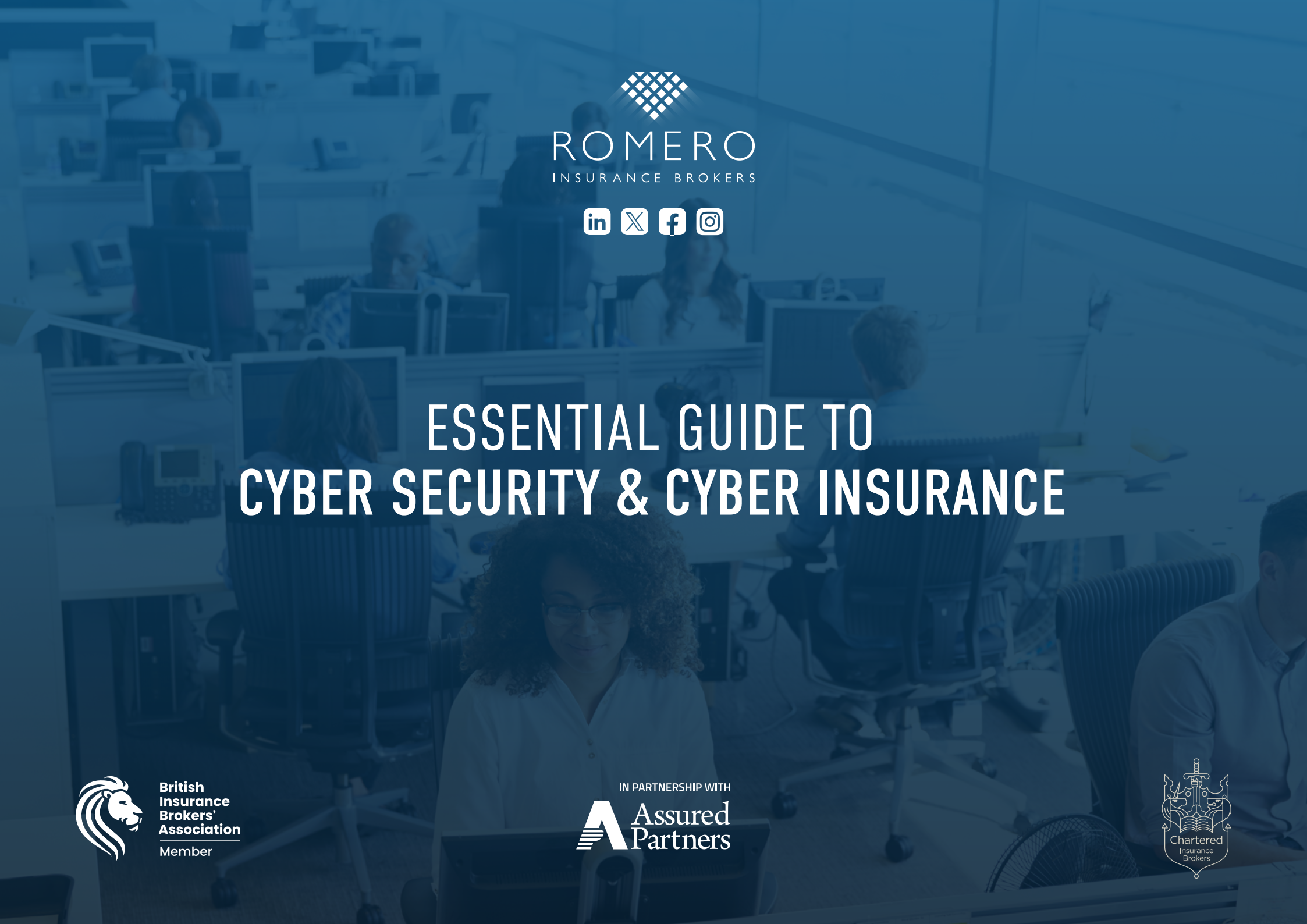
ROMERO
INSURANCE BROKERS

ESSENTIAL GUIDE TO CYBER SECURITY & CYBER INSURANCE



British Insurance Brokers' Association
Member

IN PARTNERSHIP WITH
Assured Partners

Chartered Insurance Brokers

CONTENTS

INTRODUCTION

Cyber security and cyber insurance are some of the most overlooked areas when safeguarding and protecting a business. This is because the area is relatively new, and constantly evolving. Cyber crime is a 21st-century threat and is, unfortunately, here to stay.

