canadian Underwriter reports an increase in fraudulent Microsoft password change notifications and Cisco Webex alerts. Since January 2020, the CCCS has also reported an increase of hackers leveraging the vulnerabilities in popular virtual private networks (VPNs). Many businesses have been breached and still have no idea, and as hackers get more sophisticated, it will only take businesses longer to realize that they have been compromised.

Although some cyber breaches linger under the radar for long periods of time, they could quickly put your business out of commission.

> According to the IBC, 47 per cent of businesses haven't implemented defenses against cyber attacks.



5 TIPS ON HOW TO RECOVER FROM A CYBER BREACH

Given that small businesses are top targets for cyber criminals, and given how effective some cyberattacks can be, how do small business owners feel about cyberattacks heading their way? According to a recent TruShield Insurance poll, not great. According to our poll of small business owners, 61 per cent of them believe they are not currently at risk of a cyber-attack.

In the unfortunate scenario that your small business falls victim to a hack, there are specific steps that you can take to recover from the breach and minimize your losses. Here are five tips on how to recover from a cyber breach:

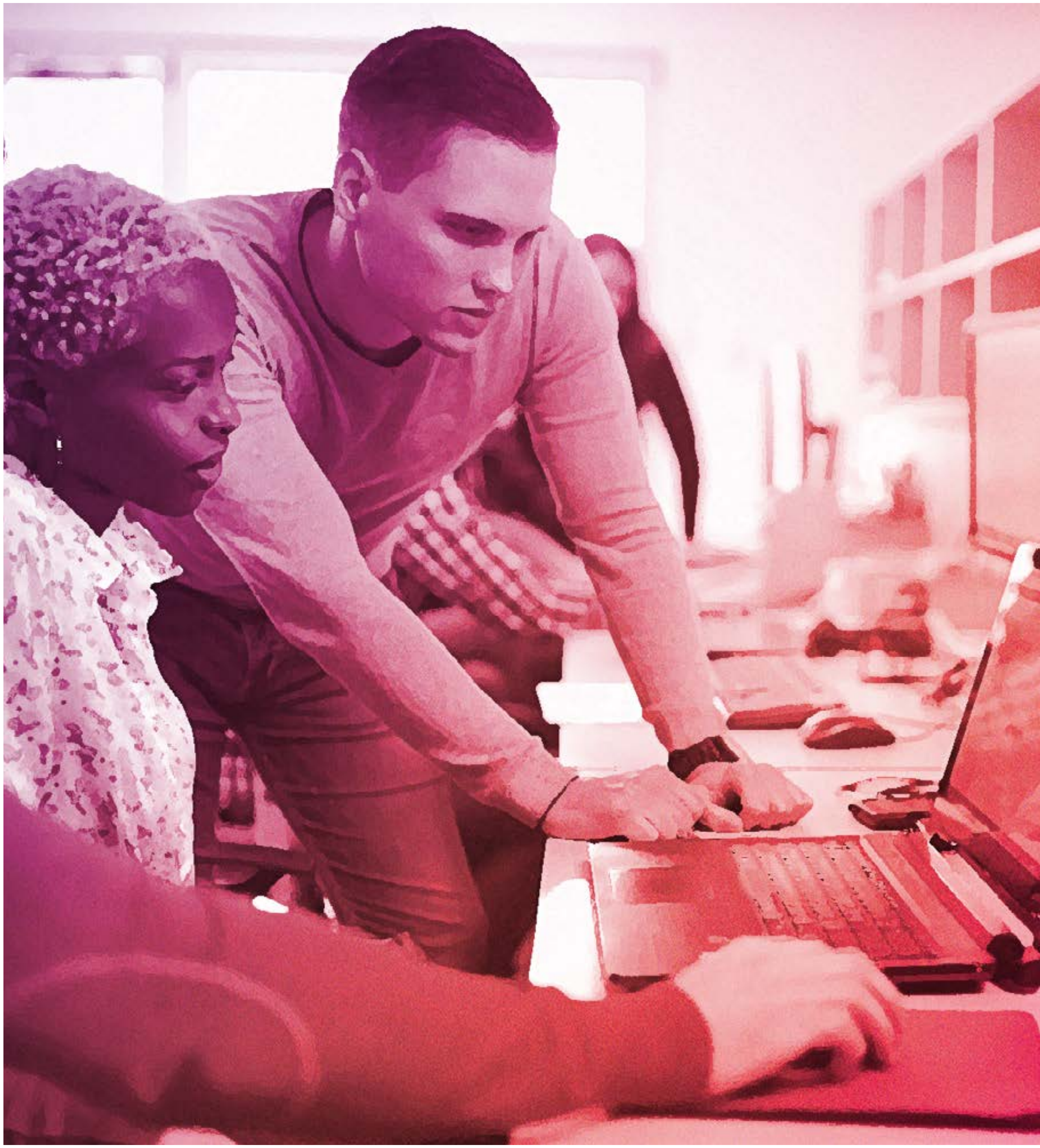
1. **Do not unplug:** We know that your gut instinct after experiencing a cyber breach may be to unplug and turn everything off right away. But shutting down a machine can delete valuable information on where the hack originated and the extent of the damage.

