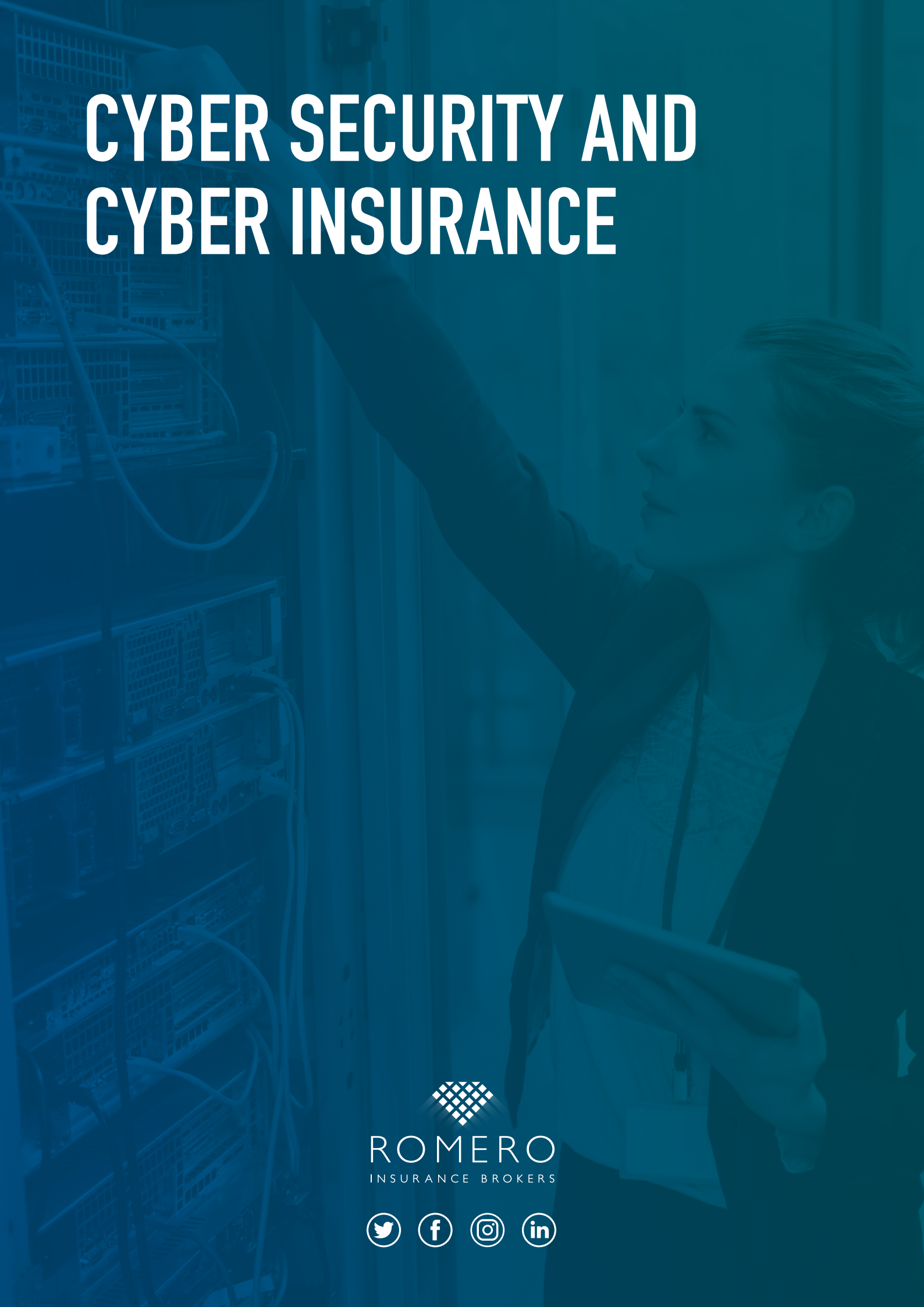
CYBER SECURITY AND CYBER INSURANCE



ROMERO
INSURANCE BROKERS

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.

