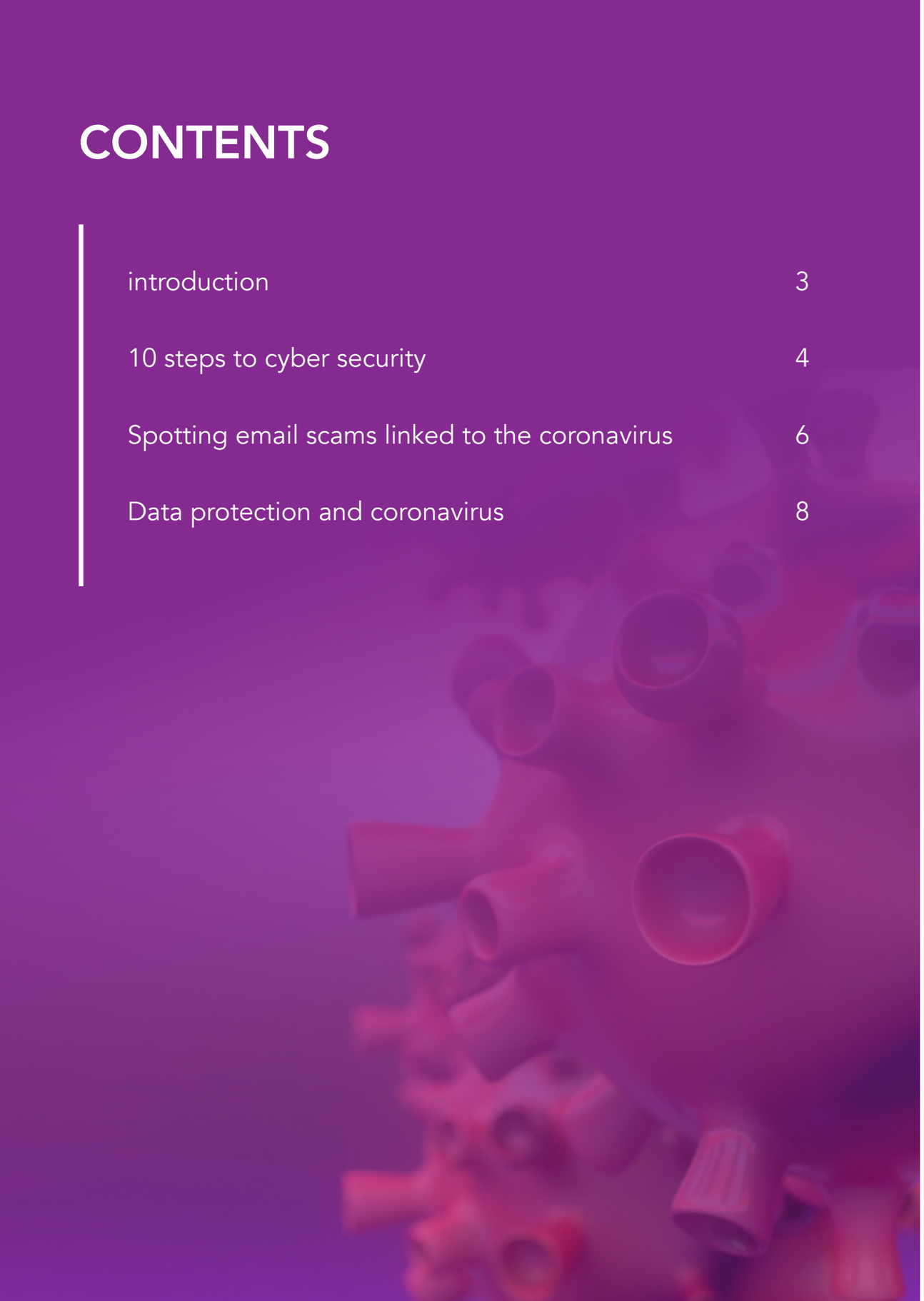
james & lindsay ltd

CYBER SECURITY:

GUIDANCE ON PROTECTING YOUR BUSINESS DURING THE COVID-19 PANDEMIC

CONTENTS

introduction	3
10 steps to cyber security	4
Spotting email scams linked to the coronavirus	6
Data protection and coronavirus	8



INTRODUCTION

With millions of employees now working from home, companies are having to look at how to keep as many business-critical functions running as possible while at the same time maintaining adequate security. New figures show that phishing attacks have risen 667%* in the UK in March. These attacks aren't just happening infrequently either, Government statistics show that 75%* of large organisations were hacked last year.

