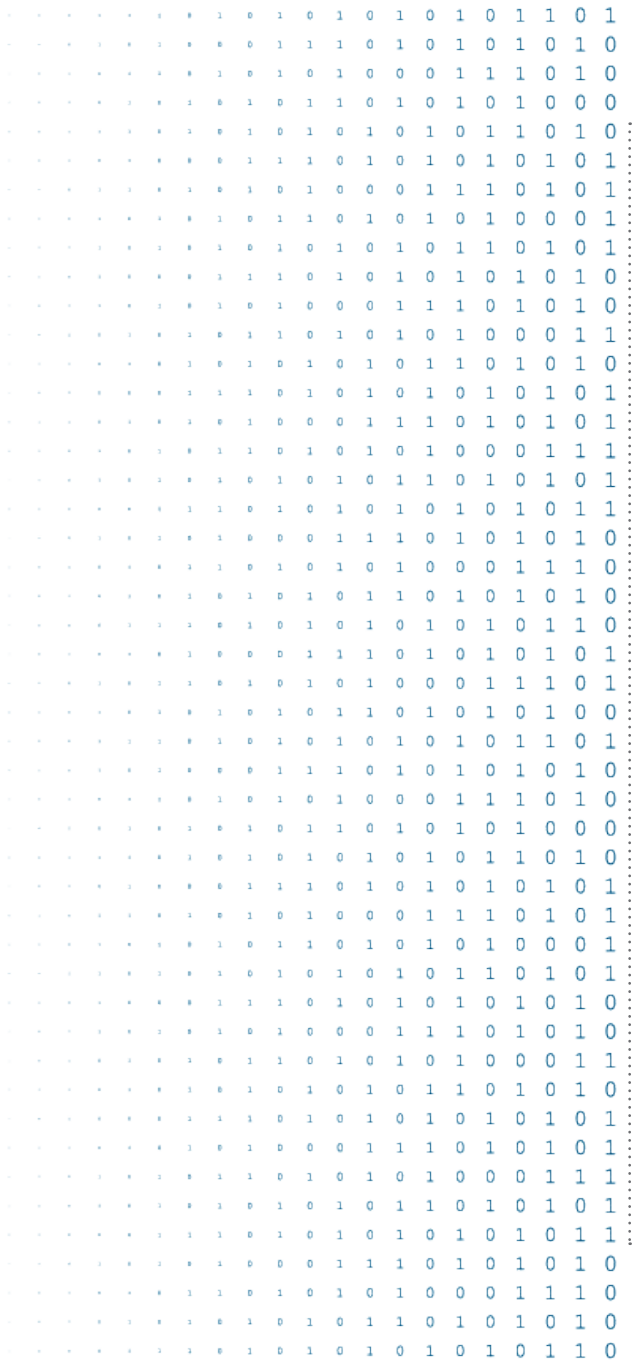
The first 48 hours:

# How to effectively respond to a **data breach**



A data breach can cause any business owner a great deal of stress. And to make matters worse, some cyber attacks are not immediately visible. Recent research pegs the average time to identify a breach at 196 days, and it often takes over two months to contain it.

That's why it's so important to have a plan in place for when you discover a breach, so you know your next steps immediately. Because any business can suffer from a cyber attack suddenly, a solid response plan is vital in order to avoid sustained damage and loss.

This whitepaper will outline what you can expect in the first 48 hours following a data breach. It will explore what a response plan can do for your business, teach you how to build it and put it in action and review the next steps to take towards recovery. With these tools, you will be equipped to develop a succinct and practical response plan to help your business during and after a data breach.


01
PLAN TO
SAVE

When it comes to a data breach, time is money – quick, well-organized responses often end up costing less. So, if you invest in a sound data breach response plan now, you may find that it pays for itself several times over in the years ahead.

A well-developed, thoroughly tested response plan can impact your post-breach costs more than you might imagine. Ponemon Institute's 2018 study found that leveraging an incident response team was particularly helpful, saving companies an average of $14 per compromised record from the average per capita cost of $148.

Why? Because activities like incident forensics, communications, legal expenditures, and regulatory mandates account for a big chunk of total data breach costs.

Outside experts can play a critical role in your plan, but so can those within your organization. Reacting and recovering is a team effort from start to finish, and the two days that follow a data breach are crucial.

Knowing just what lies ahead can help you prepare much more effectively.