And while the COVID pandemic has forced stagnation in many sectors, cyber crime has continued to grow. The increase in attacks has centred around medium and large businesses and high-income charities. This could be due to businesses finding it harder than ever to administer cyber security measures during the pandemic. Consequently, the past year has seen the most dramatic material outcomes due to security breaches; this is without factoring in the 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, surveyed companies report that cyber attacks are experienced every week. Yet as businesses aim to cut costs after the COVID-19 fallout, 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 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. Cyber security expert and keen-eyed analyst, Mark has been within business security longer even than most cyber security terminology. He walks us through the more intricate cyber techniques that criminals are starting to employ.

CONTENTS

MARK NOBLE

IT Director

Mark oversees the day-to-day running of the large IT department at the Romero Group. A well-versed IT professional, Mark has a wide knowledge of modern practices and business strategies. He has 30 years' experience implementing technology to benefit businesses, be it maximising serviceability, automating invoicing or employing cyber security.

As the technology sector has evolved, so too has Mark. Now heading up a top independent insurance broker, Mark regularly combats increasingly sophisticated cyber threats. He understands what holes often need patching and where businesses should best lend their attention to maximise protection.

THE RISE OF **CYBER THREATS**

Businesses are facing new and ever evolving risks at a rate faster than ever before. It's easy to dismiss serious cyber threats as something that only happens to major corporations. That's not the case.

DATA BREACH INVESTIGATION REPORT FROM VERIZON REPORTS THAT ALMOST A THIRD (28 PER CENT) OF DATA BREACHES INVOLVE SMALL BUSINESSES. 1.6 MILLION OF THE 5.7 MILLION SMBS IN THE UK PER YEAR SEE A HACKING ATTEMPT.

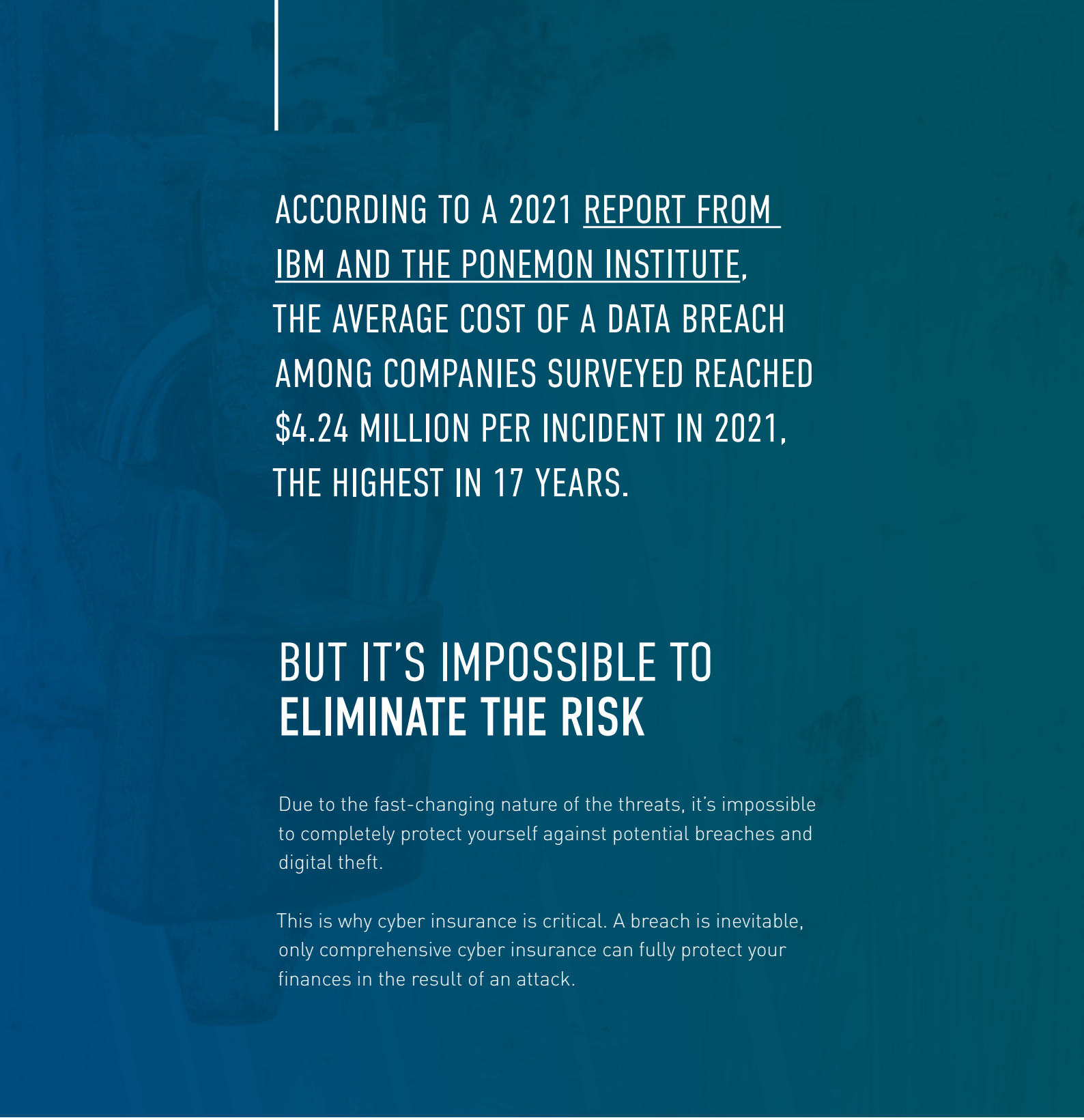
FORTUNATELY, MOST BUSINESS OPERATORS ARE BECOMING MORE AWARE OF THE DIFFERENT TYPES OF CYBER ATTACKS, AS WELL AS THE VARIOUS METHODS AND SYSTEMS REQUIRED TO PROTECT AGAINST THEM. HOWEVER, THE COVID-19 PANDEMIC HAS CREATED SERIOUS VULNERABILITIES IN MANY WORKFORCES AS THEY ADOPT WORKING FROM HOME.

