TruShield Insurance

COSTLY CYBER BREACHES YOUR SMALL BUSINESS COULD FACE...

...and tips to help you protect yourself from them.

WHAT'S INSIDE

CYBER BREACHES: THE BYTE-SIZED BASICS

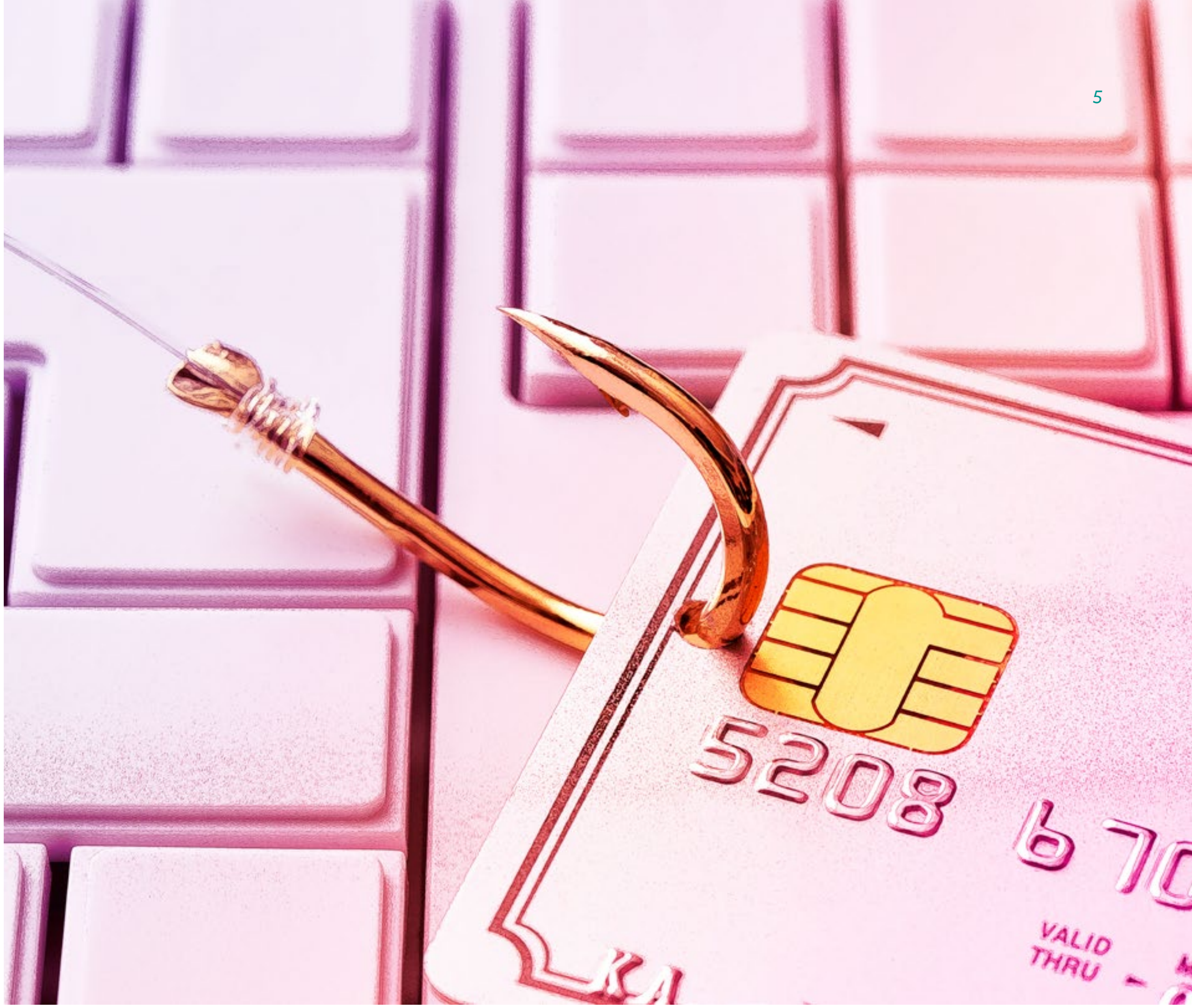
Picture this: you're checking your email account, and you open an email that appears to be from a recent customer. You don't recognize the email address, but you open the email anyway. The sender has attached a digital receipt and wants you to take a look at it. Thinking nothing of it, you decide to 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.

