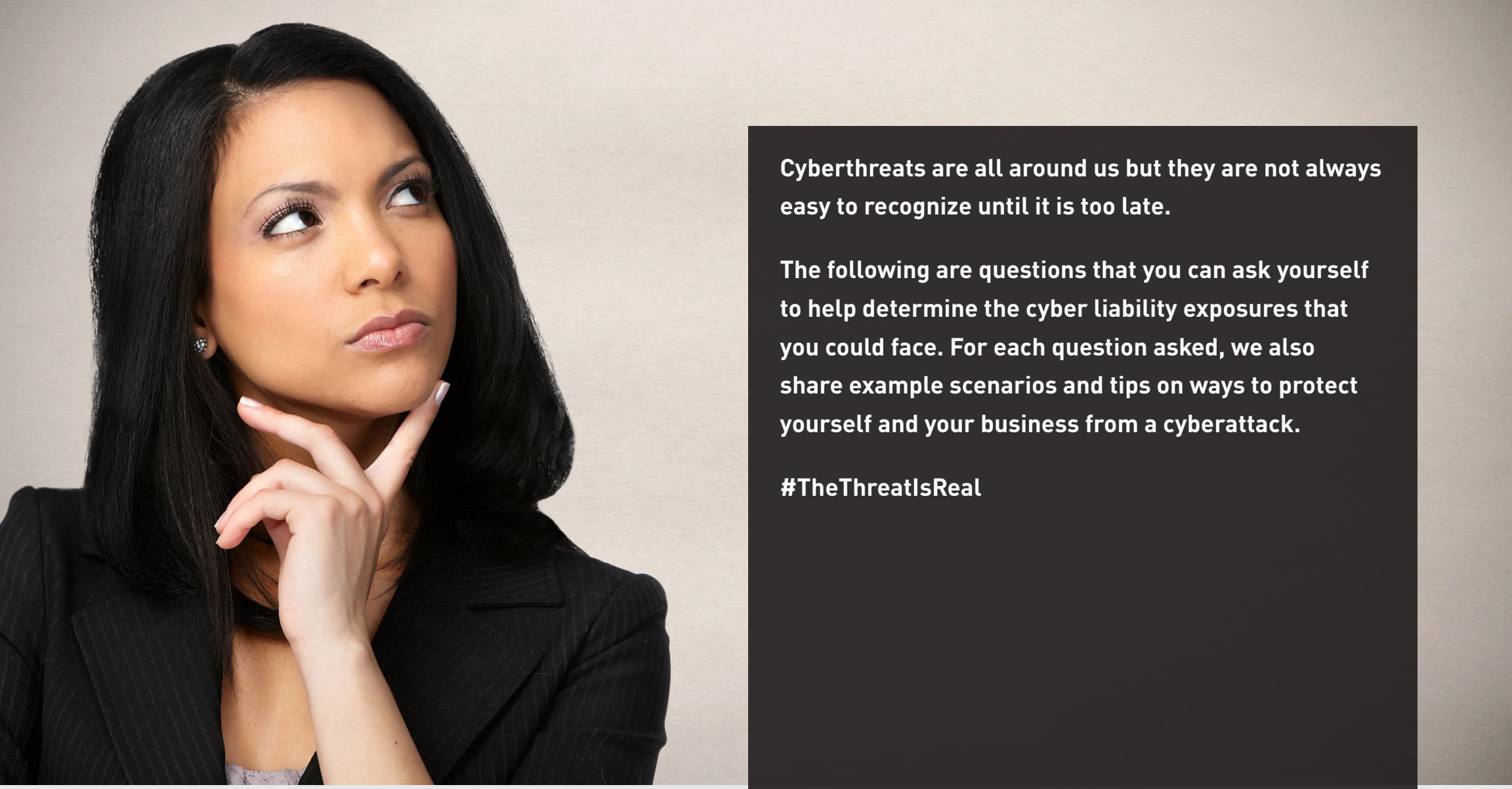
# Cyber liability exposures

## How to protect you and your business

VICTOR



Cyberthreats are all around us but they are not always easy to recognize until it is too late.

The following are questions that you can ask yourself to help determine the cyber liability exposures that you could face. For each question asked, we also share example scenarios and tips on ways to protect yourself and your business from a cyberattack.