ALMOST THREE QUARTERS (73 PER CENT) OF SMALL BUSINESSES LACK THE CAPABILITY AND EXPERTISE TO WITHSTAND A CYBERSECURITY ATTACK.

BALANCING THE IMPORTANCE OF CYBER SECURITY WITH CORE BUSINESS ACTIVITY IS CHALLENGING FOR MANY FIRMS.

ACCORDING TO ARCTIC WOLF'S STUDY, 55 PER CENT OF BUSINESS OWNERS SAID THEY REGULARLY DEPRIORITISE CYBER ISSUES IN FAVOUR OF OTHER BUSINESS ACTIVITIES.

YET, EFFECTIVE CYBER SECURITY CAN SAVE YOUR COMPANY MILLIONS; SMALL HABITS CAN KEEP YOU, YOUR BUSINESS AND YOUR STAFF SAFE.



ACCORDING TO A 2021 REPORT FROM IBM AND THE PONEMON INSTITUTE, THE AVERAGE COST OF A DATA BREACH AMONG COMPANIES SURVEYED REACHED $4.24 MILLION PER INCIDENT IN 2021, THE HIGHEST IN 17 YEARS.

BUT IT'S IMPOSSIBLE TO **ELIMINATE THE RISK**

Due to the fast-changing nature of the threats, it's impossible to completely protect yourself against potential breaches and digital theft.

This is why cyber insurance is critical. A breach is inevitable, only comprehensive cyber insurance can fully protect your finances in the result of an attack.

MARK SAYS

The role of the IT department has changed and evolved so much over the past few years. There is more of a focus on the monitoring and security aspects, making sure the users can work quickly but also safely. And yet, no business can be 100% secure from a cyber attack.

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, and unlike other crimes, the offenders will often have no prior knowledge of your company before the targeted attack.

What could cyber criminals be after?