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**, as copyrighted materials, patents, and trademarks



What are some examples of cyber breach threats?

Here's a fun fact: Adorable dogs can come in many shapes and sizes! Here's a not-so-fun fact: so can cyber breaches. Here are the main types of 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. Like "smog" or "brunch", malware is an amalgamation of two words: malicious and software...we'd rather have brunch, personally.

Phishing – This refers to cyber criminals attempting to extract sensitive information by disguising as a trustworthy contact or online entity. Phishing lures are often disguised 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. It's like real fishing, only the stakes are a lot higher (and it might be less boring). Some phishing attacks can be quite sophisticated. An investigation from Fortune revealed that Google and Facebook were the victims of an elaborate email phishing scam that lasted two years. How much did it cost them? $100 million. Talk about a big catch.

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. This is a guessing game you definitely don't want to participate in. Password attacks can lead to devastating results: in 2016, a massive password attack on the popular ecommerce website Alibaba affected over 20 million accounts.

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. Think of it as the worst way someone could ask you for money. 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 May 2017, thousands of organizations across 150 countries were attacked by a ransomware virus known as WannaCry.

Are small businesses really prone to cyber breaches?

Based on the sophisticated examples above, you might think that cyber criminals only target larges organizations. Sure, Target, Sony, and even the 2018 Pyeongchang Winter Olympics have all be attacked by cyber criminals. But what are the chances that small businesses like yours could ever be targeted by hackers? Well, they're higher than you might think.

According to Symantec, 54% of small businesses have been targeted by cyber breach attacks. Furthermore, Public Safety Canada states that 71% of breaches in Canada involve small- to medium-sized businesses. These stats may startle you, but if you step into the shoes of cyber criminals, they might make more sense. 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 credentials and gain access to a large corporation's data. In the case of the $202 million USD cyber breach against Target, investigators found that cyber criminals gained unauthorized access to Target's server by stealing credentials from a third-party HVAC vendor. If your small business is a third-party vendor or provides services to a larger organization, cyber criminals may very well use you as a Trojan Horse of sorts.

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. Kaspersky Lab estimates that the average impact of a cyber breach to North American small- and medium-sized businesses is **$117,000 USD**. This includes costs associated with lost business, bringing in external cyber experts, repairing brand damages, and improving software and infrastructure.

Our internal insurance claims data has shown us that claims resulting from cyber incidents can range anywhere between $5,000 CDN and just over $100,000 CDN. These claims range from email viruses to ransomware extortions. Like we said, cyber breaches can come in all shapes and sizes.

Kaspersky Lab estimates that the average impact of a cyber breach to North American small- and medium-sized businesses ***is $117,000 USD.***

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. Osterman Research found that more than one-third of ransomware infections obtained by small- to medium-sized businesses spread quickly to other devices. When something like this occurs, it can lead to costly downtime and could do significant damage to your brand's reputation.

Getting hacked is wack…yet it could still happen to you

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. There's still a chance you'll miss a blindspot however.

Research from the Erlangen-Nuremberg University states that 78% of people who claim to know the risks that come with clicking unknown links in emails still click unknown links. That's a large chunk of people who could fall victim to a cyber breach!