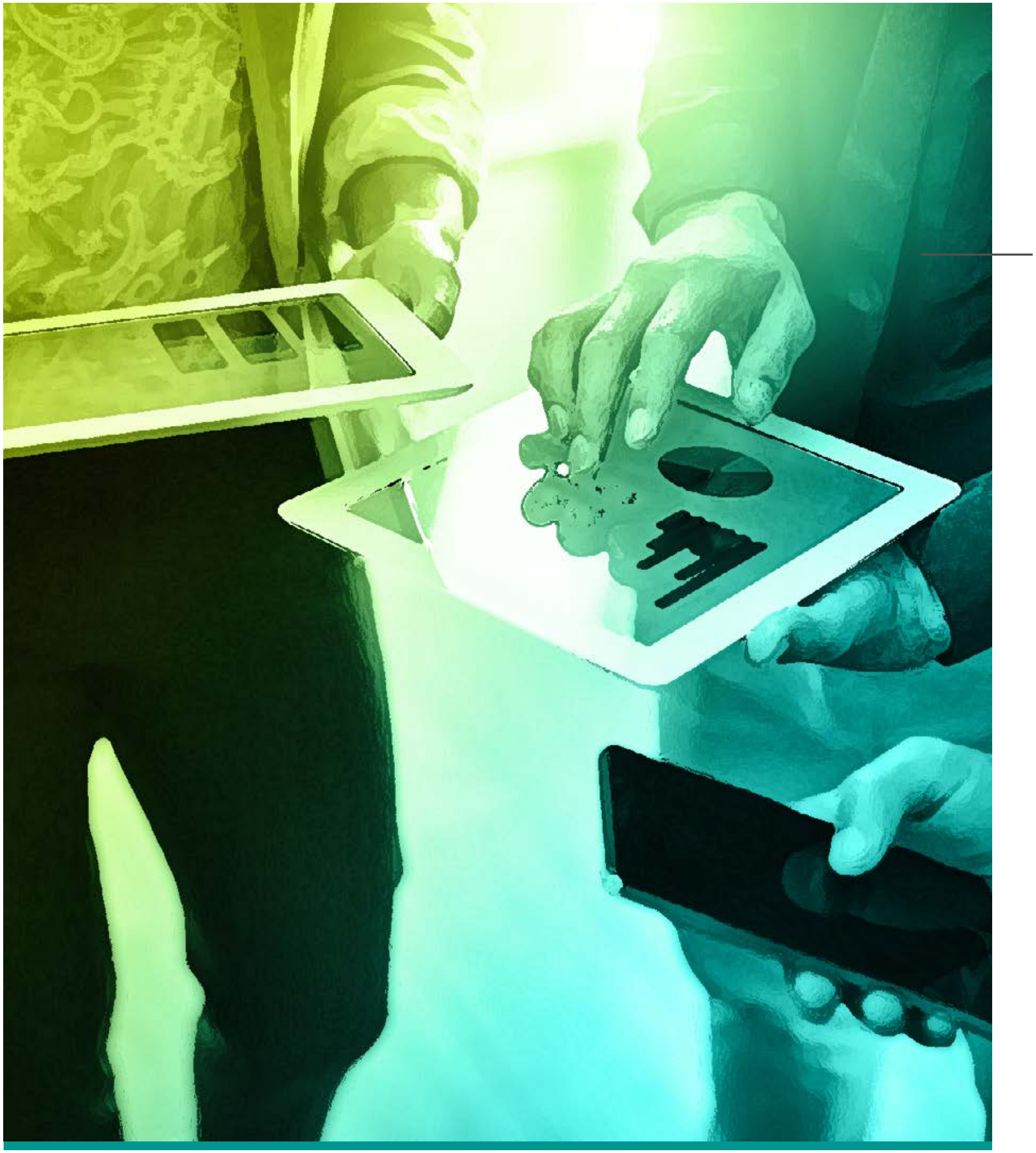
2. **Call in a pro:** Unless you've got a degree in post-breach forensic investigating, you're likely in over your head at this point. Bringing in someone who specializes in cyberattacks is a good next step after identifying a hack. They'll be able to determine important details including the scope of the damage that's been done. Once all the important information has been pulled by a specialist, they can help contain the situation.