Cyber criminals could be after any number of a range of things, including:

1. Money and transferable funds
2. Bank accounts details
3. Influence – blackmail and holding to ransom
4. Personal data – of clients or customers
5. Corporate data – of businesses and employers
6. Sensitive information – government documents, criminal records or harmful personal information
7. Product research and product development information
8. System access
9. Planting surveillance programs

Who do cyber criminals target?

While larger companies do generally yield more valuable results, SMEs will also hold much of the valuable assets listed above. The data that these small businesses process is often extremely valuable, both to the company and to the client; cyber criminals will target this.

Potential perpetrators will produce programs which scour the web for businesses that are not properly protected. Larger companies are able to allocate more financial resources to invest in defence, but SMEs are perhaps less well equipped and perhaps less aware. Cyber criminals know this; cyber attacks on SMEs have grown by 14% with 62% of SMEs reporting an incident. 22% of SMEs fell victim to 1 or more cyberattacks in the last two years, a figure which does not including those companies which have perhaps been breached unawares.

Truly, it is difficult to know the full extent of how many businesses are being scouted by cyber criminals and rogue programmes. But some methods of penetration are more common than others and can be easily combatted.

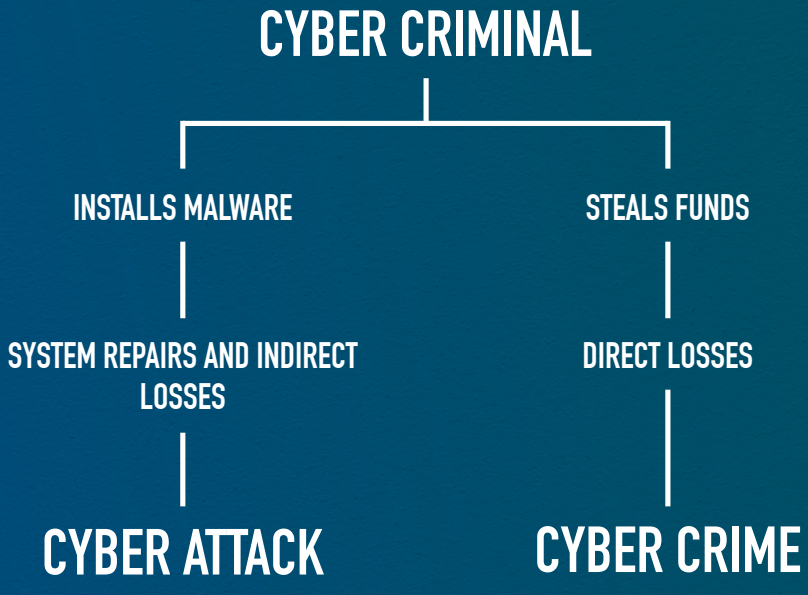
IS THERE A DIFFERENCE BETWEEN CYBER CRIME AND CYBER ATTACKS?

The key difference between cyber crime and cyber attacks lies in objective of the attack. To distinguish between the two, we must ask: What does the individual want?

Both originated in a similar way, using the same methods to penetrate a company. Through malware, phishing emails or property theft, individuals are able to affect a business, however the motive changes the way we determine the attack and therefore how we act to protect against it. Cyber crime is primarily motivated by money. Cyber criminals will target your business in order to steal your financial details or to hold you at ransom for financial gain.

Cyber attacks are motivated by the destruction and dismantling of a business's infrastructure. This creates economic damages by interrupting business practices, shutting down systems and forcing repairs, therefore causing indirect financial losses.

Once having breached your system, cyber criminals can act to steal your data, your monetary funds, or act to bring down your system and install spyware. These two distinct threats bring separate risks and hence require different policies. Businesses need to cater for this by having a fully comprehensive cyber insurance portfolio.



THE MOST COMMON CYBER THREATS AFFECTING BUSINESSES

There are four common methods of penetration, each provides a threat and can be prevented through effective cyber security techniques. In order to know how to protect yourself, you first need to know where you could be exposed:

Phishing attacks

These attacks come in many forms. They can be fraudulent emails intended on fooling business operators - emails could be under the guise of an employee, senior member of staff, or affiliate company asking to share passwords, banking information or product blueprints. They could be telephone callers purporting to be from the bank the police or a fraud agency attempting to make employees reveal valuable information. More recently attackers are operating through links, often spread through text, trying to get employees to enter fake copycat sites that ask for sensitive information. A little education and employee awareness can go a long way towards preventing a breach.

