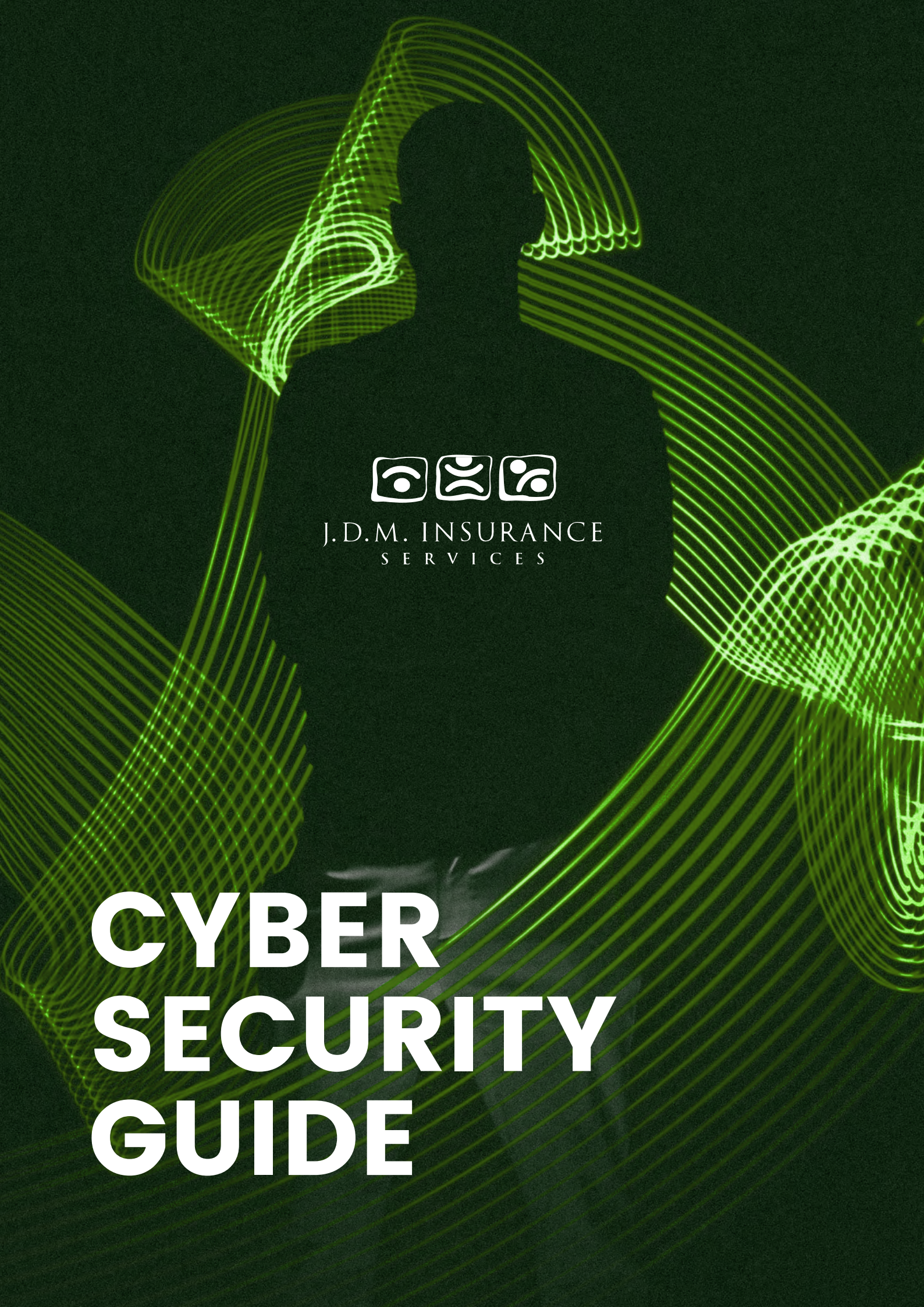


J.D.M. INSURANCE
SERVICES

CYBER SECURITY GUIDE

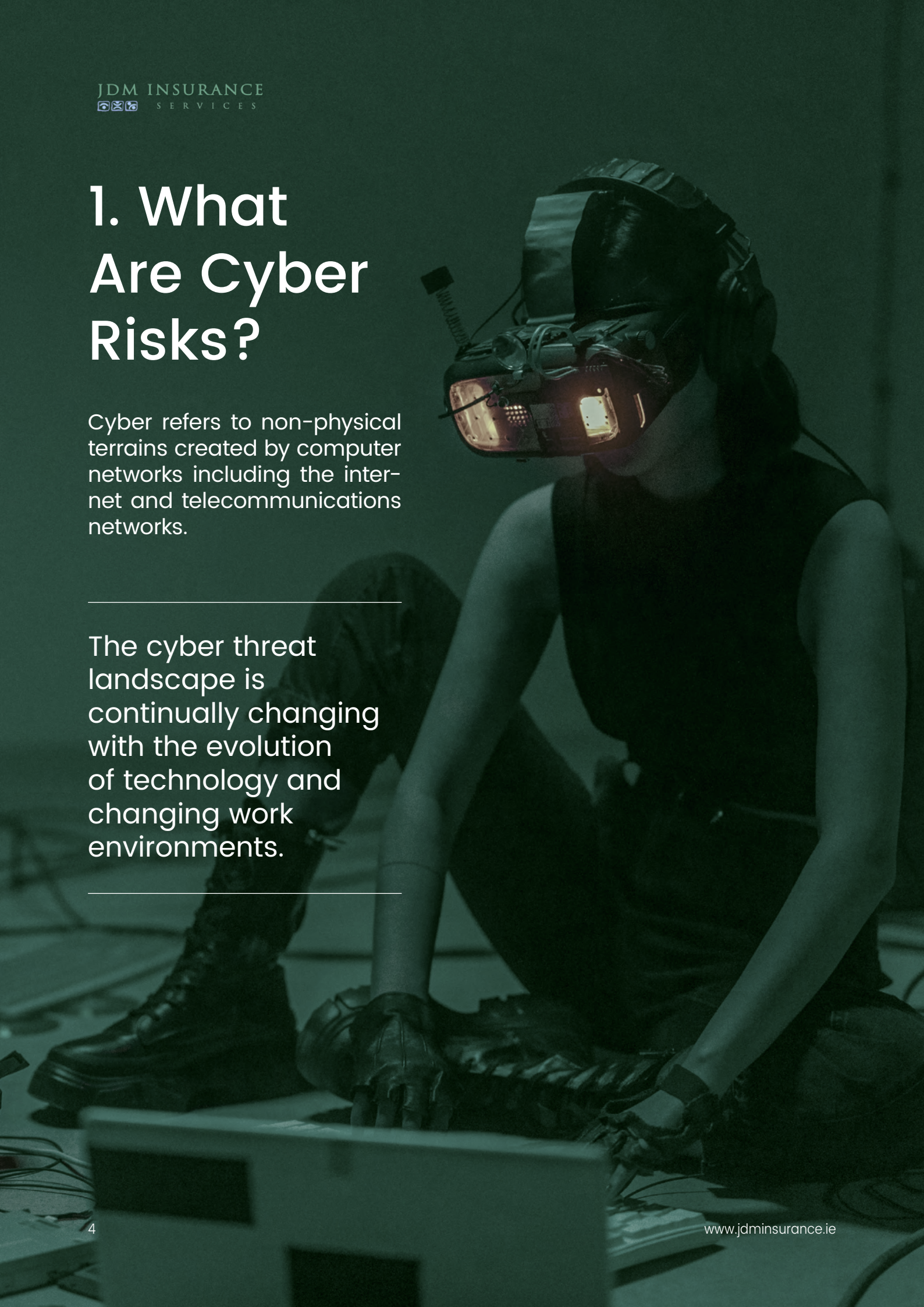
CYBER SECURITY GUIDE

CONTENTS

1. What Are Cyber Risks?

Cyber refers to non-physical terrains created by computer networks including the internet and telecommunications networks.

The cyber threat landscape is continually changing with the evolution of technology and changing work environments.