As your broker we want to not only provide you with advice on how to insure against cyber risks, but also to direct you to relevant support so that you can avoid issues from occurring in the first place. Within this pack we have collated guidance from a range of trusted sources that we hope will help to make a positive difference to your business during this difficult time.

If you have any specific queries, please contact us today. We are waiting for your call.

USEFUL RESOURCES FOR BUSINESSES

The information within this pack is by no means exhaustive and the situation changes daily. For up to date details, please refer to ongoing advice and support offered online:

The **CBI** is running a **daily webinar** specifically on their response to the Coronavirus outbreak. Each day they update on what they are doing to lobby the Government and offer support and guidance on topics such as access to finance and cyber risks. You can view the full catalogue of their insight here: www.cbi.org.uk/coronavirus-hub

The **NCSC** offers a huge amount of support for businesses and has created a **dedicated guide on working from home** securely. We have included some of their key guidance within this pack, but keep up to date at: www.ncsc.gov.uk

Securing your social media accounts is vital at the moment – take a look at the guide from the NCSC to ensure you are doing everything by the book: www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely

The **ICO** has collated an **FAQ guide on data protection** (included later in this pack). You can keep up to date with their evolving support by visiting their website or calling the hotline on 0303 123 1113.

The **Global Cyber Alliance** has pulled together its **top recommended actions** from the GCA Cybersecurity Toolkit that you can implement quickly. Click here to access the toolkit. workfromhome.globalcyberalliance.org/

KnowB4, a cyber education training provider, offers lots of **free tools and resources** on its website. Visit this blog to complete a range of phishing tests with your team and your clients, and view the on demand webinar to help you prepare for cyber risks.

Source:* **Barracuda Networks, a global security company

10 STEPS TO CYBER SECURITY

The following guide is taken from the NCSC website which includes a wealth of advice and support for businesses and individuals during this crisis. As the situation around COVID-19 is changing daily, for up to date guidance, please visit www.ncsc.gov.uk/collection/10-steps-to-cyber-security/the-10-steps

RISK MANAGEMENT REGIME

Why defining and communicating your Board's Information Risk Management Regime is central to your organisation's overall cyber security strategy.

SECURE CONFIGURATION

Having an approach to identify baseline technology builds and processes for ensuring configuration management can greatly improve the security of systems. You should develop a strategy to remove or disable unnecessary functionality from systems, and to quickly fix known vulnerabilities, usually via patching. Failure to do so is likely to result in increased risk of compromise of systems and information.

HOME AND MOBILE WORKING

Mobile working and remote system access offers great business benefits but exposes new risks that need to be managed. You should establish risk based policies and procedures that support mobile working or remote access to systems that are applicable to users, as well as service providers.

INCIDENT MANAGEMENT

All organisations will experience security incidents at some point. Investment in establishing effective incident management policies and processes will help to improve resilience, support business continuity, improve customer and stakeholder confidence and potentially reduce any impact.

MALWARE PREVENTION

Malicious software, or malware is an umbrella term to cover any code or content that could have a malicious, undesirable impact on systems. Any exchange of information carries with it a degree of risk that malware might be exchanged, which could seriously impact your systems and services. The risk may be reduced by implementing appropriate security controls as part of an overall 'defence in depth' approach.

MANAGING USER PRIVILEGES

Giving users unnecessary system privileges or data access rights means that if the account is misused or compromised the impact will be more severe than it needs to be.