Mark says, *"On top of the list of most common threats is emails. It's the easiest way to disrupt a business. Staff need to be vigilant when clicking links, even those provided by a trusted source."*

Malware

This is software designed to infiltrate computers and extract data. Spyware, ransomware and viruses are all easily capable of bringing your business operations to an abrupt halt.

Staff Negligence

This involves employees making a mistake or being tricked into offering information to criminals. An employee could send data to the wrong place or source, they could lose hardware such as a mobile phone or laptop, or they could become victim to a phishing email. These issues could have devastating ramifications for businesses, yet are the most direct and common ways criminals get a hold of unintended information. Simple training and procedures should prevent this threat.

Mark notes, *"Without doubt the greatest threat to a business is from employees. Asking questions before sending data is crucial. With regular training exercises, workforces can start to see how much of a serious threat negligence is to any business."*

Rogue individuals

Internally or externally, rogue individuals can cause severe harm at great expense. Be it hackers or employees, rogue individuals are out to steal your data. Their motives may 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. The options are endless.

NEW CYBER THREATS AND **RECENT CHANGES**

There are key risks that we have noticed are disproportionately affecting clients and having severe consequences. We want to make you aware of these risks so you can take special measures to negotiate your way around them.

Key risk: Data Theft

Information is power, and stealing data is an attack indicative of a cyber criminal.

99% of all UK businesses with 10 or more employees handle and keep forms of digitised data, data that can be valuable to those who would choose to abuse it. The 2020 GDPR Data Protection Act strengthened the rights of individuals about how their personal data can be used, and the loss or extortion of this data can force a huge lawsuit.

Businesses are collecting more data than ever before due to the technical tools they have available. They also have a responsibility to inform clients and customers if the data has been stolen or leaked, leading to complications, masses of paperwork, and financially disastrous fines. Safeguarding data should be heavily prioritised.

Criminals will attempt any one of a number of techniques to gather data; the most common listed previously; however most can be easily combatted.

Key risk: Stopping Machines Working

Be it office computers or factory equipment, stopping your machines from working is an effective attack and causes major business disruption. Equipment that is running on old software is most at risk of hijackers. Update your office computer regularly to ensure it cannot be easily infiltrated; penetrative testing will be key. Also, businesses should research whether their other machinery is vulnerable to attack and perhaps might need to be replaced with more up to date secure models. Wi-Fi printers, PCs, tablets and phones can quickly become outdated.

Mark says, *"If you are a large manufacturing company, your machinery has computers, has software. So, in the event of a cyber attack, there is potential for your whole company to be ground to a complete halt."*

Key risk: Property Exclusion

Commercial property cover includes very little on the side of cyber-related losses; this cover is nowhere near as sufficient or detailed as is needed. Most property policies include some reference to electronics, however it is typically limited to physical components. And as businesses are becoming increasingly dependent on technology, this exclusion for certain cyber threats is a huge risk.

Necessary is a standalone cyber insurance policy that is more suited to cover incidents such as data breaches and cybercrime. As to not leave any holes in their cover, businesses should have a comprehensive review of both their property and cyber policies. This can ensure gaps are filled and the two policies work well together - contact Romero Insurance Broker for a comprehensive review.

WHAT CAN BUSINESSES DO TO **PREVENT A CYBER ATTACK**

There is a list of actions businesses should consider when working to protect against cyber attacks and deter cyber criminals. These processes and techniques will all but assure security, with most only requiring minor adjustments to be implemented.

Another important reason why businesses should employ these preventative processes is because insurers and underwriters will factor these controls into their decision-making. These processes help businesses monitor control issues and work to minimise risk.

As a broker, our mission is to help businesses minimise risks and provide information on what insurers are focussing on. Hence, we have laid out these processes below with some explanation as to how they can be effectively implemented.