3. **Communicate quickly:** It's not only best practice to communicate quickly if you're hit by a cyber breach, it's the law! In 2018, changes to Canada's federal private-sector privacy law came into force. Organizations are now obligated to record and report any breaches of their security safeguards, and notify individuals that are affected by the breach if it could cause them harm.

4. **Fix the gaps in your security:** The investigation you do following a breach will shine light on any vulnerabilities in your security system and will allow you to fix any holes to help avoid any future hacks. Investing in firewall systems and educating yourself and your employees on cyber best practices can give you another layer of security against the threat of cyberattacks.

5. **Revisit your coverage:** There are a number of myths associated with cyber risks for small business that can cloud your judgement and leave you vulnerable. Speak to your insurance provider about revisiting your policy to ensure you're covered for the damages that a cyber breach can cause.





YOUR SAFEGUARD: CYBER RISK AND DATA BREACH INSURANCE

After reading our tips, do you think your business would be able to recover from a cyber breach? Cyber risk insurance, along with similar coverages, can help you and your business recover from a cyber breach so you can focus on running your business. In the same Leger study mentioned previously, only 34 per cent of small businesses that were surveyed have invested in services to help guard against cyber risks, and only 11 per cent have invested in cyber risk insurance.

What is cyber risk and data breach insurance?

Cyber risk and data breach insurance is designed to help protect small businesses like yours from certain losses associated with data breaches and hacks. If your business ever gets hacked, this coverage could help shoulder the costs of restoring or recovering stolen data after a breach. It could also help cover the costs of notifying your customers that private information may have been compromised.

Cyber risk and data breach insurance is particularly important for entrepreneurs who rely on computers and technology for their services. If you provide services in a digital capacity, rely on a computer for your business, or collect any type of customer data and financial records, cyber event expense coverage should be a key ingredient of your small business insurance policy.

What is e-commerce insurance?

Do you sell products or services online, or use an e-commerce platform such as Shopify? Whether you sell B2B or B2C, running an online shop exposes you to cyber risks – from system reliability, privacy and fraud. A good insurance policy adds value and peace of mind to your business' risk management plan. Here are situations where this coverage could help:

- A hacker gains access to your company's private information including customer information, client information or employee information, and threatens to sell or disclose it.
- A hacker encrypts or threatens to encrypt electronic data on your company's computer system, preventing authorized access to any insured person.
- A hacker threatens to introduce a virus into your company's computer system.
- A hacker interrupts or threatens to interrupt your company's computer system, also known as a denial of service attack.

What is business interruption insurance?

Business interruption insurance is designed to help you recover lost business income and pay for ongoing business expenses when a sudden loss impacts your business operations. This includes interruptions to your services that are directly caused by a cyber breach or a network security incident. If a cyber breach interrupts your services and causes you to suffer a loss, business interruption insurance can help you recover lost business income and pay your regular ongoing business expenses until your computer system is restored.