BE CYBER SAFE:

DO NOT USE ANY CORONAVIRUS TRACKING MAPS BESIDES THOSE ON THE PUBLIC HEALTH ENGLAND WEBSITE. SOME MAPS INCLUDE MALICIOUS SOFTWARE THAT STEALS DATA FROM YOUR WORKSTATION.

MONITORING

System monitoring provides a capability that aims to detect actual or attempted attacks on systems and business services. Good monitoring is essential in order to effectively respond to attacks. In addition, monitoring allows you to ensure that systems are being used appropriately in accordance with organisational policies. Monitoring is often a key capability needed to comply with legal or regulatory requirements.

NETWORK SECURITY

The connections from your networks to the Internet, and other partner networks, expose your systems and technologies to attack. By creating and implementing some simple policies and appropriate architectural and technical responses, you can reduce the chances of these attacks succeeding (or causing harm to your organisation). Your organisation's networks almost certainly span many sites, and the use of mobile / remote working, and cloud services, makes defining a fixed network boundary difficult. Rather than focusing purely on physical connections, think also about where your data is stored and processed, and where an attacker would have the opportunity to interfere with it.

REMOVABLE MEDIA CONTROLS

Removable media provide a common route for the introduction of malware and the accidental or deliberate export of sensitive data. You should be clear about the business need to use removable media and apply appropriate security controls to its use.

USER EDUCATION AND AWARENESS

Users have a critical role to play in their organisation's security and so it's important that security rules and the technology provided enables users to do their job as well as helping to keep the organisation secure. This can be supported by a systematic delivery of awareness programs and training that deliver security expertise as well helping to establish a security-conscious culture.

BE CYBER SAFE:

AVOID CLICKING WEBPAGE LINKS IN ANY EMAILS THAT RELATE TO THE CORONAVIRUS. REPORT THESE TO YOUR IT TEAM AND GO TO THE RELEVANT WEBSITE INDEPENDENTLY.

BE CYBER SAFE:

BE VERY CAREFUL WHERE PAYMENTS AND DONATIONS ARE CONCERNED – IF YOU'RE UNSURE THEN VISIT THE WEBSITE DIRECTLY AND ONLY DONATE TO REPUTABLE SOURCES.

SPOTTING EMAIL SCAMS LINKED TO THE CORONAVIRUS

Phishing and scam emails are increasingly becoming an issue for many businesses as fraudsters try to capitalise on their vulnerability. To help you and your teams remain vigilant, we have collated guidance and resources below.

The following guide is taken from the NCSC website which includes a wealth of advice and support for businesses and individuals during this crisis. As the situation around COVID-19 is changing daily, for up to date guidance, please visit www.ncsc.gov.uk/guidance/home-working

Cyber criminals are preying on fears of the coronavirus and sending 'phishing' emails that try and trick users into clicking on a bad link. Once clicked, the user is sent to a fraudulent website which could download malware onto your computer, or steal passwords. The scams may claim to have a 'cure' for the virus, offer a financial reward, or be encouraging you to donate.

Like many phishing scams, these emails are preying on real-world concerns to try and trick people into doing the wrong thing. Please refer to our guidance on dealing with suspicious emails to learn more about spotting and dealing with phishing emails.

For genuine information about the virus, please use trusted resources such as the Public Health England or NHS websites.

WHAT TO DO IF YOU HAVE ALREADY CLICKED?

The most important thing to do is not to panic. There are number of practical steps you can take:

- Open your antivirus (AV) software if installed, and run a full scan. Follow any instructions given
- If you've been tricked into providing your password, you should change your passwords on all your other accounts
- If you're using a work device, contact your IT department and let them know
- If you have lost money, you need to report it as a crime to Action Fraud. You can do this by visiting www.actionfraud.police.uk.

BE CYBER SAFE:

ONLY VISIT TRUSTED WEBSITES, DON'T VISIT SITES FROM BUSINESSES YOU'VE NEVER HEARD OF. CHECK THE SPELLING OF WEBSITE NAMES OR, BETTER STILL, ACCESS VIA YOUR 'FAVOURITES'.