When it comes to a data breach,

# time is money— quick, well-organized

responses often end up costing less.

02

# YOUR ACTION PLAN

**As soon as you suspect a breach, it's time to spring into action.** Taking smart, measured steps in the hours following the breach can help you limit the damage, halt the negative effects, and position your business to recover more quickly and thoroughly.

While there are **four main steps** in a data breach action plan, there's a lot that goes into each of those steps. This means you need a well-prepared team at the ready – the more allies you have, and the more everyone is aligned, the stronger your chances of emerging without lasting damage to your business, your reputation, and your bottom line.

Taking smart, measured steps
in the hours following

the breach can help you limit the damage,

halt the negative effects, and position your business to recover more quickly and thoroughly.

# STEP 1: CONTAIN

There's been a breach – your first job is to stop the damage from continuing. You'll need to take immediate action with the help of IT, security, and personnel measures.

**At this point, you have three vital tasks:**

1. Preserve metadata (that is, data that provides information about other data).
2. Retain, segregate, and preserve documentation (swapping hard drives of affected servers is one way to do so).
3. Involve legal counsel.

While it may seem premature to address liability concerns, it's important to loop in legal counsel at an early stage. If privacy concerns develop, having breach counsel under privilege from the get-go will help preserve any information found at this stage, preventing if from being discovered.


The next step in your response will be to assess the situation. This requires more than a quick glance: you'll need to gather information on what was affected and how, and be careful not to make assumptions.

### What Data Was Affected?

You need to know what data was affected, not only to understand the extent of the problem but also to determine whether you're obliged to notify your customers and employees. "Phone book data" (like name and address) may not trigger a notification obligation, but if sensitive information is leaked (think social insurance numbers or account numbers), those people are exposed to more risk – and you should take that very seriously.

### How Did The Event Happen?

Phishing. Hacking. Social engineering. These are the type of attacks that news outlets latch onto, but they're not always to blame for a breach. Cloud computing is generally considered a more secure technology in terms of cyber risk, but it's not infallible: while cloud providers follow security standards, those standards aren't necessarily reflective of Canadian business security needs.

Even well-intentioned employees can make mistakes: laptops are misplaced, passwords are weak, or attachments that look valid are opened. In other cases, there could be malicious intent. For example, a resentful or opportunistic employee could install key loggers on your computers to collect dozens of passwords. It's important to consider all possible gateways that could have led to the breach.

***Is your network vulnerable to phishing attacks? Learn more about the growing risk.***


## Can You Fix The Problem Yourself?

Once you get a handle on the nature and extent of the breach, you can decide how to proceed.

Your IT department's role might depend on the cause of the breach. For instance, if accidental or intentional human error caused the breach, your IT experts will likely need to focus on:

- Determining what data was exposed or leaked
- Documenting the technical aspects of the event

If technology is to blame for the breach, your IT team will also work to stop the flow of data. This task may require the help of a specialist computer forensics vendor, who will be able to dig deep into your technology and free up your in-house teams to tend to your vital security systems.

## Stay Calm And Keep Quiet

If you think you know where the problem lies, stop right there. It's important not to act hastily. Turning off a compromised server could destroy essential evidence, and firing a malicious employee could cost you leverage in an investigation.

Sometimes it can be better to allow the event to continue, monitoring how your data is being extracted and used. This sit-and-wait approach can help you recover more swiftly and help you notify those who need to be informed. However, this isn't the right approach for every breach. If ransomware is involved, you would likely want to terminate the network connection right away and attempt to restore data backups. Not sure what path to take? Your cyber experts and legal counsel will help you decide how best to proceed, so lean on them for information before making a call.

## Protect Privilege

Legal counsel is an important ally in the earliest stages of your data breach. After all, these are the experts who can help you protect privileged information uncovered during the investigation stage, as well as inform the necessary parties of anything they may need to know.

You might need both internal and external legal help to respond to a breach involving sensitive information. Inside legal counsel is familiar with your business, but they may rely on outside counsel for their expertise on privacy and regulation issues.

Pairing your internal legal expertise with that of an outside firm can be impactful, especially when the external counsel has experience with cyber security and privacy issues and knowledge of insurance coverages and regulatory matters.


Your legal team will play an important role in communicating the effects and extent of the breach – there may be statutory obligations to abide by – but other key personnel must help with vital post-breach communication and notification, too.