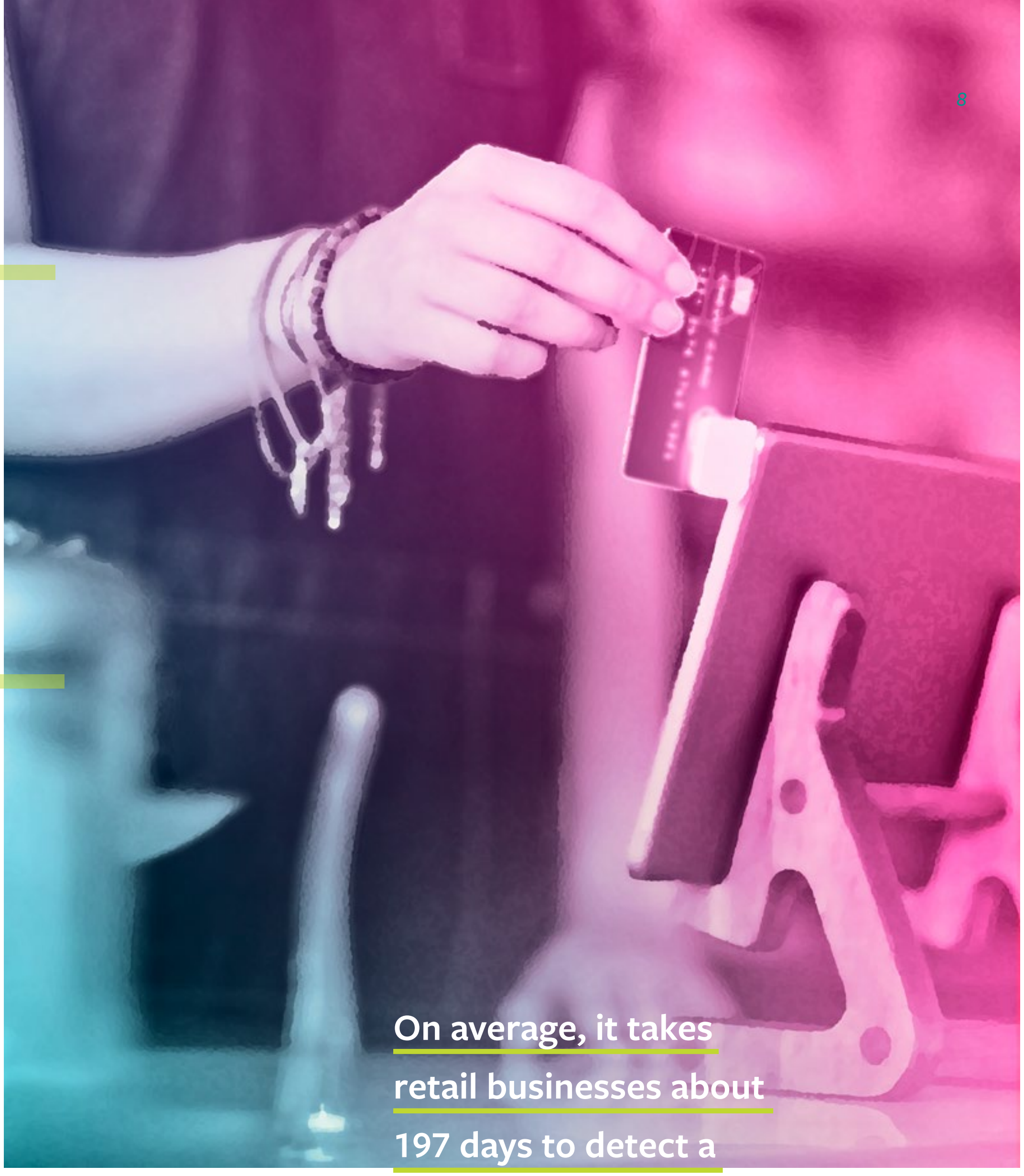
Hackers excel at extortion

The FBI (yes, that FBI) suggests that, based on their data, more than 4,000 ransomware attacks occur globally every day. This number is projected to only keep increasing as hackers continue to choose ransomware as their preferred method of attack. In fact, Symantec research indicates that ransomware attacks worldwide increased by 36% in 2017. The concerning part of this research is that 34% of global ransomware victims are willing to pay a ransom to their hackers. Those are pretty good odds for hackers.

Breaches can interrupt your business

Cyber criminals work in the shadows and will go under the radar to breach businesses. They often do it successfully. Research from Ponemon Institute states that, on average, it takes retail businesses about 197 days to detect a cyber breach. That's more than six months; think about how many family and friends' birthdays you'd have to celebrate before noticing your business has been hit! What's alarming is that it takes these businesses an average of 39 days to address and contain the breach. That's more than a month where your business could be out of commission. 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 can quickly put your business out of commission. Osterman Research found that among small- to medium-sized businesses that experienced a ransomware attack, 22% reported that they had to cease operations immediately. Talk about quickly closing the curtains.