BE CYBER SAFE:

MAKE SURE YOUR PASSWORD HASN'T ALREADY BEEN BREACHED. YOU CAN CHECK USING THIS LINK: HAVEIBEENPWNED.COM/PASSWORDS

We have also taken note of the following scams and phishing attempts that are circulating at the moment:

- The Sophos Security Team reported a scam using an email that seemed to come from the World Health Organisation, including safety measures on the Coronavirus. The email includes a link to a page that has the WHO website embedded and includes a form which captures login information. Another seems to come from the UK Government offering a tax rebate. Click here for further details: news.sky.com/story/coronavirus-criminals-exploiting-covid-19-pandemic-with-email-scams-11959433
- INTERPOL has highlighted that criminals are stealing money from individuals and businesses by purporting to sell medical supplies such as masks online. Click here to read more: www.interpol.int/en/News-and-Events/News/2020/INTERPOL-warns-of-financial-fraud-linked-to-COVID-19
- There are also reports of fake charitable causes, counterfeit hand sanitisers and bogus telephone calls pretending to come from utility companies and banks. Click here to read more: news.sky.com/story/coronavirus-how-criminals-are-exploiting-the-covid-19-pandemic-to-scam-the-public-11962897

DO YOU KNOW WHAT A PHISHING OR SCAM EMAIL LOOKS LIKE?

TAKE A LOOK AT THE REAL-LIFE EXAMPLES BELOW FROM KNOWB4.

Phishing examples www.knowbe4.com/covid-gallery-phishing-examples

Scam examples www.knowbe4.com/covid-gallery-spam-scam-examples

DATA PROTECTION AND CORONAVIRUS: WHAT YOU NEED TO KNOW

The following guide was taken from the Information Commissioner's Office website. As the situation around COVID-19 is changing daily, for up to date guidance, please visit ico.org.uk/for-organisations/data-protection-and-coronavirus/

The ICO recognises the unprecedented challenges we are all facing during the Coronavirus (COVID-19) pandemic.

We know you might need to share information quickly or adapt the way you work. Data protection will not stop you doing that. It's about being proportionate - if something feels excessive from the public's point of view, then it probably is.

And the ICO is here to help – please see below for answers to the questions we're being asked. If you need more help, call us on 0303 123 1113.

During the pandemic, we are worried that our data protection practices might not meet our usual standard or our response to information rights requests will be longer. Will the ICO take regulatory action against us?

No. We understand that resources, whether they are finances or people, might be diverted away from usual compliance or information governance work. We won't penalise organisations that we know need to prioritise other areas or adapt their usual approach during this extraordinary period.

We can't extend statutory timescales, but we will tell people through our own communications channels that they may experience understandable delays when making information rights requests during the pandemic.

As a healthcare organisation, can we contact individuals in relation to COVID-19 without having prior consent?

Data protection and electronic communication laws do not stop Government, the NHS or any other health professionals from sending public health messages to people, either by phone, text or email as these messages are not direct marketing. Nor does it stop you using the latest technology to facilitate safe and speedy consultations and diagnoses. Public bodies may require additional collection and sharing of personal data to protect against serious threats to public health.

BE CYBER SAFE:

ACCESSING ORGANISATIONAL DATA OR YOUR WORK EMAIL FROM A PERSONAL DEVICE COMES WITH A HIGH RISK. WITH THIS IN MIND, USING PERSONAL DEVICES TO DO SO SHOULD BE AVOIDED.

BE CYBER SAFE:

LOCK YOUR SCREEN WHEN NOT USING YOUR WORKSTATION. IF A CHILD OR PET CORRUPTS ANY DATA OR SETTINGS, IT WILL BE DIFFICULT TO FIX REMOTELY.

More of our staff will be homeworking during the pandemic. What kind of security measures should my organisation have in place for homeworking during this period?

Data protection is not a barrier to increased and different types of homeworking. During the pandemic, staff may work from home more frequently than usual and they can use their own device or communications equipment. Data protection law doesn't prevent that, but you'll need to consider the same kinds of security measures for homeworking that you'd use in normal circumstances.