An adequate response to a data breach could take weeks or months. If you can't justify diverting your internal employees from their revenue-generating tasks to manage your breach response, you'll need to call on outside experts in breach response management who can take on the extra work and streamline your response plan with sound expertise.

## Evaluate Risk of Significant Harm

As of November 1 2018, Canada's federal Personal Information Protection and Electronic Documents Act will require organizations to notify affected individuals and organizations of certain data breaches that create a real risk of significant harm. The breach must also be reported to the Privacy Commissioner of Canada, and records of the breach will need to be maintained.

The act makes it more important than ever for companies to determine their legal obligations to evaluate the risk of potential significant harm. If there's no risk, no notification is required – but you can't assume that's the case without careful consideration.

## External Communications

A public relations (PR) team can gather facts from your security or digital forensics team about the extent of the breach, and work with legal counsel to craft an appropriate message for the public. Like legal counsel, your public relations effort could combine internal experts and outside specialists to cover all your bases.

How well-versed is your in-house PR team in crisis communications? Can they divert attention away from their daily responsibilities to address the data breach? What work can they afford to put on hold while the crisis is managed? Unless your internal team has assembled a clear and comprehensive communications plan for a data breach of this sort, you may want to contact an experienced PR firm to help manage communications and minimize reputational damage. They can guide your media response and any other necessary post-breach communications.

## Internal Communications

While your PR team handles external communications, your human resources (HR) team oversees your employee communications. HR should be briefed on developments following the breach, and the PR team can help devise talking points for HR to use with employees.

If your organization is large, there may be more work than your internal HR department can handle. If the volume of employee inquiries is high, you can set up an outsourced perimeter contact center that can handle basic first interactions. Callers who aren't satisfied with scripted answers can be escalated to your internal HR department for more personal treatment.

## Notifying Directors, Regulators, and Stakeholders

Your PR, IT, and legal teams must inform your board members of the information that's been shared with the public, and keep them informed with frequent updates on developments and communication plans. Once your board is briefed on how to respond to inquires from the media, you can be confident that your message is aligned.

If you've determined that there's a real risk of significant harm, you'll need to notify any affected individuals or organizations, along with the Privacy Commissioner, which can bring on extra expenses. Since unforeseen costs can impact stakeholders, they should also be notified.

Board members may have liability insurance to help with costs arising from legal action. You'll want to consult with your legal team to see if you have coverage that may apply after your breach.

## Who's in Charge?

Someone needs to stay at the helm during your data breach response – who will that be? Managing your response is a big task, considering the whole process can take weeks or months to resolve. In many cases, you can minimize the impact to your business and customers by keeping your staff in their established roles, so choose a response leader at the start and stick with the supporting structure of internal and external experts you've set up.

# STEP 4: REMEDIATE

Once you've come to terms with the scope of the situation, and stymied any ongoing data leaks, you can turn attention to your recovery. This will involve recovering lost data, preventing more loss, and understanding the varied repercussions of the breach.

**You'll need to:**

- Take steps to recover data
- Take steps to prevent further disclosure of data

In many cases, this will call for expert guidance and hands-on help.

## Access Credit Monitoring Services

Offering credit monitoring to potentially affected parties is a customary practice, and a measure of good faith. Companies who facilitate the credit monitoring process after a breach also help to build a defence to use if they're met with a class action lawsuit: determining who was financially impacted during the data breach will more accurately determine the extent of the damage.

## Choose Your Recovery Partners Wisely

Data breaches can require complex responses, and there's no reason to go it alone. However, you also don't want to team up with just anyone. Instead, take the time to find allies who can help you avoid further problems, deal with the fallout efficiently, and get your business back on track as soon as possible.

If you decide to involve vendors in your recovery effort, resist the temptation to work with the first one who answers your call. Before you decide to accept their help, ask about their experience with your type of breach, posing questions like:

- How many data breaches have you responded to?
- How severe were the breaches?
- Do you work with insurance companies?
- Can you provide a specific selection of services, or is it a package deal?
- What are your contract processes and terms?

Some vendors require a per-breach minimum, which could mean you end up paying more than necessary. It's important to take the time to clarify the terms and obligations involved in the vendor relationship before signing up for anything.

## Plan For Litigation

There may be laws governing who you must notify after a breach. This is something to investigate beforehand, so you know what will be expected of you once you contact law enforcement to report your breach.