2. What Is Cyber Insurance And What Does It Typically Provide Cover For?

Cyber insurance can form part of a company's risk management procedures by acting as a risk transfer mechanism, allowing a business to operate with a greater peace of mind. Not only will you receive financial assistance after a cyber attack, but cyber insurers often provide access to a network of cyber risk experts who can help to minimise the associated disruption caused by the attack.

A cyber insurance policy can provide coverage for both first-party and third-party losses. First-party coverage aims to reduce the financial impact following a data breach or cyber attack, whilst third-party coverage is designed to protect from any claim made against a person or business for causing damage to another individual.

First-party coverage examples:

- Fraudulent input
- Hacking
- Social Engineering
- Business interruption
- Network and data restoration

Third-party coverage examples:

- Failing to secure data
- Unintentionally transmitting a virus
- Loss of reputation resulting from the content of an insureds website, emails, or data

Incident Response

What is the difference between a computer and cyber policy?

The main difference between the two is that a computer policy provides coverage for your physical equipment and data, whilst a cyber policy provides coverage for first- and third-party cyber losses.

A computer policy typically provides protection against loss and damage, theft, and breakdown to hardware (including static, portable, and even electronic office equipment) and its software. Cover can extend to include the cost of reconfiguring a computer system, reinstating data and increased costs incurred in minimising or preventing the interruption.

Some computer and cyber policies can extend cover to offer solutions to both types of risks.

3. Common misconceptions about cyber

Whilst cyber is one of the most talked about risks, it is also a topic that is often misunderstood. There are many common misconceptions, and the following are just a few examples.

Smart phones and tablet devices don't get viruses

All operating systems can be vulnerable to malware and viruses if a weakness is exploited. According to US.Norton.com[1], some operating systems benefit from a closed system where the source code is not released to app developers and restricts owners from modifying the code on their devices themselves. This creates difficulty for cyber attackers trying to find vulnerabilities on these devices but is not impossible.

Users have also been known to remove the restrictions to install non-standard features/ apps but at the expense of increased vulnerabilities.

Our business has already been attacked so it won't happen again

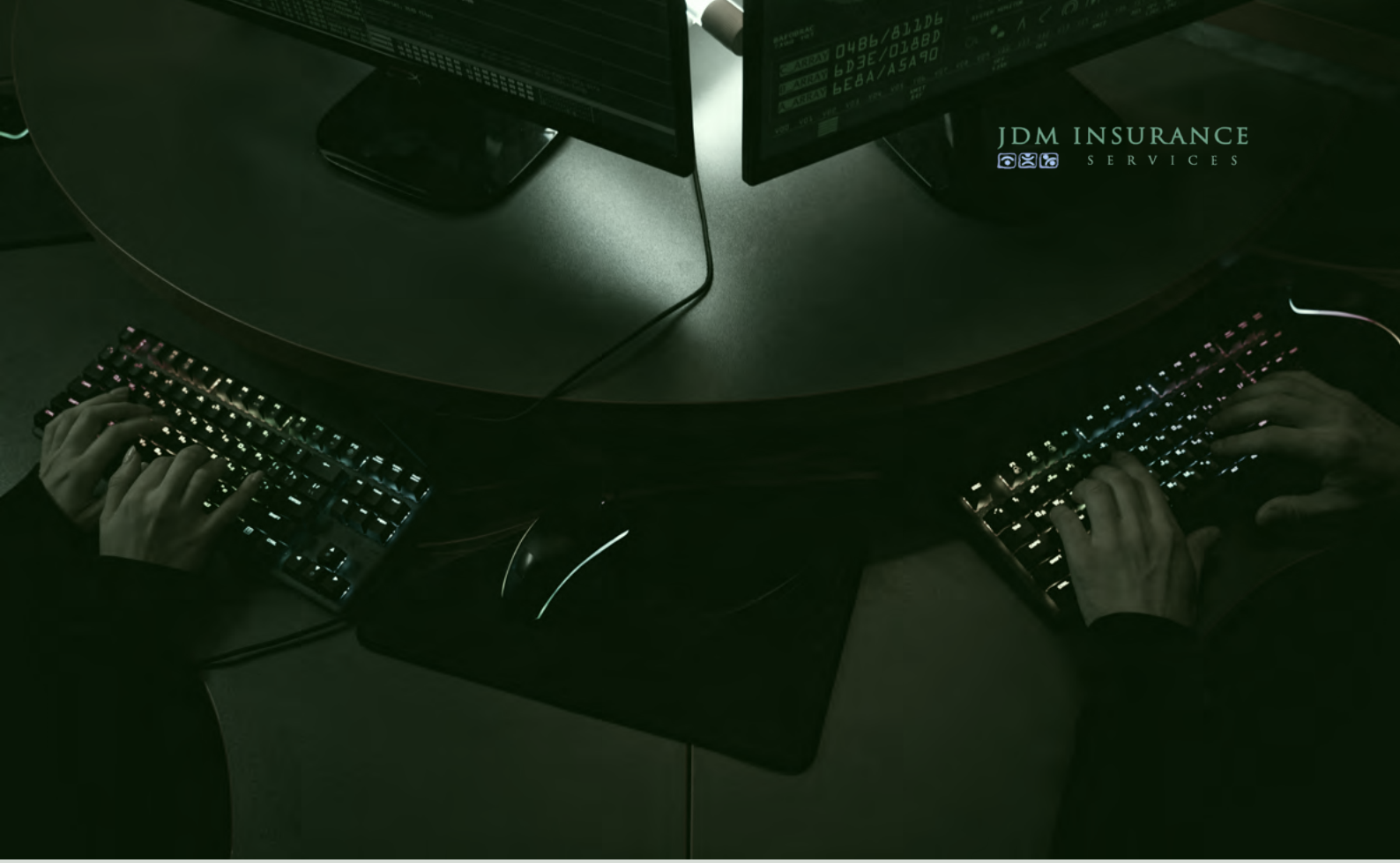
Lightning can strike twice and usually within close proximity! Cyber attackers are hoping to exploit organisations that have not patched the vulnerabilities, leaving a door open for them to breach the network for a second time.