Multi-factor Authentication

Control access to your systems more acutely with multifactor authentication, also known as MFA. This is an authentication method that requires the user to provide two or more verification factors to gain access. This means a stolen phone or laptop hard drive won't be enough for criminals to access your systems. It secures the environment without requiring resets or complex policies.

Secured and Tested Backups

A tactic for attackers is to try to eliminate any opportunities for resets by deleting backups. This will then make ransomware extremely capable of bringing down your business operations. Therefore businesses need to keep up to date backups, and keep them 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.

Find vulnerabilities with penetration testing

Annual penetrate testing helps to find the vulnerabilities in your software. Make sure you find them before somebody else does.

Regular scans help you understand how a cyber criminal would gain access to your systems if they planned a targeted attack. Creating practices and procedures to ensure this is done regularly should be added to your risk management plan.

Filter emails

The primary and most common way hackers infect your systems is by sending links and data requests through emails. Don't give your employees any opportunity to fall victim to these scams by filtering emails. This is the first line of defence and should easily test and block most malicious content.

Update systems

Regular updates are annoying but necessary. Keeping your systems updated will stop hackers exploiting old loopholes and gaps which have since been patched. Make sure you add this to your risk management plan as a regular practice to maintain. Mandatory updates from developers should also be conducted as it often means a patched hole or system weakness being resolved.

Limit number of admin accounts

The most important accounts, admin accounts and super admin accounts, should be limited in order to protect access. Fewer admin accounts means a lower risk of becoming victim to rogue employees or infiltration.

Incident response plans

Having an incident response plan in place is something we, as your broker, will mandate and help to organise. They are necessary to improve your quality of response to cyber incidents. It will also help to limit your overall cost of cyber security. Incident response plans should be tested, at least annually, and reviewed by your broker.

Protect Network

All businesses should be utilising firewalls. A firewall is a barrier that sits between a private internal network and the public Internet. Ensuring firewalls are up to date and healthy through the use of penetrative testing is imperative to maintaining a secure network.

Monitor Network

Your 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.