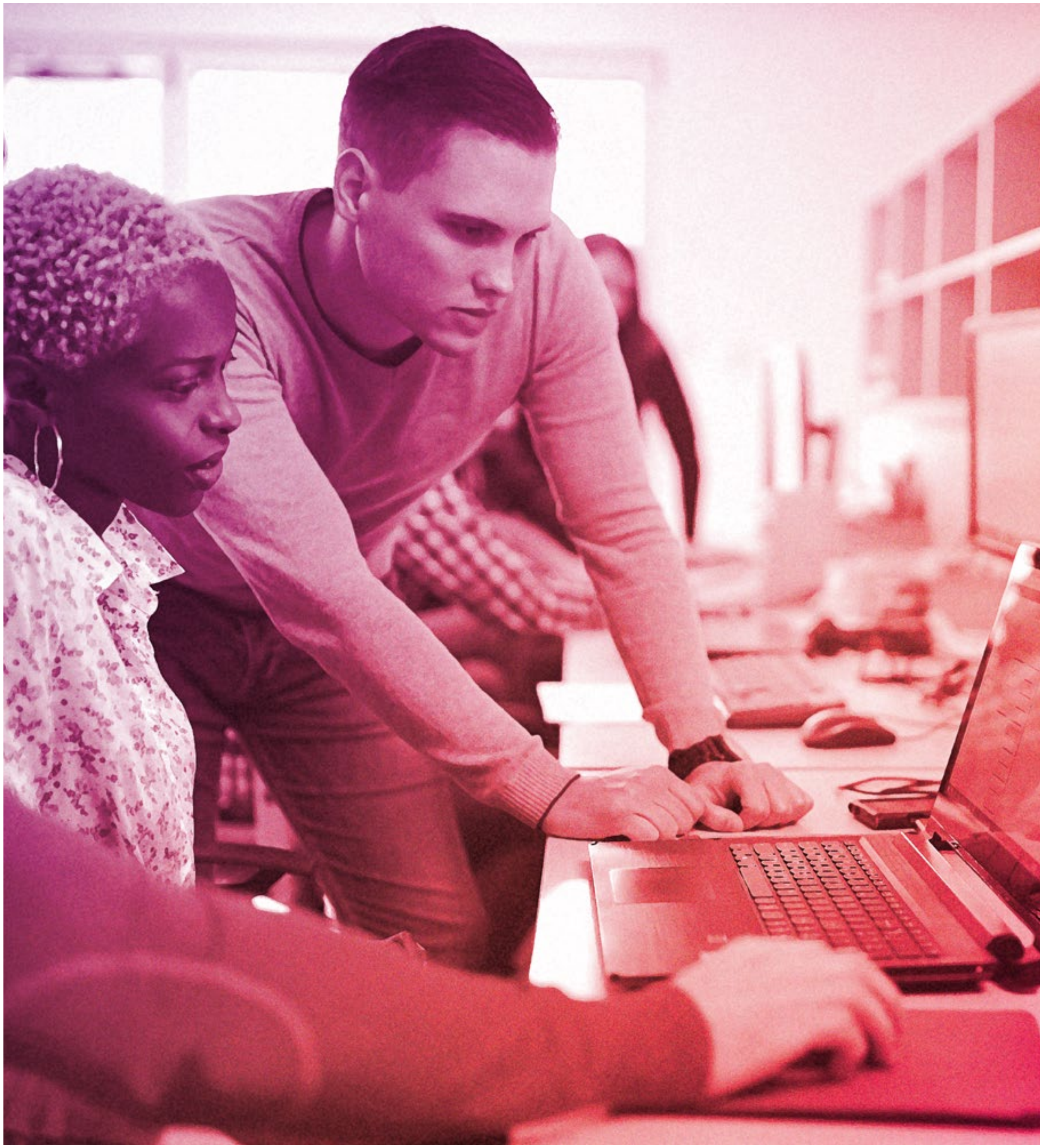
On average, it takes retail businesses about 197 days to detect a cyber breach, according to research from Ponemon Institute.

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. We polled hundreds of Canadian small business owners, and 65% of them said they aren't very confident their business could survive a cyberattack. Are you?

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 how 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:** Delivering bad news to your customers, employees, and partners is never fun, but it's often best to take care of this quickly. Consider communicating promptly, and be as honest as possible. Forbes found that customers are actually more interested in how a company handles a breach than the fact that one occurred in the first place. Be sure to provide consistent updates as they come in, too!
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 EVENT EXPENSE INSURANCE

If after reading our tips, you're still among the majority of Canadian small businesses that don't think they can bounce back from a cyber breach, don't worry just yet. Cyber event expense insurance, along with similar coverages, can help you and your business recover from a cyber breach, so you can focus on running your business and delighting your customers.:

What is cyber event expense insurance?

Cyber event expense 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, cyber event expense insurance could help cover 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 event expense 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 extortion expenses coverage?

