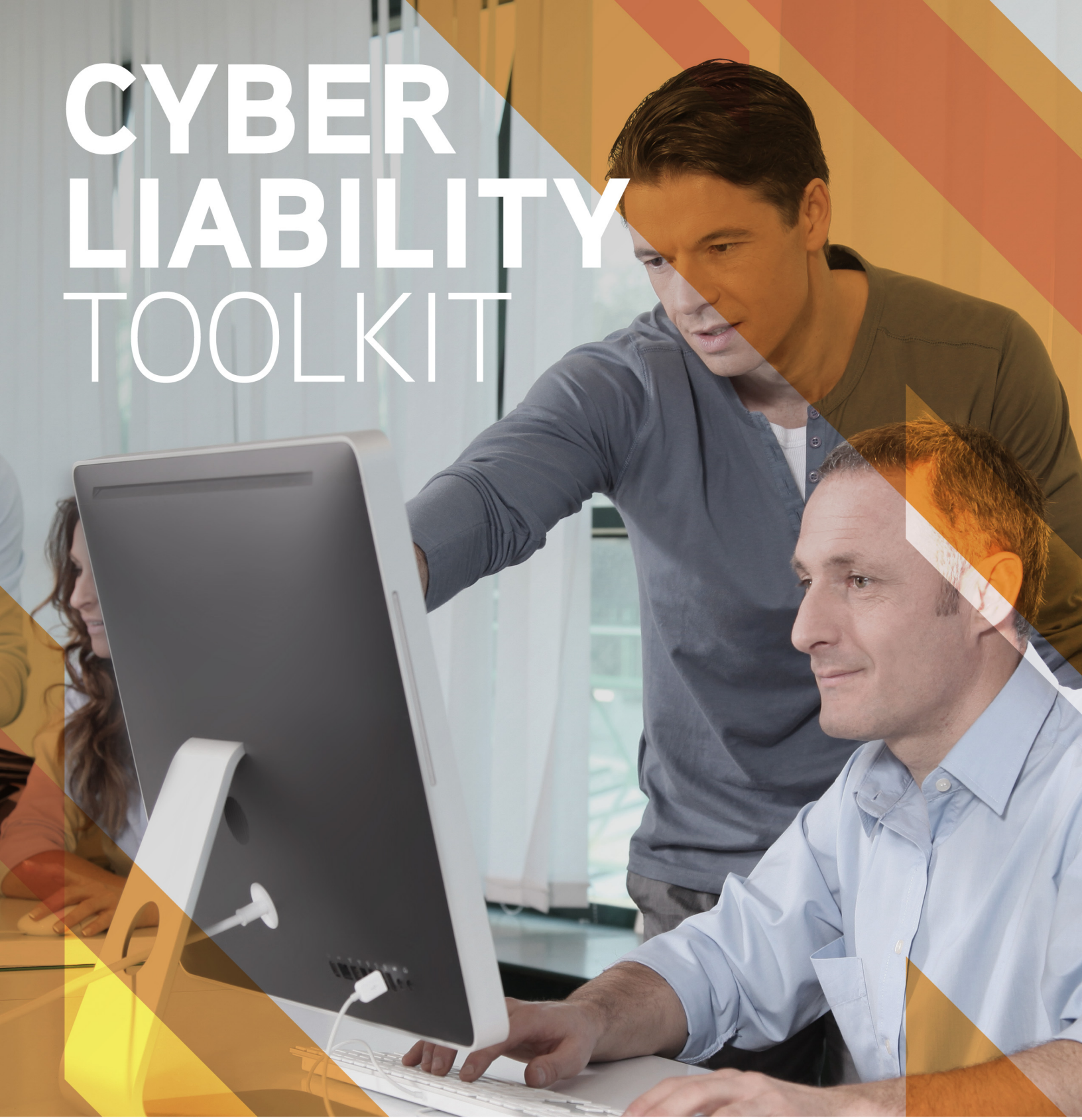
CYBER LIABILITY TOOLKIT



THOR INSURANCE & REGISTRIES

Provided by: Thor Insurance & Registries Ltd
PO Box 299
Tofield, AB T0B 4J0
Tel: 855-662-3465

How to Use This Guide

Businesses both large and small need to be proactive in order to protect against growing cyber threats. As larger companies take steps to secure their systems, smaller, less secure businesses are becoming increasingly attractive targets for cyber criminals.