THE TRUSHIELD DIFFERENCE

When you get small business insurance coverage from TruShield, you'll be provided with a flexible policy that fits the needs of your business. One thing that sets TruShield apart from our competitors is our value-added services. These useful perks help us take your policy to the next level at no additional cost to you. These services allow us to be there for your business every step of the way—before, during and after a liability claim.

24/7 Claims Service

Our 24/7 Claims Service is available for you 24 hours a day, every day of the week – just like the name promises! Our dedicated claims representatives will help you make a claim settlement with ease and without undue stress, giving you peace of mind when you need it the most.

Want to avoid a long wait after getting rear-ended? Try out our Express Claim service! Using your smartphone, you can work remotely with one of our dedicated claims adjusters to snap photos of the accident, assess the damage of your vehicle, and quickly produce an appraisal of your auto claim settlement.

Not only that, but we'll help you find a trusted collision repair centre and arrange for a rental if needed, so you can get back on the road as quickly as possible. Want to know the best part about this service? We can complete your appraisal in as little as half a day. Oh, the wonders of technology.

Legal Assist*

Small business owners are exposed to legal risks on a daily basis and lawsuits are a costly and time consuming process – better to avoid one before it happens. TruShield can help with that. As a TruShield customer, you'll have access to our Legal Assist service, which gives you unlimited telephone access to general legal advice to discuss any legal matters related to your business.* This can help small business owners better navigate their legal paths and help them avoid difficult and costly lawsuits before they occur.

Risk Management Assist**

Wouldn't it be great if you could stop a loss before it happens? Our Risk Management Assist program gives you access to our team of Risk Services Specialists who can provide professional guidance on risk management and loss prevention planning.** This advice can help you effectively manage risks within your business that you may not have been aware of.

Trauma Assist***

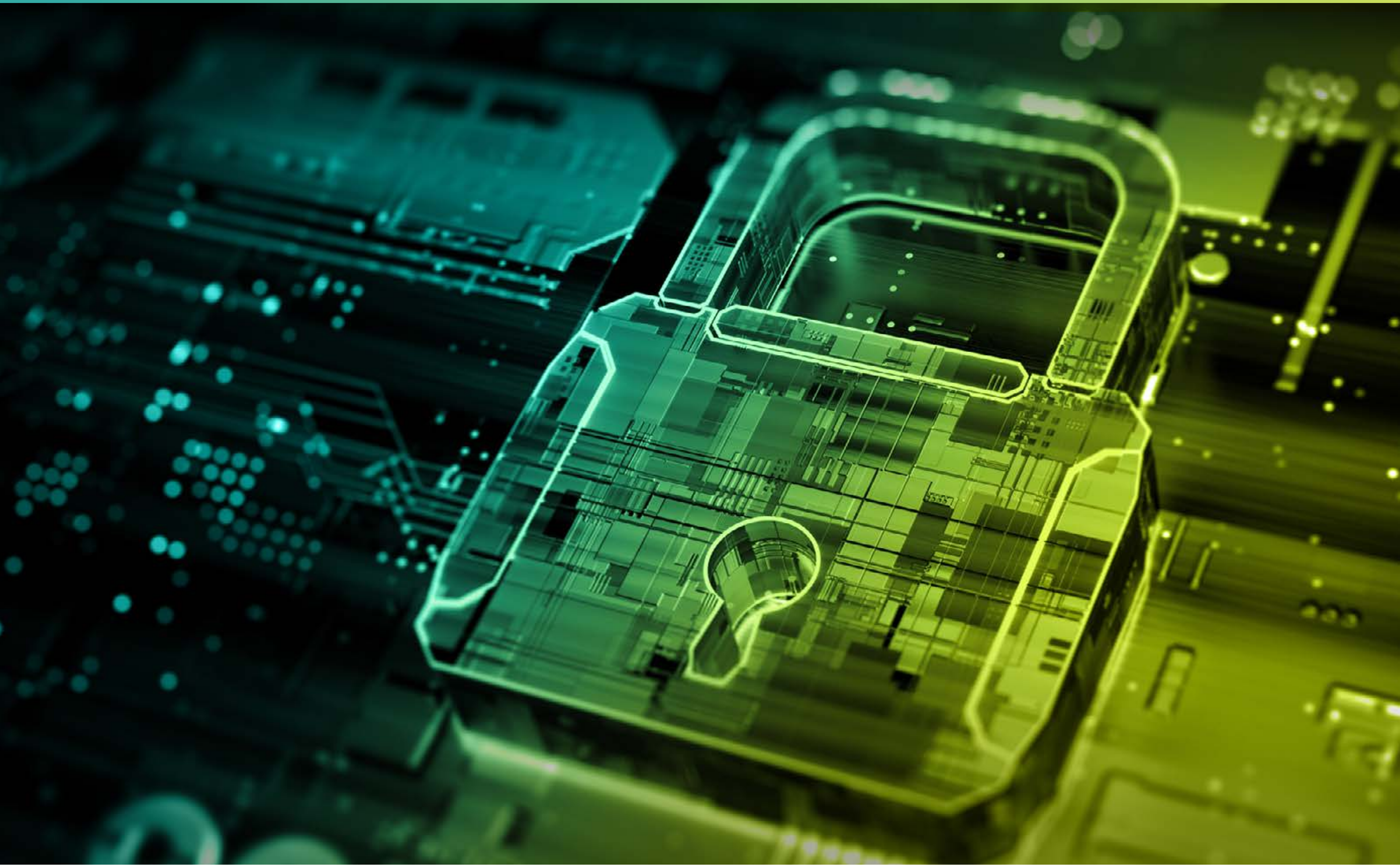
Suffering a loss within your business is not an easy experience. Our Trauma Assist program is designed to help both business owners and employees cope with the emotional effects of a loss.*** Through independent third-party professionals, we're able to offer personal one-on-one telephone or in-office counselling as well as critical incident stress management for groups. All of our Trauma Assist services are strictly confidential.