Small businesses aren't attacked

Incorrect! Small businesses are attacked and regularly! Verison's 2021 Data Breach Investigation report[2] highlights that 28% of cyber attacks were found to have targeted small businesses. Cyber attackers can exploit vulnerabilities in cyber security to gain unauthorised access to data, often with ease. As small businesses tend to have less sophisticated cyber security, they are more likely to be targeted, compared with larger corporations who have developed to a high degree of complexity and have more stringent cyber security measures in place

[1] https://us.norton.com/internetsecurity-mobile-android-vs-ios-which-is-more-secure.html

[2] https://www.verizon.com/business/resources/reports/dbir/



4. Types of cyber attacks

The cyber threat landscape is continually changing with the evolution of technology and changing work environments. Covid-19 encouraged more remote working, creating more vulnerabilities in the IT infrastructure. The types of cyber attacks are rapidly changing but common attacks include the following (these are a few examples and not a definitive list).

Malware (including Ransomware)
Malware (short for malicious software) is a blanket term to capture all files and programs that are intentionally harmful to computers and networks, including viruses and ransomware. There are several reasons why cybercriminals use malware, which include[3]:

- Tricking a victim into providing personal data for identity theft
- Stealing consumer credit card data or other financial data
- Assuming control of multiple computers to launch denial-of-service attacks against other networks
- Infecting computers and using them to mine bitcoin or other cryptocurrencies

[3] https://www.mcafee.com/en-gb/antivirus/malware.html

Phishing / email compromise

Most of us are likely to have received a phishing email, but what is phishing? Public sources of information (typically social networks) are used to gather information on interests, activities and even employment history. This information may reveal an email address and leave individuals vulnerable to a phishing attack. Usually, the target receives a believable message that appears to be sent from a trusted source with the intent of either directing the person to a fake website or enabling malware to be installed on their system. Fake websites will mislead you into providing personal or sensitive information, potentially leading to a financial loss.

What are the key things to spot? Look at the email address, not just the sender. Sense check the email address with any emails received from the same company to see how the email compares. In particular, pay attention to the domain name as any misspelt name suggests it is likely to be a scam.