Cyber crime has continued to grow. The increase in attacks has centred around medium and large businesses and high-income charities. These businesses and organisation typically place less investment into cyber security. Consequently, the past year has seen the most dramatic material outcomes due to security breaches; this is without factoring in wider business disruption.

A cyber attack is, by far, the most common risk a business will face. Where the probability of a flood is one in maybe a hundred years, cyber attacks are experienced every week. Yet as businesses aim to cut costs amidst inflation and economic uncertainty, cyber insurance is not regularly being prioritised.

Overlooking a cyber insurance renewal is a huge misstep that could have severe consequences for businesses. As a dedicated broker, our mission is to protect the future of our clients and to communicate the emerging threats that are most likely to affect their finances.

Hence, at Romero Insurance Brokers, we have pulled together this whitepaper which lays out the dangers of cyber attacks. From the most common issues to emerging threats, we illustrate exactly what a business needs to do to best protect itself from cyber attacks and what actions to take in the event of a breach.

Our explanation has been peer-reviewed by The Romero Group's IT Director, Mark Noble, and Broking Director, Paul McAndrew. Cyber security expert and keen-eyed analyst, Mark has been within business security longer even than most of the terminology he uses. Long-time insurance expert, Paul McAndrew is a dedicated professional who has witnessed the implications of poor security for SME businesses and corporations. The following whitepaper they have co-authored walks readers through the more intricate cyber techniques that criminals are starting to employ, and how best to combat cyber crime.

THE RISE OF CYBER THREATS

The Cyber Security Breaches Survey report that, in 2024 alone, half of all businesses and a third of all charities experienced a cyber breach. Despite the extent of these nationwide attacks, only 31% of businesses and 26% of charities have undertaken cyber security risk assessments in the past year.

Indeed, compared with 2023, the deployment of cyber security measures have improved. Malware protection implementation is up, as is admin rights, firewalls and processes around phishing emails.

Yet still, balancing the importance of cyber security with core businesses activity is a challenge for many SMEs and corporations. There's still an 'it will never happen to me' mentality, when in reality small businesses receive the highest rate of targeted attacks.

Phishing and ransomware attacks are the most popular. 84% breaches are stemmed from phishing emails. Also, 51% of small businesses that fall victim to ransomware pay the money – mainly because 75% of SMBs could not continue operating if they were hit with ransomware.

WHAT DO CYBER CRIMINALS WANT?

Cyber criminals are individuals or groups who use technology as a means to steal something of value from your business. Sometimes cyber criminals may not commit theft; they may act to shut down your systems and machines, interrupt your business or perhaps open up your business to a separate attack. They can then extort you by holding your business to ransom.

The motives of cyber criminals are wide ranging and varied. Yet uniquely, often the offenders will often have no prior knowledge of your company before the targeted attack.

What could cyber criminals be after?

1. Money and transferable funds
2. Bank account details – of both clients and employees
3. Personal data – of customers and employees
4. Corporate data – of clients or affiliates
5. Sensitive information – documents or personal information
6. Product development information
7. Access to surveillance systems

Who do cyber criminals target?

43% of cyber attacks are targeting SMEs, and scarily, 60% of these SMEs go out of business six months later. This is because SMEs regularly do not invest in the security procedures needed to combat cyber criminals, and cannot survive the cost of an attack.

The average cost of a cyber attack is £10,830, with businesses taking an average of 38 days to identify and attack, and 43 to recover. 50% of all UK businesses have been made victim to cyber-crime in 2024, ultimately costing the UK economy £27 billion per year.

While corporations risk more costly data breaches and larger transferable funds, they are able to allocate more financial resources to invest in defence.

Cyber criminals are often unscrupulous with who they target, scouring the web for any holes or deficiencies potentially offering a breach. Attacks such as phishing scams are widespread do not discriminate the size of a business; yet because of the cybersecurity culture present at large business, it is more likely that SMEs get caught by phishing attempts.