This planning guide is designed to help employers protect their business, information and customers from cyber threats. This guide is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. It is generally recommended that businesses using sophisticated networks with dozens of computers consult a cyber-security expert in addition to using this cyber security planning guide.

The checklist at the beginning of the guide outlines key action items that should be taken to ensure cyber security. The title of each section of the checklist corresponds with an educational article housed in this toolkit that can be located for more detailed information. Take advantage of the linked table of contents below for easy toolkit navigation.

Table of Contents

Cyber Liability Toolkit Checklist

Complete the following checklist as you utilize the Cyber Liability Toolkit. This checklist serves as a reminder of risks and issues your business may face. Work with your IT department to implement and update cyber policies and ensure employees are properly trained on best practices for data security.

Understanding and Preventing Data Breaches	Yes	No	Comments
Do you know what a data breach is? Would you be able to recognize it if it occurred?			
Do you know your responsibilities in the event of a data breach?			
Have you established organizationwide procedures to isolate and contain a data breach to limit damage?			
Do you have procedures in place to notify affected parties and appropriate regulatory bodies?			
Do you regularly review your cyber security policies and procedures?			How often?

Spam, Phishing and Spyware Defined	Yes	No	Comments
Do you have an email and internet usage policy?			
Are your employees trained to recognize electronic scams such as spam, phishing and spyware?			
Do you take measures to keep electronic scam prevention top of mind for employees?			List measures:

Defining, Identifying and Limiting Cyber Crime	Yes	No	Comments
Do you stay up to date on emerging cyber risks?			How?
Are you familiar with any computer intrusions, such as viruses, worms, Trojan horses, spyware and logic bombs?			List computer intrusions you know of but are not familiar with:
Does your organization use firewalls, routers, anti-virus programs, policies or any other means to limit intrusions?			List:

Keeping Your Data Secure	Yes	No	Comments
Have you identified the types of data your business keeps on file?			List data types:
Have you classified your data?			
Do you know where your physical and virtual data is stored?			Locations:
Have you assessed the security of your data transfer and storage procedures?			
Have you established data access restrictions based on employee role?			
Do you use more than one security mechanism to protect your data?			List mechanisms:
Is your data backed up regularly?			

Physical Protection of Cyber Assets	Yes	No	Comments
Have you secured your organization's facilities?			List methods:
Do you require badge identification for visitors?			
Do employee computer screens face away from public traffic?			
Do you use cable locks and/or tracking software to prevent laptop theft?			
Have you established procedures to minimize and safeguard printed materials containing sensitive information?			
Is your mail centre secure?			
Do you have procedures in place to securely dispose of electronic equipment and papers containing sensitive material?			
Are employees trained in all facility security policies and procedures?			

Mobile Device Security	Yes	No	Comments
Do your mobile devices have complex passwords or PINS with time-sensitive, automatically locking security features?			
Are all mobile devices set to reject open Wi-Fi or Bluetooth connections without user permission?			
Have you established a Mobile Device Policy and trained employees on it?			
If you allow employees to use their own mobile devices, have you established a Bring Your Own Device Policy?			
Are all mobile devices kept updated with the most current software and anti-virus programs?			
Is content from mobile devices backed up regularly?			

Safely Disposing of Your Devices	Yes	No	Comments
Do you have set procedures in place to properly remove information from and dispose of your devices?			
Do you use one or a combination of the following methods to dispose of your devices? • Physical destruction • Overwriting • Restoring to factory settings • Sending to a specialist • Formatting			List methods:

Protecting Your Email	Yes	No	Comments
Do you have a spam filter set up?			
When sending sensitive information through email, is the information properly encrypted?			
Do you have an email retention policy?			