Unfortunately, legal fallout is common after a data breach, and that can be both stressful and expensive for your business. Have a plan in place to handle any lawsuits that may come your way – this is where the right business insurance can come to your rescue, shouldering some of the financial burden that could severely impact your bottom line.

Legal fallout is common after a data breach, and that can be both stressful and expensive for your business.

# 03
# REVIEW AND PLAN

**Beware:** cyber threats continue, evolve, and mutate. It's virtually impossible to guarantee your business will avoid another data breach, no matter how extensive your resources or coordinated your response. In fact, Bell Canada suffered two data breaches within a year of each other. However, by reviewing what you've learned – and modifying your current routine accordingly – you can help reduce the likelihood your defenses will be breached again.

### Memory Fades – Keep a Record

Documentation helps you respond to future complaints, audits, and investigations. Since there can be differences of opinion regarding what constitutes a breach and the appropriate subsequent course of action, you'll want to show your process, analysis, and reasoning in case you need to defend your actions down the road.

***Process***

When you open your investigation, create a timeline: an ordered account of events will help to recount what happened when, which can be an important asset when memories get fuzzy. Consider documenting everything, including the minutes of early internal phone calls.

Your security team can work to determine the type of data that was exposed and the extent of the exposure. Include all technical support decisions and work in an appendix to the account.

***Analysis***

Once you've clarified the scope of the event and determined any notification regulations you need to abide by, spell out exactly what happened, how you've responded, and why. This way, all the aspects of your event response will be clear when you revisit this record in the future.

By reviewing what you've learned–and modifying your

current routine accordingly–

you can help reduce the likelihood your defenses will be breached again.

***Reasoning***

It's a good idea to not only consider the risk or hazard exposure, but compile those considerations in a clean, concise report. What potential harm could your customers or employees have been exposed to? If you're audited or investigated by a regulator, you can show the effort you made to establish the impact on your customer and employees, as well as the steps you've taken to notify the affected parties and resolve the issues.

## Improve Security

So, you've wrapped up your data breach response and you're ready to get back to business as usual. This is a great opportunity to make sure your operations are compliant, and that your security measures satisfy requirements.

Audit your security measures at least once per quarter against the latest threats by:

- Keeping your systems and software updated with the latest security patches.
- Engaging an external penetration testing service to feign an attack on your system. Based on the results, they'll be able to recommend ways to shore up your weaknesses.