Truly, it's impossible to know who is in the target of cyber criminals and why – but most attack attempts can be easily defended against.

THE DIFFERENCE BETWEEN CYBER CRIME AND CYBER ATTACK

The difference between cyber crime and an attack is the motive of the individual. Both involve the same methods of penetration - phishing, malware, theft – however the individual's motive can differ.

Cyber crime is motivated by money. Criminals target businesses to steal finances, financial information and hold them at ransom. Cyber criminals are out for themselves, utilising cyber breaches and weaknesses to gain.

Cyber attacks are motivated by the dismantling and destruction of a business. Through poor cyber awareness and processes, spyware and malware can infect our systems.

By shutting down services and causing business disruption, cyber attacks can severely impact business revenue and their future.

These two separate threats require different insurance policies. Only comprehensive cyber insurance can cater for these risks.

CYBER ATTACK

Install Malware – Requires System Repairs – Indirect Losses to the Company

CYBER CRIME

Criminal steals funds and data – Ransomed – Direct Losses for the Company

THE MOST COMMON CYBER THREATS

There are four main methods of penetration. Cyber insurance protects against all of the following threats. It is imperative businesses leaders understand every threat in order to put in place adequate measures to stay secure.

Phishing attacks

Fraudulent emails, text messages, social media messages, telephone calls, letters; phishing attempts are varied and comprehensive.

They pose a particular risk because they target the employees of a business, often pretending to be a boss with the aim of acquiring sensitive information. The employee can unknowingly pass on bank details, passwords, or product information, placing the business in great risk.

Malicious links can be transferred to your employees any number of ways. The best way of protecting against the risk of phishing is through education and building employee awareness. Ultimately, staff need to be vigilant when clicking links, even those provided by a trusted source.

Malware

Malware is software designed to interrupt your business processes and potentially steal information. Also known as viruses, both Windows and Mac operating systems are prevalent to malware, infecting via unsecure links on the internet or through Word and PDF documents.

Methods of malware implementation increased sharply in 2023, with smartphone malware now comprising 16% of all malware attacks. Signs your phone is infected are a rapidly draining battery, increased data usage or increased popups and spam messages.

Awareness is key to detecting a scam or malware risk. The cost of cyber attacks is far likely to be higher than the cost of increasing cybersecurity, and education is large part of cyber risk management.

Staff negligence

The most likely reason a business's systems will be compromised is due to employees making a mistake. An employee could be victim to a phishing email, lose their work phone or laptop, or send sensitive information. The ramifications for a business with negligent staff can be devastating; have them hand over logins and

information is the most direct and immediate way criminals access a business's systems. Education is the key to prevention. Mandatory cyber security courses and training should be provided, and vulnerable individuals should be identified. A cyber awareness strategy involving every member of the workforce, as well as lockdown procedures incase of a breach, are necessary.

Rogue individuals

The physical presence of individuals with unscrupulous intentions can pose a cyber threat. These rogue individuals could be external, or even work internally. Their motives vary; stolen sensitive information can be used to extort employees; duplicated data can be sold to competitors; unauthorised access can lead to a total shutdown of business operations.

A cybersecure culture and reminding employees to keep an eye out is essential. It only takes one person with an external usb to compromise precious company data.

EMERGING CYBER THREATS

Cyber crime is evolving, and as we progress through the second quarter of this century, businesses need to be more alert than ever to emerging threats.

Artificial Intelligence – Criminals have started to use AI to create sophisticated social engineering scams. Employees need to be aware of deepfakes and recent examples of identify fraud attempts.

Ransomware – An attack with the intention of locking operators out of their systems in order to extort a fee; experts predict this type of attack will rise and continue to disrupt businesses.

Increased cyber usage – There will be an increased access to cyber tools, meaning a higher risk of staff negligence, more vulnerable users online, and an increase in low-sophistication threats from novice cyber attackers.

Increased information-stealing malware – Known as 'infostealer malware', these programs will continue to be a major threat. Data breaches will only increase in number and the time it takes for a business to be comprised will shorten.

WHAT BUSINESSES CAN DO TO PREVENT A CYBER ATTACK

Businesses need to be proactive in their fight against cyber attacks. A range of processes and techniques can be implemented to deter cyber criminals and keep your employees alert.