Cryptojacking

To understand cryptojacking we must first learn what cryptocurrency is. Cryptocurrency is a digital currency that is created by "mining". The mining process uses GPU or ASIC chips to solve complex mathematical equations. The first computer to find the solution receives the cryptocurrency as a reward and the process starts over. An example of a cryptocurrency would be Bitcoin.

At its peak, Bitcoin was worth over €55,000 in November 2021 and offers a clear incentive to mine. The more GPU or ASIC chips you have, the more likely you are to succeed at securing a Bitcoin. However, with more computers comes increased cost from both the initial investment and operating costs. Cyber criminals have found a way around this, they will hijack your computer system by gaining unauthorised access with the sole purpose of mining cryptocurrency. This is known as cryptojacking. Victims will usually need to click on a malicious link from an email that uploads malware containing cryptomining code. Alternatively, victims can access an infected website that contains JavaScript code that automatically loads in the browser. The first method is more intrusive with the cryptomining programme constantly running in the background whereas the latter only impacts the system whilst the victim is accessing the website.

DDOS

A distributed denial of service attack (DDOS) is a malicious and unauthorised attack. The intention is to overload the computer system, temporarily interrupting the services of its hosting server. Similar to cryptojacking, computers and other devices can become infected with malware and be controlled remotely. These devices are then referred to as "bots." A network of bots is referred to as a "botnet."

An attack consists of remote instructions sent to individual botnets to target a victim's IP address / server. The larger the botnet, the greater the force of the attack, increasing the chances of the network to become overwhelmed. Have you ever tried to purchase an item that has just been released and the website crashes because there is too much activity on the online retailer's server? A DDOS attack is using the same concept to disrupt the servers.

SQL injection

Structured Query Language (SQL) is the language used by and to communicate with databases. So, SQL injection introduces malicious code that is used to manipulate databases to display and access data that contains sensitive information. This type of attack must exploit a security vulnerability such as the Log4shell vulnerability.

IoT-based attacks

The Internet of Things is the growing network of connected objects that exchange data with other devices and systems over the network. Examples include thermostats, lights and even washing machines. The majority of IoT devices do not have the ability to install or update security software and therefore are becoming prime targets for cyber criminals, due to the relative ease with which access or control can be gained over the IoT device. This unauthorised access forms the basis of an IoT attack. A common event could see an attacker gain access to personal data by eaves dropping on not only audio streams but also live videos. IoT technology can enhance our lifestyles and convenience but can also make us vulnerable.

5. Five steps to protect against a cyber attack

Use up-to-date software

Updating software provides patches and fixes to potential software vulnerabilities that have been identified or previously exploited. Not only does updating software keep businesses safe from cybercriminals, but it can also offer increased efficiency and potentially reduce costs. Older and out of date systems generally have more issues causing more down time.

Use strong complex passwords

This may appear obvious but complex passwords help to prevent unauthorised access and help to keep data safe. A common approach for a hacker to break into a computer system is to guess passwords. The greater the complexity, the greater the difficulty of guessing the password.

Encrypt your data

Data encryption is a way of converting data from plain text to a series of randomised letters and numbers commonly known as ciphertext. Encryption will prevent cyber criminals from using or even understanding the data they find should they breach the network. 256-Bit AES Encryption is considered as a heavy-duty encryption process.

Use a combination of Antivirus, Firewalls and Endpoint Detection and Response (EDR) software

A combination of security software is more likely to be effective at combatting a cyber attack.

- A firewall monitors and filters incoming and outgoing network traffic and acts as a barrier between the internal network and the public internet. Firewalls can be both hardware and software.
- An antivirus software will protect a computer system by spotting malicious files and viruses. A firewall defends the systems from external attacks, whilst an antivirus software will safeguard against internal attacks.
- EDR software is considered to be the next level of protection. EDR not only includes antivirus but can also include firewall, monitoring tools and much more. The main difference for EDR is that it aims to detect all endpoint threats providing visibility on all devices within the digital perimeter. The benefit here is that the source of unauthorised activities on the network can be identified allowing the threat to be addressed more effectively.