E-commerce extortion expenses coverage can help your business recover if you fall victim to a ransomware attack, or other types of cyber breaches. Here are some situations where this coverage could help:

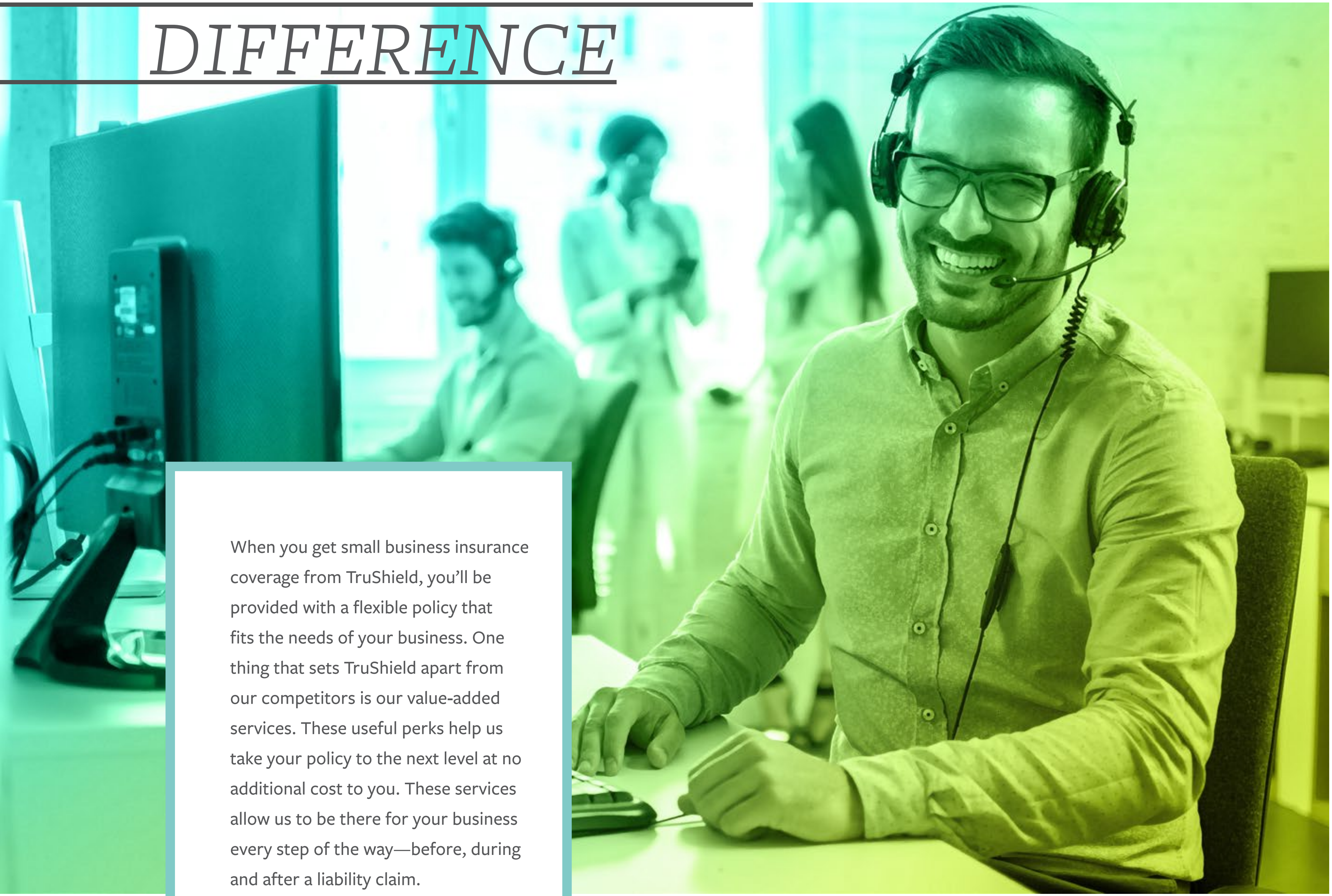
- A hacker gains access to your company's private information including customer information, client information or employee information, and threatens to sell or disclose it.
- A hacker encrypts or threatens to encrypt electronic data on your company's computer system, preventing authorized access to 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.

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!

trushieldinsurance.com
1.844.429.9480

@trushieldins
@trushield
@trushieldins

Stuff from our legal team

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.