Implementing effective preventative processes will have a beneficial effect on a business's insurance. Underwriters will factor these controls into their decision-making. These processes help businesses monitor control issues and work to minimise risk. Businesses need to know what measures they can feasibly implement and where they can improve.

Multi-factor Authentication

Multifactor authentication, also known as MFA, is an authentication method that requires the user to provide two or more verification factors to gain access. Employees use their phone or extra passcode to access the business's operating systems securely.

Secure backups

Backups ensure your website can be reverted back to an earlier state – therefore fixing any changes made by unauthorised infiltrators. Ransomware attackers will look to delete backups, neutralising this action, which is why a business's backups need to be secure.

Encrypt your backups and also isolate them from the network so they cannot be accessed online. Regularly test your backups to ensure they can be used in the event of a crisis.

Penetration testing

Penetration testing assesses the security of your business, looking for holes or weaknesses which could lead to a breach. Annual testing improves the likelihood of insecurities being found and fixed before an attacker can infiltrate.

Penetration testing should be done annually, and added to your risk management plan.

Filter emails

Don't give employees an opportunity to fail, and start filtering emails. Keep spam out of inboxes to improve both productivity the business's cyber security. Filtering emails is the first line of defence against the most common threat, so business's should ensure they have a comprehensive system in place.

Update systems

Updates are essential. Updates are often required to patch holes which have been found by the developer. Hackers often target old loopholes and gaps, so these need to be patched.

Mandatory updates should be done as quickly as possible, and added to your risk management plan.

Incident response plans

Incident response plans are essential to reducing the business disruption faced after a cyber attack. They contain how to organise a full lockdown of your systems and a plan of how to conduct a recovery in the event of an attack.

As a dedicated broker, we will assist with the formation of an effective incident response plan. Plans should be tested and reviewed and regularly updated whenever a business system or procedure is altered.

Protect network

Firewalls are barriers that sit between a private network and the public internet. Penetration testing will ensure your firewalls are up and secure, and regular updates will ensure your firewall and network is protected.

Anti-virus software will protect your network from possible data-leaks. Having anti-virus solutions installed and on-hand is mandatory.

Monitor the network

A business's network should also be monitored constantly to ensure it is secure. Your IP address can be hidden through the use of a VPN. Tracking your bandwidth usage will help to uncover network issues and to discover if more than the intended number of devices are utilising your network. More devices or rogue devices will increase your company's risk of a breach.

Educate the workforce

And most importantly, the number one-way firms are being put at risk is through a poorly-educated and negligent workforce. No amount of technology can cater for an employee who falls for every trick in the book. Effective education is paramount for security as there will always be attackers that are out to deceive people. Combat phishing by ensuring your people remain vigilant.

WHAT BUSINESSES SHOULD DO WHEN A CYBER BREACH HAPPENS

Procedures business operators need to take in the event of a breach should be included within an Incident Response Plan. The aim of an incident response plan (or business continuity plan) should be to stop the incident getting worse. This plan needs to layout the road to recovery, and include how to properly report the incident.

As a dedicated broker, we've created a six point plan which is detailed here. These actions reference a business's responsibilities, and can be tailored to work effectively.

1

Assess the extent of the attack

You must do all you can to stop the incident from getting worse. Your team may be able to minimise damages by shutting down the system and changing logins if necessary.

2

Report the Attack

You should report a significant attack to the National Cyber Security Centre (NCSC) as well as the FCA. Depending on the breach, you may be required to report the incident to the Information Commissioner's Office and the Office of Financial Sanctions Implementation (OFSI).

3

Contact your broker

Early contact gives you the best chance to recoup any losses you may sustain.

4

Consult the Experts

Businesses should have Insurer cyber incident response companies (CIR) on standby. All cyber security incidents involving data should be reported to Action Fraud, they will then refer you to law enforcement experts. The NCSC will also refer technical authorities to assist.

5

Draft a brief for staff and clients

Staff, customers, clients and stakeholders all have a right to know of a breach, especially if it is their personal data that may have been compromised.

6

Resolve the Issue

Utilise your backup data, change all passwords and eradicate any holes used to breach - ensure your defences are safer and stronger than ever.