Use Multi-Factor Authentication (MFA/2FA)

MFA is an authentication method that requires multiple factors of authentication. In order to understand how this works, we must first look into a factor of authentication. These are pieces of evidence that an individual uses to prove who they claim to be and can be split into three different types:

- Knowledge: what you know such as a password or memorable word
- Possession: what you have such as access to a phone
- Inherence: who you are, such as your fingerprint or facial recognition

A common example used is 2FA which would use two factors of authentication for a user to prove who they are. Usually, a password is entered each and every time an application is accessed. So, the 2FA would require an additional factor authentication such as a push authentication where an access code is sent to a mobile, which is then required before access is gained to the system. In the event that your password has been compromised, then an additional factor of authentication acts as a fail-safe

6. Why is cyber insurance important and how does it respond?

It is increasingly difficult to keep systems safe and even the best efforts are sometimes not enough. Cyber insurance reacts to the loss and helps to put the insured's business back in its original financial position prior to the loss.

Cyber insurance can pay for professional support to help businesses restore data and be up and running as soon as possible. The expertise offered by these professionals can help identify the vulnerability and provide guidance on how best to protect systems to prevent a similar incident in the future.

- Cyber insurance offers protection from cyber risks which could be damaging to a business and its reputation, such as data recovery following system damage or full-scale data breach.
- Cyber insurance can assist in helping businesses recover after a cyber attack by providing access to a network of cyber professionals.
- Cyber insurance can pay for professional support to help businesses who are the victim of cyber crime with the threat of damage to their computer system by virus, hacking or disclosing of data.

Unlike other risk management tools, cyber insurance does not prevent an attack, but it certainly helps in protecting businesses against a financial loss.

Data encryption is a way of converting data from plaintext to a series of randomised letters and numbers commonly known as ciphertext.

7. What information is typically required to obtain cyber insurance?

The information required can vary amongst insurers. However, in addition to the customer's general details and required sum insured, it is common for insurance companies to request the following:

Turnover

Turnover is demonstrative of the size of the customer's business. A higher turnover usually results in a greater frequency and increased amount of payments made to third parties, which can influence the exposure to cyber crime. On the other hand, higher turnover companies may have access to in house cyber specialists who can react to cyber attacks. It is often thought that larger companies are tougher to penetrate, with small to medium sized enterprises being an easier target.

Backup procedures

A data backup is a copy of the data taken from the company's computer systems. The copy is then stored away from the original computer network so it can be used to restore the computer systems in the event of a cyber attack or another data loss. The frequency and nature of the back-ups can influence the success of data recovery. Whether the data is backed up incrementally or in full, stored on a hardcopy or in the cloud can influence the underwriting decision.

Employee training

Insurers can often request details surrounding the training given to their employees. Specific topics would include internet and usage policies and payment procedures. Cyber criminals not only look work to exploit the IT vulnerabilities but also employees by gaining their trust and abusing their knowledge and IT access. Training will assist in increasing the awareness of cyber threats to employees and should reduce the chances of a cyber attack causing a financial loss.

Defence Software

Details of the software that is designed to defend the computer systems and networks is crucial to any underwriting decision. Defence software can come in many different forms and can even exist as hardware. A combination of several types of defence software/hardware will offer the best protection.