Network Security	Yes	No	Comments
Have all devices on company networks been identified?			
Have boundary points been identified and evaluated to determine best security controls?			
Is the network separated from the public internet with strong user authentication mechanisms and policy enforcement systems such as firewalls and web filtering proxies?			List:
Are monitoring and security solutions such as anti-virus programs and intrusion detection systems used?			List:
If cloud-based services are used, have you consulted about the terms of service with your providers to ensure company information and activities are fully secure?			
Is your organization's Wi-Fi secure and encrypted?			
Are all systems, software and equipment updated in a timely fashion (including all patches and firmware upgrades)?			
If remote access is allowed, is it secured through a Virtual Private Network (VPN) and accompanied by two-factor authentication?			
Do you have a safe-use policy regarding flash drives?			

Website Security	Yes	No	Comments
Have you developed appropriate web management security practices and policies?			
Is a team assembled to manage the deployment and continued operation of the web server and supporting infrastructure?			
Do allwebserver operating systems and applications meet your security requirements? Are servers configured to meet your specific security needs?			
Do you employ a strategy to prevent inappropriate or sensitive information from being published on the website?			
Are there procedures in place to prevent unauthorized access or modification to the site?			

Understanding and Preventing Data Breaches

What do Kroger Co., Best Buy Canada, AbeBooks and major banks and credit card issuers like Barclays Bank and Capital One have in common? All these companies have been victims of a data breach in 2012, totalling millions of stolen records that include personal information such as social insurance numbers, credit card numbers and bank account numbers.

If your company handles critical assets such as customers' personal data, intellectual property or proprietary corporate data, you are at risk of a data breach. It doesn't matter if you are a Fortune 500 company or a small "ma and pa" shop, cyber thieves are always looking for their next score. It is often assumed that smaller businesses can escape attention from cyber crooks, but according to the Symantec SMB Threat Awareness Poll Global Results, 40 per cent of data breaches were at small to mid-sized businesses. No company of any size is completely safe from a data breach.

Data Breach Basics
A data breach is an incident where private data is accessed and/or stolen by an unauthorized individual. Data can be stolen by a third party, such as a hacker, or by an internal actor (perhaps a disgruntled or recently fired employee).

Data Breach Prevention Techniques
To reduce the chance for a data breach, it is wise to develop an IT Risk Management Plan at your organization. Risk management solutions should use industry standards and best practices to assess hazards from unauthorized access, use, disclosure, disruption, modification or destruction of your organization's information systems. Consider the following when implementing risk management strategies at your organization:

- Create a formal, documented risk management plan that addresses the scope, roles, responsibilities, compliance criteria and methodology for performing cyber risk assessments. This plan should include a description of all systems used at the organization based on their function importance to the organization, and the data stored and processed within them.
- Review the cyber risk plan on an annual basis and update it whenever there are significant changes to your information systems, the facilities where systems are stored changes, or other conditions occur that may affect the impact of risk to the organization.

Not all companies have the resources to create and implement a fully customized plan. However, there are many simple, cost-effective steps any business can take to help prevent a data breach.

- Never give sensitive information like social insurance numbers or credit card numbers out over the phone unless you can verify the identity of the person on the other line.
- Shred all credit reports and other sensitive data before disposal.
- Educate employees about phishing and pharming scams. Remind them not to click on anything that looks suspicious or seems too good to be true.
- If your company doesn't have an IT department, hire an outside company to set up the proper security measures for your computer network.
- Always monitor credit reports and other financial data for the company. If you see things that don't belong, investigate.
- Do not allow employees to write down passwords in the office.
- Always encrypt sensitive data.

What to Do if You Have a Data Breach
It is common to have an "it will never happen to us" philosophy when it comes to data breaches. Unfortunately, that thinking can lead to lax security measures and carelessness when it comes to protecting sensitive information. If your company suffers a data breach:

For full access version, please contact us.

Contact Info

Thor Insurance & Registries
PO Box 299, 324 50th St.
Tofield, AB, T0B 4J0

Phone: 1(855)-662-3465

Thor Financial
450 Ordze Road
Sherwood Park, AB, T8B 1C9

Email: tjones@thorinsurance.ca