THESE PROCEDURES ARE NECESSARY ***FOR ALL SIZES OF BUSINESSES***

Cyber attacks don't just happen to big businesses. All businesses need an Incident Response Plan because all businesses record data, be it employee or customer data, and are therefore responsible for its privacy and security.

The costs and manpower required to recover from a breach are significant. Therefore, ensure you always have your Incident Response Plan and cyber insurance policy reviewed by a reliable broker.

If you don't have an Incident Response Plan, making one should be a top priority. It should detail first steps, how to safely recover affected systems, as well as the necessary checks and precautions. This should include patching, hardening and testing systems, and also how to make sure it doesn't happen again. Without annual desktop run-throughs and simulation trainings, your staff could panic in the face of a data breach.

CYBER INSURANCE

Having the right insurance means that, in the event of a cyber attack, you are protected. Cyber liability insurance will provide the support a business needs, taking the brunt of the financial hit that cyber criminals will deliver.

Many standard business insurance policies will include mentions of cyber crime but as a package add-on, or as a subset of a different policy. Cover is often miniscule and insufficient, leaving you and your business underinsured considering the potential scale of the cyber attack.

Standard insurance policies which mention cyber losses will most likely not be able to cover the full extent of major cyber attack. If your network is unavailable, if you're business can't take payments or bookings, if data is lost or stolen and needs to be recovered – these are costly scenarios; each can do irreparable damage to your business's reputation.

Comprehensive cyber cover is essential for businesses; it is necessary to protect against a wide range of vulnerabilities and circumstances. Cyber insurance arranged through a dedicated broker, not only provides the financial help in the event of a cyber attack, but also the resources needed to unravel the damage that's been caused, and help the business get back on track.

What will cyber insurance cover?

Cyber insurance is there to cover the financial costs of losses due to cyber attacks.

Paying for services to investigate the cyber crime will be covered as part of a comprehensive cyber insurance policy, alongside the cost of restoring the computer system and recovering lost data. The cyber crime may involve extortion and ransomware, in which case the payment and financial loss will be covered. Any legal expenses will be covered, as well as direct monetary losses following a breach.

Businesses will require key reputation management when an attack occurs, the scale of which can be underappreciated; the expenses of public relations can be significant.

Disruption to business practices caused by cyber losses will also be covered by your business interruption policy. Third party services are also covered, including damages incurred, settlements made and legal defence costs.

Some business will require higher levels of cyber insurance coverage depending on their size, scale and vulnerability – therefore the best solution is a tailored policy. Cyber insurance should be tailored to the business in order to ensure their specific needs are met and that the coverage limits are suitable. To understand the needs of your business and the apparent gaps, a cyber audit is required.

Cyber audits are ideal at understanding the level of cover required and in identifying next steps. Contact a decorated and dedicated insurance broker to arranging a cyber audit.

CYBER INSURANCE FROM **ROMERO INSURANCE BROKERS**

As an industry-leading dedicated insurance broker, Romero Insurance promises to deliver effective and comprehensive insurance policies for clients. Romero Insurance Brokers pledge to deliver the full package, with first-rate client services and an award-winning claims team.

Romero insurance Brokers is best placed to deliver tailored cyber insurance policies. We audit each of our clients to ensure they receive the best possible cover. We make our insurance policies transparent and understandable so businesses know exactly where they stand, while also keeping you updated on the latest industry news.

In our experience, many businesses do not fully recognise the potential impact of a cyber attack, or if they do, they have rarely invested the resources adequately. Our experts take the time to understand your business and what can be done to improve your protection.

We firmly believe no two businesses are the same, and so we tailor our cyber insurance to your needs - no matter what sector you work in, our team have the experience and knowledge to keep you safe.

At Romero Insurance Brokers, we have a large dedicated claims team able to deal with any data breach cases. Our mantra is to treat customers exceptionally, and for handling cyber issues there is no better broker.

Contact us for a free, noncommittal, confidential review today.

IF YOU WOULD LIKE TO DISCUSS YOUR CYBER INSURANCE,
PLEASE GET IN TOUCH WITH OUR AWARD-WINNING TEAM

0113 281 8110
romeroinsurance.co.uk

ROMERO
INSURANCE BROKERS