8. Cyber insurance in action

Fraudster Hacks Email

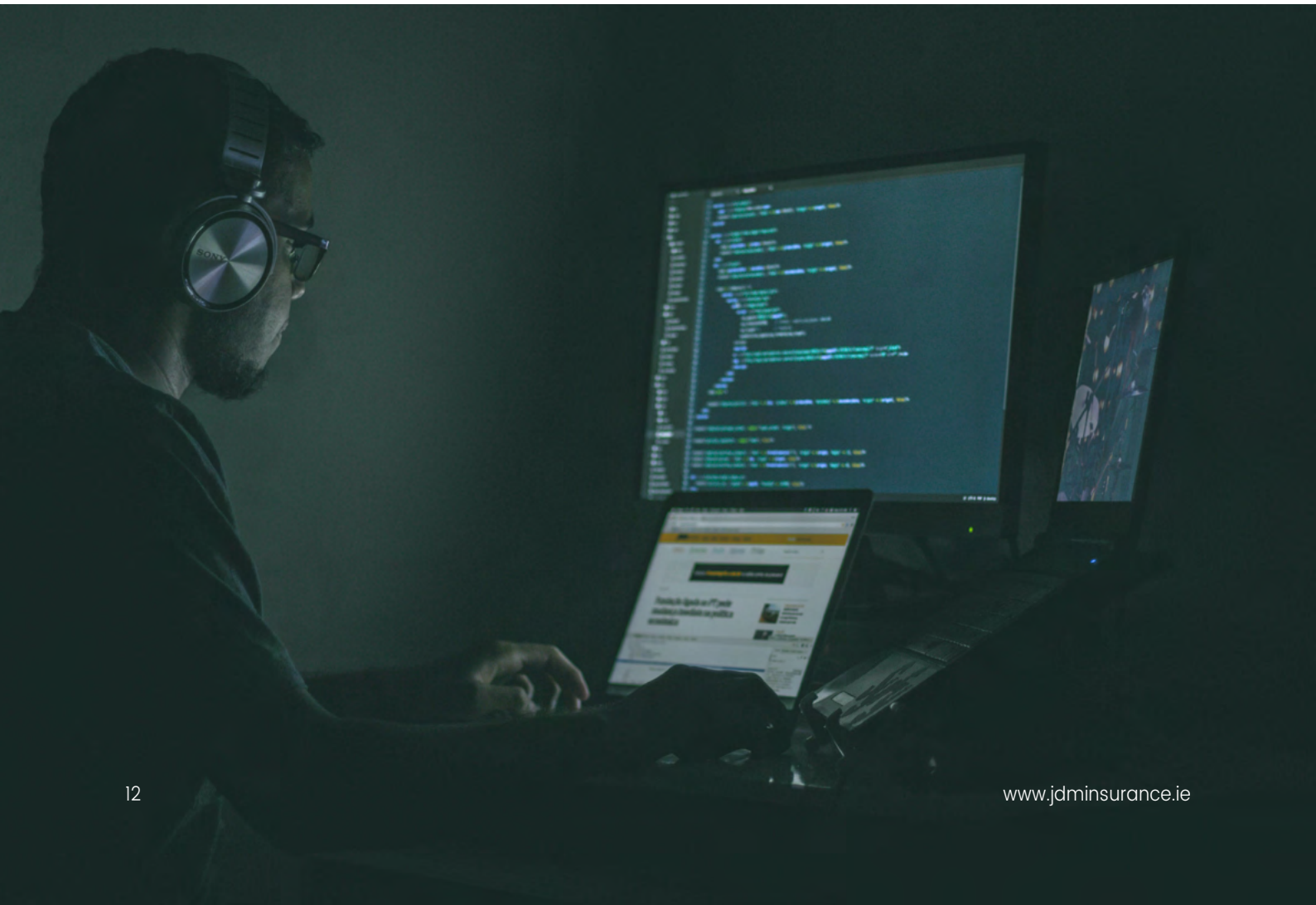
A haulage company was chasing late payment of an invoice. The customer advised that they'd received an email from the company with amended bank details and had already made three separate payments, over €120,000, to settle the account.

The company had cyber insurance in place. Investigators confirmed the breach was most likely from a phishing email and although the email account was not accessed for long, it couldn't be ruled out that no data had been copied. As a result, a security audit was undertaken, and the firewall replaced.

Hacker's code damages manufacturer's network

A food packaging manufacturer fell victim to a hacker, who gained access to their systems via a historic open remote port. Once in the network, the hacker elevated their network privileges to allow the execution of destructive code. The code encrypted several systems and resulted in permanent damage to key databases, and the erasure of a backup tape held within the network drive.

The damaged servers were rebuilt, and large volume disk drives were purchased to assist with the migration process. The cost of the IT support was covered under the insured's cyber policy.