## Focus on Your Staff

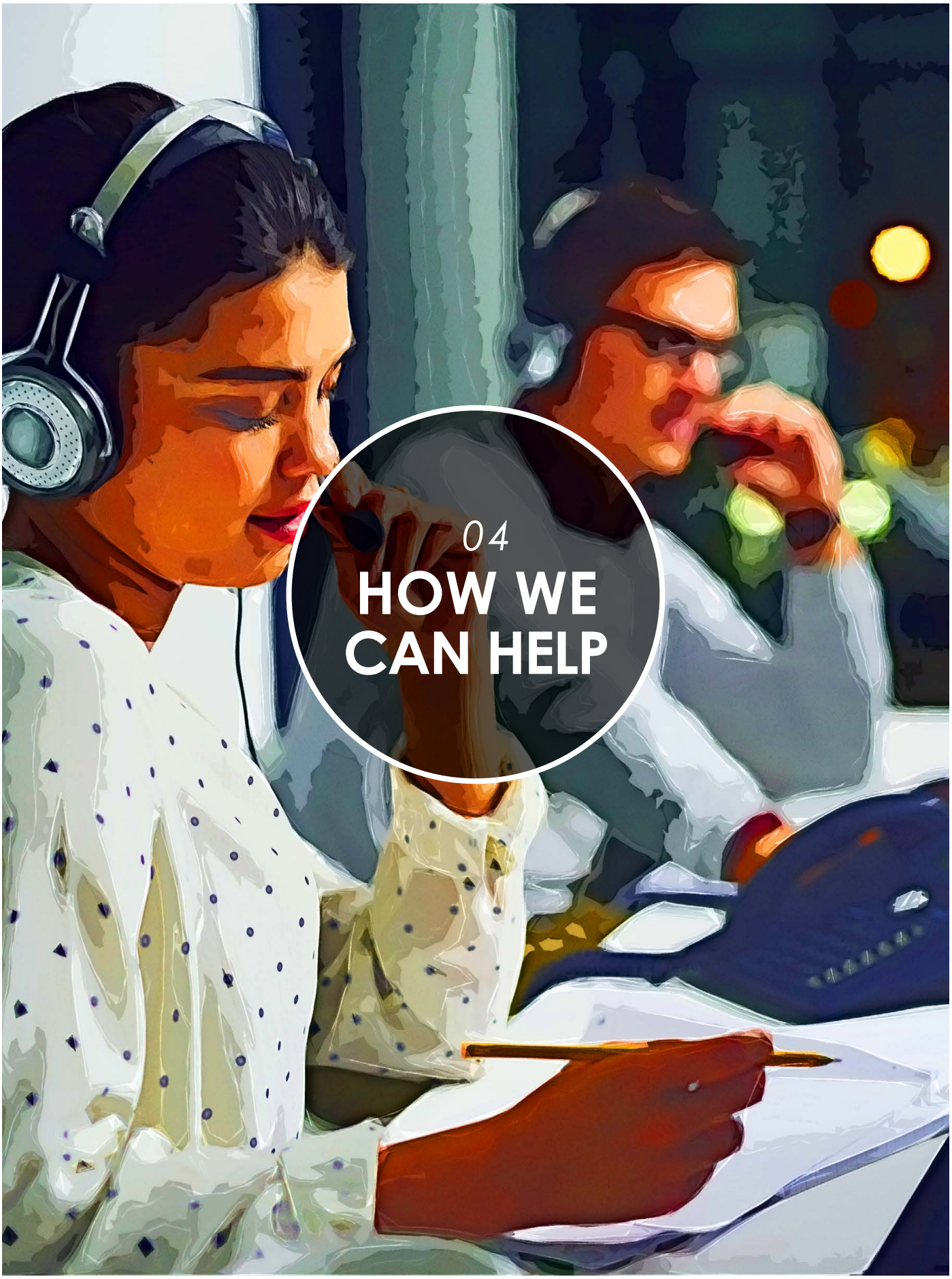
Your employees can be your weak link or your first line of defense. Take the time to educate and train your staff, and do so continuously – education is ongoing, and one training session is simply not enough to maintain a cyber-savvy workforce.

Keep your people up to date on risks, inform them of security expectations, and practice your response with mock breach scenarios that put your plan to the test.

**Here are some best practices to help your employees safeguard your business:**

- Provide an online learning platform with relevant training modules suited to your industry.
- Track your employees' progress (for internal reference and external audits).
- Encourage strong and unique passwords, and prompt employees to change them regularly.
- Test employees to recognize phishing attempts.
- Practice, practice, practice. Data breach simulations can help ensure the team is in tune with your plan and ready to spring into action at a moment's notice.

You'll also want to avoid a few common mistakes that can stall your improvement efforts. Sit-and-listen presentations can be dry, and they often fail to engage the audience – this won't do much to prepare your employees for a crisis. Also, don't neglect to assess comprehension and alertness; take the time to help your staff thoroughly understand the plan and where they fit into it.



*04*

# HOW WE CAN HELP

**Taking precautions against potential data breaches is vital, but sometimes, despite your best efforts, things can go wrong. That's where the right insurance protection comes in.**

As the world becomes increasingly digital, Ransomware, malware, and other targeted attacks have become more sophisticated and far-reaching. A single attack can cause a business serious financial strain. Having the right coverage in place can help ensure that legal fees, fines, repair costs, and business interruption expenses do not fall solely on your business' shoulders.

That's why Federated Insurance has developed a cyber risk insurance product together with CyberScout to protect your bottom line should you suffer from a cyber attack. Our coverage also gives you access to extensive cyber resources, reactive assistance, and personalized guidance.

Federated Insurance customers also have unlimited access to our Cyber Assist* service at no additional cost. This service is designed to help businesses with incident response planning, crisis management, notification assistance, and media relations consulting.

At Federated Insurance, we're committed to providing comprehensive policies and extensive information on risk management practices to help ensure your company runs smoothly.

## Our coverage also gives you access to

extensive cyber resources, reactive assistance, and personalized guidance.

*Services provided by CyberScout. Services are not an insurance policy. Not all policies are eligible, services are not included in any cyber extension or endorsements, contact us for details.

Federated Insurance

Knowing your business matters.

To learn more about our offerings and how we can help your business achieve its potential, contact us today!

Federated Insurance

1.844.628.6800

www.federated.ca