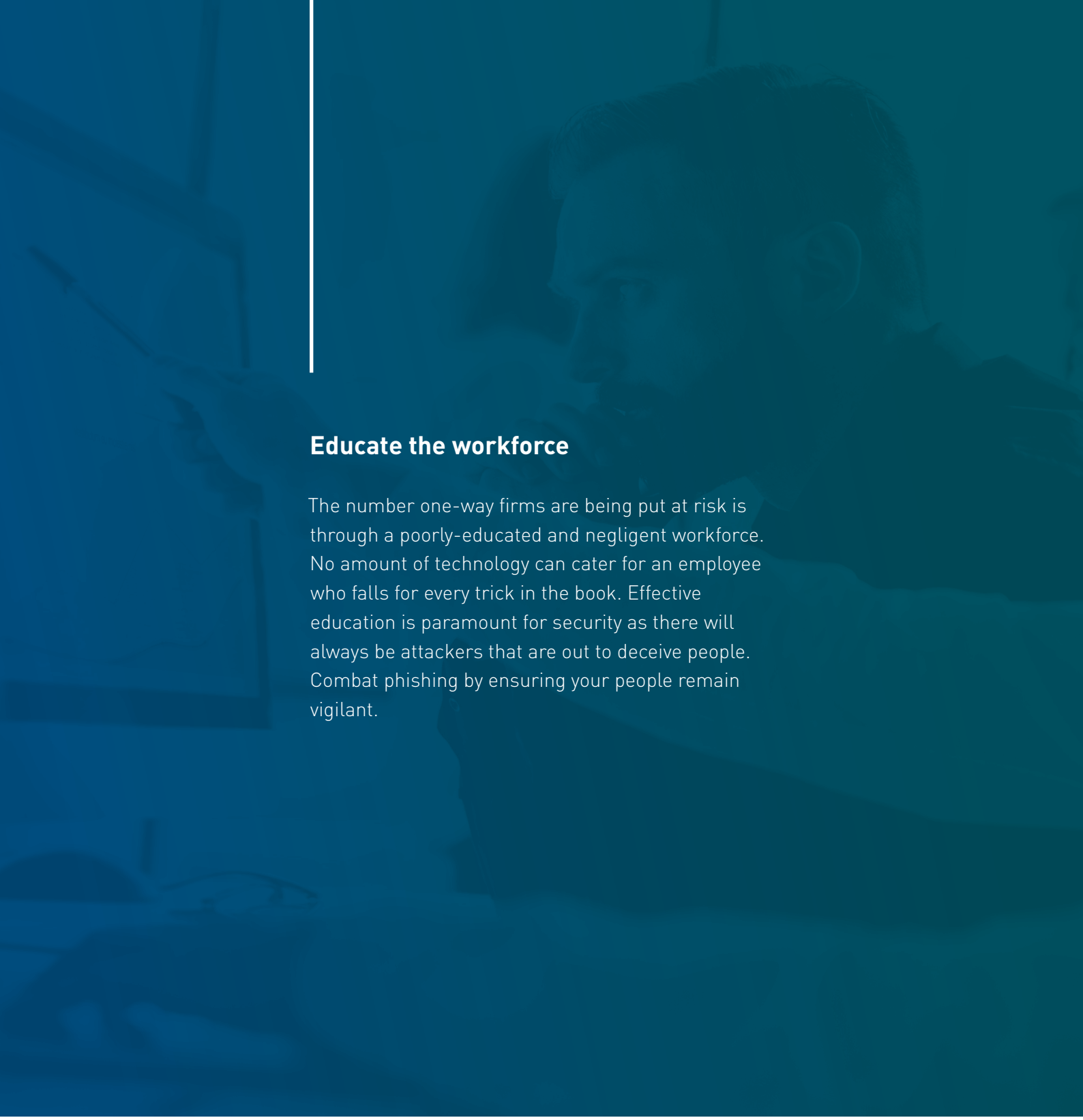
Anti-virus software

A whole host of anti-malware options are now available and choosing the correct one and keeping it up to date is essential. Prevent a data leak by having comprehensive anti-virus solutions installed and on-hand.

Don't use default settings

Many businesses have operators that work on the road who are given phones and tablets for business use. These devices have extraordinary amounts of valuable customer data that can be easily hacked into and accessed. It's just a matter of rogue individuals getting their hands on devices or utilising unprotected Wi-Fi.

To secure these devices, or harden as it's known to be called, administrators should turn off or delete non-essential services and apps, use extended passwords and a password manager, ensure updates are only performed on your own network, and create a policy that prohibits employees from improper use of the device. This should help minimise the risk of data being stolen or devices being replaced.



Educate the workforce

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.

MARK SAYS

Number one point on preventing an attack is the awareness. Businesses need to ensure that the staff are aware of these types of threats.

You wouldn't tell anyone your PIN. Why would you tell anyone your passwords?

WHAT ACTIONS SHOULD BUSINESSES TAKE IN THE EVENT OF A BREACH

If you are made victim to a cyber attack, you can use our five-point plan below. These actions reference your responsibilities and the necessary procedures which that had been breached; procedures which are explained in-depth within your Incident Response Plan. Having an updated and detailed Incident Response Plan is mandatory for all our clients; Romero Insurance Brokers will help clients create their own tailored continuity plan.

- 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.

- You should report a significant attack to the National Cyber Security Centre (NCSC). Depending on the breach, you may be required to report the incident to the Information Commissioner's Office. All cyber security incidents involving data should be reported to Action Fraud.

- Contact your broker immediately. Brokers will restate the steps you need to take to ensure you remain compliant with your policy. This gives you the best chance to recoup any losses you may sustain.

- It's important to have full communication throughout the entire process. 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.

- Once qualified cybercrime investigators have prevented further damage, you can then take steps to resolve the issue. Utilise your backup data, change all passwords and eradicate any holes used to breach.

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.

What is an Incident Response Plan?

MARK SAYS

Every business should have a BCP document, which stands for a Business Continuity Plan. This will list the actions and responsibilities upon disaster recovery or a breach. Very similar in the case of a fire or a flood - it's basically a piece of paper that prevents everyone running around in a panic when a breach is discovered.