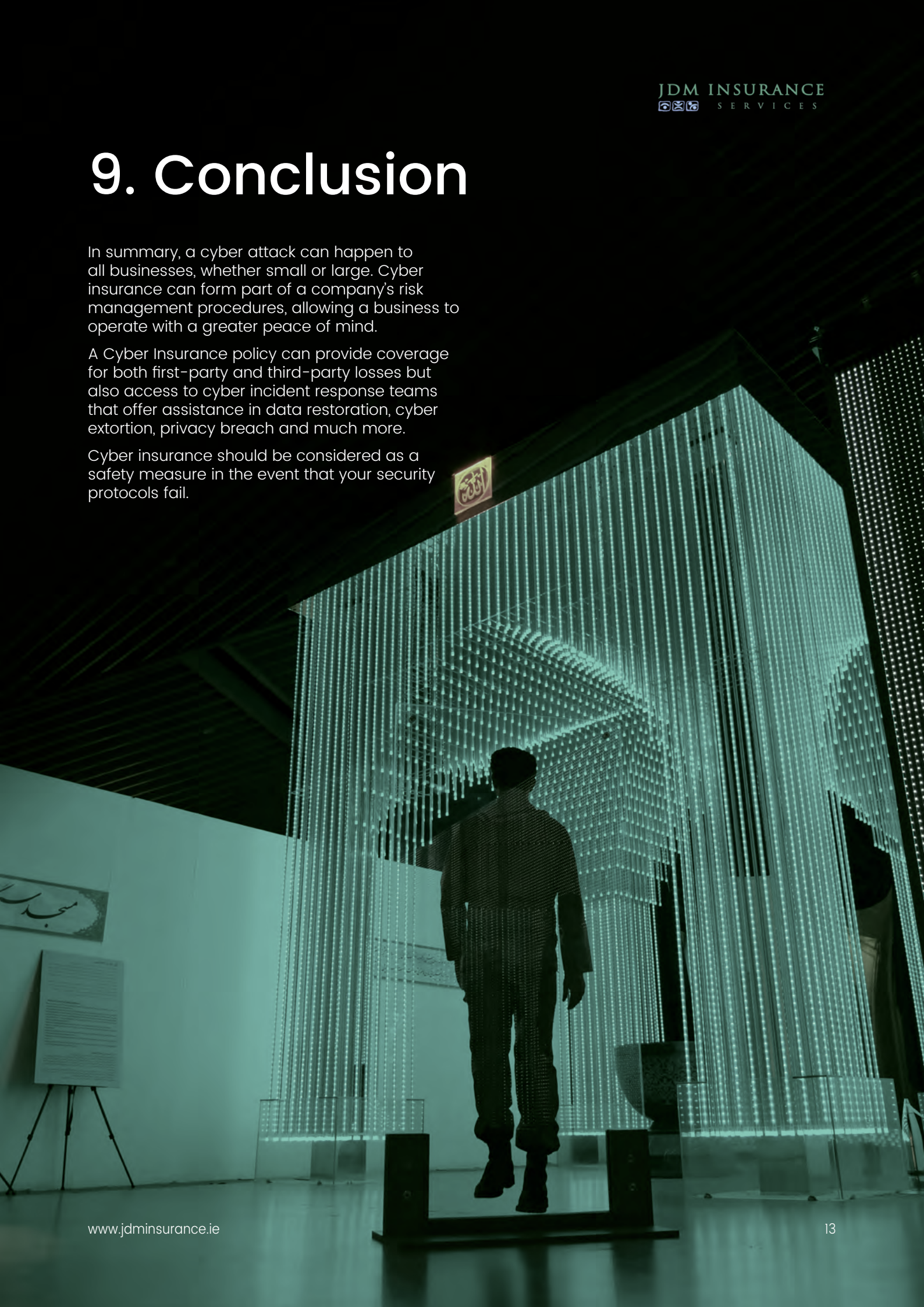


9. Conclusion

In summary, a cyber attack can happen to all businesses, whether small or large. Cyber insurance can form part of a company's risk management procedures, allowing a business to operate with a greater peace of mind.

A Cyber Insurance policy can provide coverage for both first-party and third-party losses but also access to cyber incident response teams that offer assistance in data restoration, cyber extortion, privacy breach and much more.

Cyber insurance should be considered as a safety measure in the event that your security protocols fail.



JDM Insurance Services
Melrose House, Dundrum Road, Dublin 14, D14 C1H5.
T: 01 2988266 | E: info@jdminsurance.ie

www.jdminsurance.ie

J.D.M. INSURANCE
SERVICES