YOUR NEXT STEPS TO FIGHT BACK AGAINST CYBER BREACHES

The truth is, no matter how small your business is or what type of business you run, you could still fall victim to a cyber breach. Cyber breaches can be costly and could put you and your business out of commission. To help you plan for an protect against your cyber risks, here are other resources your small business can refer to:

- Cyber threat bulletin: Impact of COVID-19 on cyber threat activity
- Building a strong business continuity plan
- Phishing 101: What to look for
- Follow these tips to avoid a phishing scam
- Cyber risks your business could face during a pandemic
- Tips to help protect your business from the risks of remote employees
- Reasons to offer a VPN to remote employees
- COVID-19 resources for businesses

If you run a small business, having a comprehensive insurance policy can help you and your business recover after a stressful scenario such as a cyber breach. If you're reluctant to take on the expense, remember that without insurance, you'll be solely responsible for dealing with repair costs, ransomware extortion fees, and interrupted business revenue. To provide you with the best recovery options for your business, TruShield has flexible policies with the right coverages you need to stay protected. To learn more about our offerings and how we can help your business achieve its potential, contact us today!



TruShield
Insurance

TruShield Insurance and TruShield Insurance logo are trademarks of Northbridge Financial Corporation, licensed by ***Northbridge General Insurance Corporation*** *(insurer of TruShield Insurance policies). Terms, conditions and exclusions apply. See policy for details. This document is provided for information only and is not a substitute for professional advice. We make no representations or warranties regarding the accuracy or completeness of the information and will not be responsible for any loss arising out of reliance on the information. *Legal Assist services not provided for criminal, personal or insurance issues, do not provide representation in legal proceedings or legal fees coverage, and provided by Assistenza International, through lawyers licensed in your jurisdiction. **Risk Management Assist provided by our Risk Services specialists and is intended to augment your internal safety, compliance and risk management practices, and is not a substitute for professional or legal advice. ***Trauma Assist provided by independent third-party professionals – long-term and specialized counseling not included. Services are not an insurance policy, and not all policies are eligible. Contact us for details.* [3800-002-ed03E | 02.2021]