In the event of a cyber incident, your IT department needs to have a clear plan. The aim is to stop the incident getting worse, as well as who to contact and notify about what has happened.

A Business Continuity Plan (otherwise known as an Incident Response Plan), helps to manage duties in a crisis. It should name a team with dedicated roles, including team leader, lead investigator, communications leader, C-suite representative, office administrator, human resources, IT, attorney, public relations, and breach response experts.

It may include how to write a statement to send out to the media to help prevent bad press and not allow the incident to look covered up. Multiple statements should target specific audiences, nipping issues in the bud, such as; what was affected, the data at risk, and when you will be back up and running.

Then it should detail how to safely bring affected systems online 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.

If you don't have an Incident Response Plan, making one should be a top priority. Then practice and review your plan. Without annual desktop run-throughs and simulation trainings, your staff could panic in the face of a data breach.

WHAT IS CYBER INSURANCE?

Having the right insurance means that, in the event of a cyber attack, you aren't alone. Cyber liability cover will provide the support a business needs, taking the brunt of the financial hit that cyber criminals can deliver.

Perhaps your standard cover already mentions cyber crime and cyber losses, perhaps as a package add-on. Check to see the extent of the cover, it could be minuscule, leaving you wide open for a devastating attack. Comprehensive cyber cover is essential and needs to protect against a wide range of vulnerabilities and circumstances, helping to avoid those unexpected fees.

MARK SAYS

Cyber Insurance not only provides the financial help in the event of a cyber attack, but also resources you need to help unravel the damage that's been caused. If your network is unavailable and you can't take payments or bookings, that's bad enough, but let's consider the damage to a business's reputation. Cyber insurance will help you get over the incident and get back on track.

What will cyber insurance cover?

Cyber insurance will cover the financial costs for your business, these business costs include:

- Investigating the crime
- Recovering data loss
- Restoration of computer systems
- Reputation management
- Extortion payments
- Fraud
- Business loss
- Business interruption – working in tandem with your business interruption policy
- Public relations expenses
- Commercial disruption

Cyber insurance also commonly covers the costs for third-party services, such as:

- Damages
- Settlements
- Legal defence costs

Certain businesses will require a higher level of coverage as they are more vulnerable to an attack. Only a tailored cyber insurance policy is able to plug the gaps and provide you with the appropriate level of cover. Contact Romero Insurance Brokers for a cyber security audit and to start taking the correct steps to protect your business.

CYBER INSURANCE WITH ROMERO INSURANCE BROKERS

An insurance broker like Romero is dedicated to protecting your today and tomorrow. But there is no other insurance broker 'like' Romero; we provide the full package from contact to service to success.

Acting as an expert middle-man between businesses and insurers, brokers are in the best position to audit cyber insurance policies. We stay up to date and well-versed on the sector's movements, offering expertise by making insurance policies transparent and understandable.

We feel strongly that businesses need to recognise the potential impact of a cyber attack, and should do all they can to protect themselves. We always have our customers' best interests at heart, which is why we offer a quote for cyber insurance at every renewal.

Dedicated to you; we believe that no two businesses are the same. We tailor our cyber insurance offers to your business, helping to ensure you achieve the correct level of cover. No matter what sector you work in, we've got the experience and skill to keep you safe.

We are a truly independent broker, with 25 years' experience and an in-house claims team. With us, you know that your claim is getting personal treatment and is being dealt with in the quickest time possible.

MARK SAYS

At Romero Insurance Brokers, we have a large dedicated claims team able to deal with any data breach cases. We will undertake a comprehensive review of your business. We go over and above, treating the client exceptionally. I personally, speak to clients and customers, helping to understand why you need cyber insurance and why certain protective software is needed.

DON'T THINK IT'S NOT GOING TO HAPPEN TO YOU, OR IT COULDN'T HAPPEN TO YOU.

IT'S JUST A MATTER OF WHEN.

0113 281 8110

enquiry@romeroinsurance.co.uk

ROMERO
INSURANCE BROKERS