Can I tell my staff that a colleague may have potentially contracted COVID-19?

Yes. You should keep staff informed about cases in your organisation. Remember, you probably don't need to name individuals and you shouldn't provide more information than necessary. You have an obligation to ensure the health and safety of your employees, as well as a duty of care. Data protection doesn't prevent you doing this.

Can I collect health data in relation to COVID-19 about employees or from visitors to my organisation? What about health information ahead of a conference, or an event?

You have an obligation to protect your employees' health, but that doesn't necessarily mean you need to gather lots of information about them.

It's reasonable to ask people to tell you if they have visited a particular country, or are experiencing COVID-19 symptoms.

You could ask visitors to consider government advice before they decide to come. And you could advise staff to call 111 if they are experiencing symptoms or have visited particular countries. This approach should help you to minimise the information you need to collect.

If that's not enough and you still need to collect specific health data, don't collect more than you need and ensure that any information collected is treated with the appropriate safeguards.

Can I share employees' health information to authorities for public health purposes?

Yes. It's unlikely your organisation will have to share information with authorities about specific individuals, but if it is necessary then data protection law won't stop you from doing so.

CYBER INSURANCE COVER FAQS

Cyber breaches can affect any one of us that uses technology, both in our business and our personal life. No-one is immune, and cyber criminals are becoming ever more prevalent in our new virtual world as they attempt to capitalise on people's lack of understanding and vulnerability amidst the COVID-19 crisis.

As your broker, our top priority is ensuring that should the worst happen, your business or personal property is covered. We do all we can to help you to prevent any risks from occurring, but even with the best will in the world it's impossible to prepare for absolutely everything. With the right cover however, you can put thorough protection in place.

With cyber and data cover being such a new insurance product, we know that some of our customers may have questions. Please take a look at some FAQs below, and if you have any more specific queries, just pick up the phone and speak to us.

Why should I consider purchasing data insurance or a cyber policy?

All business sizes from local barbers to large accountancy firms have data that could be compromised, and if this happens it could prove very costly. Cyber incidents are on the rise and a breach of your data can be expensive to rectify. By choosing to buy cover, you can maximise the security of your business while also taking responsible measures in terms of your data liability. No organisation is immune from the potentially devastating financial impacts of a cyber loss.

What sort of issues could I expect from a cyber attack that I could claim for?

You could expect to claim in the event that the systems that you use have been shut down, or your network has been breached. You could also potentially claim as a result of lost data via hardware e.g. your laptop, server or the devices your teams use to work remotely. Malicious use of your business data could also be claimed for.

Generally, through a cyber policy you could be covered for:

- Legal and defence expenses
- Coverage for PCI DSS fines.
- Extra expenses protection
- Theft of monies or securities digitally
- Third-party coverage for a privacy breach or data event
- Breach notifications
- Breach mitigation
- GDPR costs incurred to the business
- Data restoration
- Business income
- Coverage for regulatory fines

What is Cyber Business Interruption?

This specific form of Business Interruption insurance means that if your business has to close or cease trading temporarily as a result of a cyber attack, you can claim for loss of income. This is usually excluded from traditional insurance policies so it is worth considering it even if you already have something like General Liability or Professional Indemnity.

What is the EU GDPR?

From 25th May 2018, the EU General Data Protection Regulations came into force on 25th May 2018. The new rules:

- Introduce a mandatory notification period following a data breach of 72 hours
- Greatly increase the potential penalties for non-compliance to 4 of global turnover of EUR 20 million, whichever is greater
- Clearly defines the rights of individuals over the personal data held on them by all organizations.

What is PII?

PII stands for Personal Identifiable Information. The volume that is stored on your IT network could influence the cost of your premium, as more records means a higher risk.

It can include:

- Name
- Gender
- Address
- Email address
- Telephone number
- Etc.

HAVE A MORE SPECIFIC QUESTION OR READY TO ENQUIRE ABOUT COVER?

GET IN TOUCH WITH US TODAY.

james & lindsay ltd