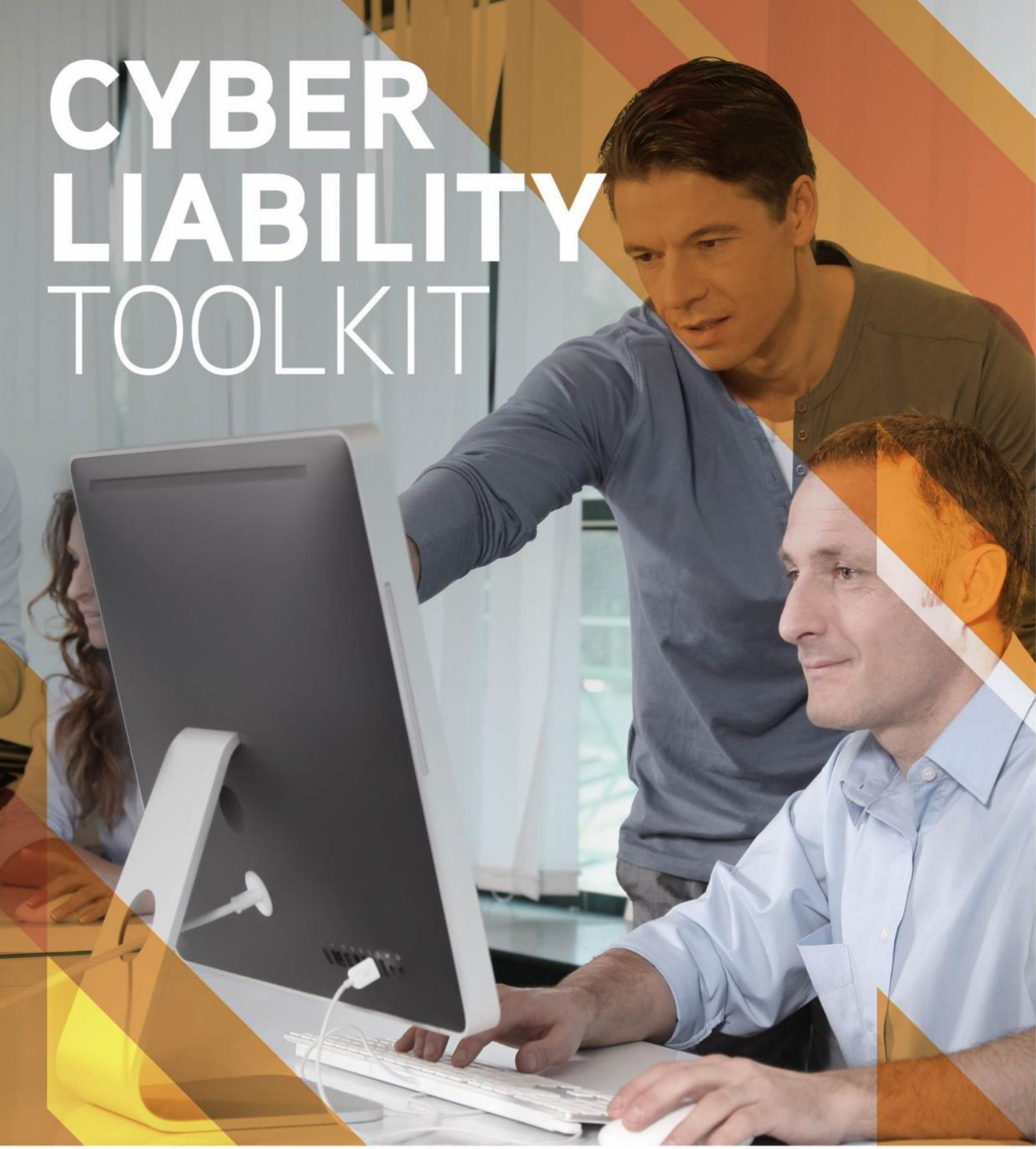
CYBER LIABILITY TOOLKIT



INSURANCE BROKERS

Robison

Challenging Convention

Provided by: Robison & Co Ltd

6 Rotherbrook Court, Bedford Road
Petersfield, Hants, GU32 3QG
01730265500
www.robison.co.uk

Design © 2014 Zywave, Inc. All rights reserved.

How to Use This Toolkit

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 toolkit 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 toolkit.

As you begin taking control of your cyber liability, use the checklist at the beginning of the toolkit and revisit it as you progress. You will also find sample policies at the end of the toolkit to help you implement your cyber liability initiatives.

Table of Contents

Cyber Liability Toolkit Checklist

Complete the following checklist as you utilise the Cyber Liability Toolkit. This checklist serves as an outline and a reminder of the risks and issues your business should be monitoring. Work with your IT department to implement and update any policies and make sure all employees are trained on best practices.

UNDERSTANDING THE RISKS

UNDERSTANDING AND PREVENTING DATA BREACHES	YES	NO	NOTES
Can you define what a data breach is? Would you be able to recognise it if it occurred?			
Do you know your responsibilities and what actions you should take if a data breach occurs?			
Have you established organisation-wide procedures to isolate and contain the breach to limit damage, including conducting a risks assessment regarding the data that was compromised?			
Do you have procedures in place to notify affected parties and appropriate regulatory bodies?			
Do you regularly review your cyber security policies and procedures to make sure everything is up to date?			How often?

DEFINING, IDENTIFYING AND LIMITING CYBER CRIME	YES	NO	NOTES
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 any computer intrusions you know of but are not familiar with:
Does your organisation use any of the following to limit intrusions? • Firewalls or routers • Antivirus programs • Policies			List :

SPAM, PHISHING AND SPYWARE DEFINED	YES	NO	NOTES
Do you have an email and internet usage policy?			

Are your employees trained to recognise electronic scams such as spam, phishing and spyware?			
Do you regularly remind or train employees to keep electronic scam prevention top of mind?			

IDENTIFYING AND MANAGING YOUR EXPOSURES: DATA

KEEPING YOUR DATA SECURE	YES	NO	NOTES
Have you identified what types of data your business holds and stores? This can include customer data, financial information, buying habits, preferences and much more.			List data types:
Have you classified your data into different categories to identify potential areas of vulnerability?			
Do you know where all of your data (including physical, website and virtual data) is stored?			Locations:
Have you assessed how secure your data transfer procedures and storage areas are?			
Have you established data access restrictions based on employee role?			
Do you use more than one security mechanism to protect your data?			List the mechanisms you use:
Is data backed up regularly to a secure location?			

PHYSICAL PROTECTION OF CYBER ASSETS	YES	NO	NOTES
Have you secured your organisation's facilities?			Methods:
Do you require badge identification for visitors?			
Do employee computer screens face away from public traffic?			
Do you use cable locks or tracking software to help prevent laptop theft?			
Have you established procedures to minimise and safeguard printed materials with sensitive information?			

Is your post/mail centre secure?			
Do you have procedures in place to properly dispose of papers containing sensitive materials?			
Do you have procedures in place to securely dispose of electronic equipment?			
Are your employees trained in all facility security policies and procedures?			

IDENTIFYING AND MANAGING YOUR EXPOSURES: DEVICES

MOBILE DEVICE SECURITY	YES	NO	NOTES
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 antivirus programs?			
Is content from mobile devices backed up regularly?			

SAFELY DISPOSING OF YOUR DEVICES	YES	NO	NOTES
Do you have set procedures in place to properly remove information from and dispose of your devices?			