#TheThreatIsReal

# 1. Do you use computers, networks or mobile devices?

**If so, in the event of a cyberattack, the following are some of the exposures that you could face:**

## Extortion costs and business interruption

### Example scenario

A hacker finds a way to access your computer and personal information – thereby making your computer unusable. The hacker also holds your personal information hostage, which leaves you at a complete loss and at the mercy of the hacker. Your information is completely inaccessible and unusable.

### Tip

As added protection from hackers, ensure that you encrypt your sensitive data (i.e., confidential or personal information) and have security protection in place such as firewalls, intrusion detection, anti-virus and anti-theft software for your computer or any technology device. Do periodic audits to test and analyze system vulnerabilities. Have a comprehensive incident response plan in place to address the breach and mitigate its impact on your business. Use a secure Wi-Fi; don't use open or publicly accessible Wi-Fi as this makes you vulnerable to hackers. Remember to practice regular backup protocols (i.e., save your files on another secure and remote drive) so that you are not at a complete loss in the event of a cyberattack.

## Social engineering schemes

### Example scenario

A bad actor is successful in deceiving and publicly releasing sensitive information about you and your company – thereby causing a financial loss for you and your business.

### Tip

Ensure that you and the employees at your company are aware of cyberthreats. Have sound security protocols in place to address and prevent fraudulent schemes that could be perpetrated against you and your business. Do periodic phishing simulations to test and evaluate your organization's cyber exposures and vulnerabilities to cyberattacks. Employees are the best line of defence in the protection against cyberattacks. Awareness and training are key factors in helping to alleviate this threat.

## Reputational damage

### Example scenario

Your reputation and your business' reputation are jeopardized because of a cyberattack. Your clients lose confidence in you and your business. The cyberattack also results in a loss of income and trust in your company's brand.

### Tip

Be proactive in the protection of confidential or sensitive information, especially when this information is in your care. Don't wait for a claim to occur to implement proper security protocols. Prevention will help to mitigate potential, devastating impacts to your reputation and overall viability. Ensure that sensitive information stored on your computer and systems is well protected with encryption and security protection software. Do periodic audits and vulnerability assessments. If you are subject to a security or privacy breach, consult experts such as a breach coach and a public relations professional. A breach coach can help you navigate the cyberbreach while the public relations professional can help you mitigate the impact of the potential reputational damage to your business.

# 2. Do you collect or store confidential or personal information (or does someone do it for you)?


**If so, in the event of a cyberattack, the following are some of the exposures you could face:**

## Privacy regulatory fines & penalties

### Example scenario

You are found liable for a breach of privacy laws in Canada as per the *Personal Information Protection and Electronic Documents Act* (PIPEDA). You could be fined up to a maximum of $100,000 CAN because of the privacy breach.

### Tip

For your business, you should be aware of the different privacy laws where you operate and where your clients are located. Make use of legal counsel that specialize in cyber and data privacy laws. They can assist you in ensuring that you meet minimum requirements and duty of care to your clients and regulatory bodies. This will mitigate the risk of claims or costly fines in the case of a privacy breach.

## Privacy breach

### Example scenario

A privacy breach occurs at your organization. A hacker has gained access to confidential client information. You face regulatory fines and costly third party claims. And, even though the confidential client information is managed by someone else on your behalf, it did not relieve you of your obligations towards your clients. You could be looking at additional expenses such as notification costs to affected individuals and government bodies, legal costs, forensic expert costs, public relations consulting costs and credit monitoring and identify theft costs because of the privacy breach. In addition, you may need to incur overtime and expenditures such as hiring a call centre to address the privacy breach.

### Tip

Have secure protocols in place to properly protect and dispose of confidential or personal information. This includes encrypting this information and limiting access to such information only to authorized individuals as a first step. Use security protection application and ensure that it is up-to-date. Regularly test your computer and systems against vulnerabilities. Implement a business recovery, continuity and incident response plan in case of a privacy breach. Also, ensure that you and your organization's employees are adequately trained on privacy and security protocols. Consider consulting a cybersecurity firm to assist you in determining your vulnerabilities. Implement a sound cybersecurity plan with security protocols in place.

## Payment Card Industry (PCI) fines and penalties

### Example scenario

Your business processes credit cards. In doing so, your business is found to be in breach of PCI Security Standards because you failed to protect cardholders' confidential or personal information. This breach leads to suits and demands from financial institutions, credit card associations and payment card processors. You may have to pay costly fines and assessments under a Merchant Services Agreement.

### Tip

If you are processing credit cards for your business, ensure you meet PCI Security Standards. This includes protecting confidential or personal cardholder information in your care and following sound security protocol practices (also mentioned previously as a tip in the **Privacy breach** section).

# 3. Do you process funds electronically?

**If so, in the event of a cyberattack, the following are some of the exposures you could face:**

## Electronic processing of funds

### Example scenario

In the electronic processing of funds by your company, a client's information is compromised by bad actors. This could now lead to financial loss if your client's information contained credit card or banking information. The compromised information, which is now at the hands of bad actors, could also expose your client to identity theft. As a result, your reputation and your company's reputation could ultimately suffer. You could be faced with costly claims if your client alleges he or she suffered damage due to your negligence in allowing the cyberattack.

### Tip

Ideally, use a trusted ecommerce platform that will ensure that proper security protections are in place and that ongoing security and vulnerability assessments and monitoring are conducted at your company. Use HTTP with SSL (secure sockets layer) for your web platform to ensure that the link is encrypted between web server and browsers. This will also help ensure that sensitive, financial and confidential information that you are digitally storing in your computer systems remain private and secure. Finally, ensure that you are PCI DSS compliant. Keep your company's website updated with the most recent applications and patches to mitigate against potential cyberattacks.

# 4. Do you have a website, a social media account or do you publicly advertise?


**If so, in the event of a cyberattack, the following are some of the exposures you could face:**

## Defamation, libel and slander

### Example scenario

You are faced with personal injury claims because your website, social media and advertising content promotes alleged false truths, defamatory comments or reveals sensitive information.

### Tip

Ensure that you obtain proper permissions from third parties before communicating any information about them or their business including logos or photos of their products or services. Communicate fact and avoid biased opinions that could be seen as defamatory, which could also lead to reputational damage for you and your company.

## Infringement

### Example scenario

You improperly use someone else's copyright such as pictures, logo or text without their permission.

### Tip

Always do proper searches to avoid infringement when developing products including communications vehicles such as website. This also includes conducting proper searches when creating and publicly sharing print and digital material. Remember to obtain permission from third parties before using their proprietary information.

## Electronic theft or fraud

### Example scenario

A hacker or scammer uses your website and social media accounts to try and steal funds and potentially extort you and your clients. The hacker sends an email to your clients pretending to be you and asks for funds in return for your business services. Your client pays the hacker (thinking it is you). Your client never receives your business services.

### Tip

Protect yourself, and be wary of email messages from unknown or suspicious senders. Don't click on any link unless you have a reasonable basis to trust it, or if the email is originating from a well-established organization.

# 5. Do you have employees?

**If so, in the event of a cyberattack, the following are some of the exposures you could face:**

## Human element (human error)

### Example scenario

One of the employees at your business accidently clicks a malicious link in a business email that causes your computer and systems to be infected with a virus – thereby making your computer unusable (similar example mentioned previously in the section, Extortion costs & business interruption. The "human element" is one of the most common causes of cybersecurity breaches. Improper training, rogue employees and carelessness can all lead to human error, which can result in costly claims and financial loss to you and your company.

### Tip

Ongoing training and awareness are key to avoid human errors. Ensure that your company has security and privacy protocols in place and that your employees are aware of them. Test your employees periodically to assess this knowledge. Check for vulnerabilities. Consider a proactive approach when protecting yourself, your employees and your business from cyberattacks.

As you can see, these are just some of the cyber liability exposures that you could face because of the technologies, processes and people that you have in place to run your business. Whether you own or manage a business, make sure you have cyber liability coverage to help protect yourself and your company from cyberattacks.

#TheThreatIsReal

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

- Victor (formerly ENCON) Cyber Insurance
- COVID-19 Resources
- Infographic: "Typical day in the life of a business owner"
- Infographic: "Cyberattacks: A threat to all businesses"
- Guide: "Cybersecurity: Work securely from home"
- Animated video: "A day in the life of a business owner in a cyberworld"
- Video: "Victor experts share preventative measures as cyberattacks on the rise."

## Visit us at victorinsurance.ca to learn more.