CYBER & CRIME INSURANCE: THE RISKS TO YOUR BUSINESS & HOW TO PROTECT IT

JULY 2019

ROMERO
INSURANCE BROKERS

CONTENTS

THE RISE OF CYBER THREATS

90% of all cyber attacks are successfully executed with credentials stolen, or socially engineered from employees.

Identity Management Institute

Businesses are facing new and ever evolving risks at a rate faster than ever before.

Traditional risks to businesses such as fire, flood and theft are still very much in the minds of business owners. They will always pose a potential threat.

But as cyber threats are growing, adapting and becoming more sophisticated, it's more important now more than ever to make sure your business is protected.

It's easy to dismiss cyber threats as something that only happen to major corporations. That's not the case.

Every business, whatever their size, are targets for cyber crime and fraud.

Businesses at SME level often hold customer data with lower levels of protection, and may be more exposed due to lack of available expertise to defend these ever evolving attacks.

Whilst the probability of a flood may be a 1 in a 100 year event, 74% of SMEs have reported a cyber-security breach in the past year alone.

Department for Digital, Culture, Media & Sport

It's the relentless and continually changing nature of these threats that make them more important than ever to have at the forefront of your mind when keeping your business & customers secure.

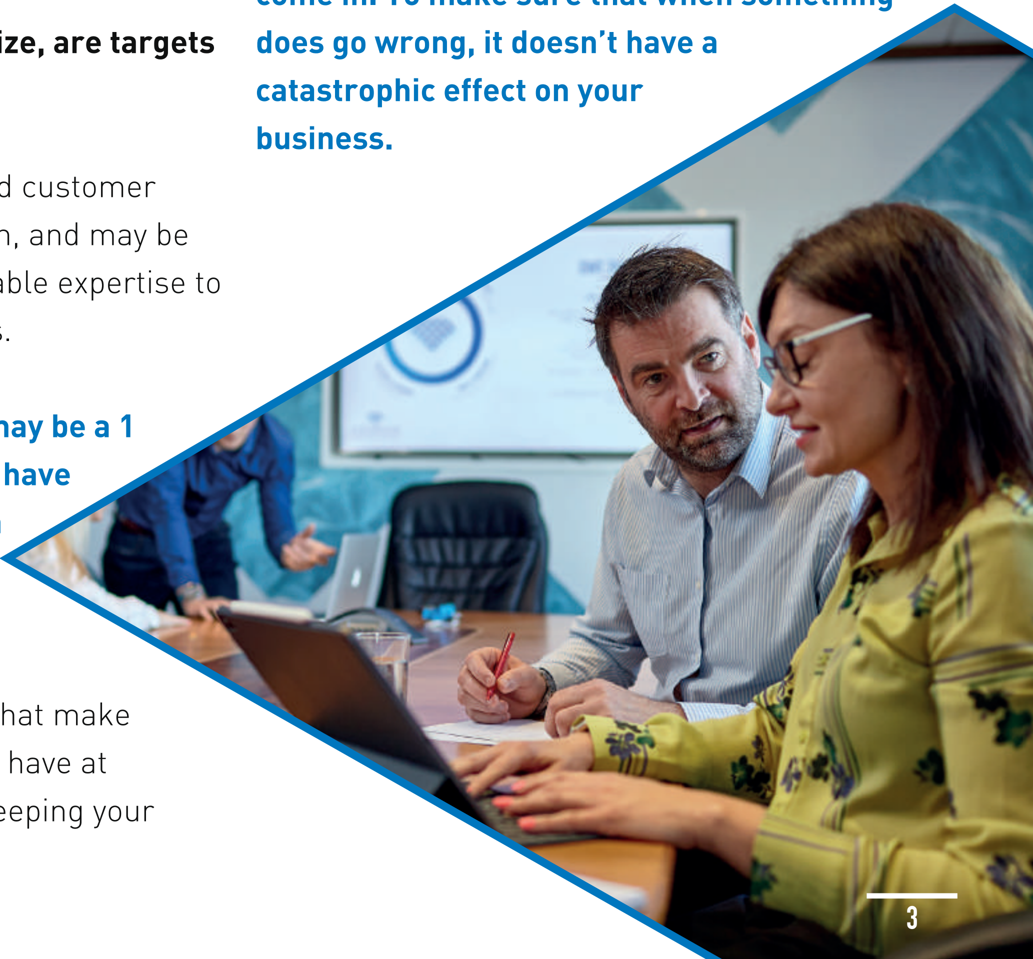
But it's not all negatives. Whilst the risks around cyber security are on the up, so are the ways in which you can protect yourself.

By having internal processes and policies, alongside investing in tools to protect yourself, you can help reduce the risk posed to your business.

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.

That's where Cyber & Crime Insurance policies come in. To make sure that when something does go wrong, it doesn't have a catastrophic effect on your business.



TYPES OF THREAT TO BUSINESSES

There are four key areas of threat to businesses, each with their own unique risks. In order to know how to protect yourself, you first need to know where you could be exposed:

Rogue Employee

- Physical theft of data
- Data could be sold to competitors
- Could be used for extortion

Negligence

- Employee could send data to the wrong place or source
- Physical loss of hardware such as a mobile phone or laptop
- Victims of phishing emails

Outsider Threat

- Hacking / Hacktivism
- Malware, ransomware & viruses
- Leads to theft of data, unauthorised access to systems or total shutdown of systems/sites

3rd Party Vendor Threat

- Cloud & other storage or data systems
- Network interruption
- Loss of data or theft of data
- Backdoor intrusions

Whilst both originate in a similar way, there are some distinct differences between the effects of cyber and crime on your business. And this means that they need protected differently.

WHAT ARE THE MOST COMMON THREATS?

Ransomware

- Designed to encrypt your files and data, blocking access until a sum of money is paid.
- To add pressure, these are often time limited with data deleted after the deadline has elapsed.
- Businesses without data backups are particularly vulnerable as they cannot restore.
- Research shows that Ransomware damages in 2018 cost over $8bn globally ***ThreatMetrix***

THINK - what would you do if you lost access to ALL your data?

Social Engineering Type 1

This can be split into a number of categories:

Vishing

- Contact is made by telephone
- Caller purports to be from your bank, the police or a fraud agency
- Purpose is to get you to reveal confidential information

Phishing

- Contact is made by email
- Sender impersonates well known companies such as banks
- Purpose is to get you to click on a link or attachment

Malware & Ransomware

- Malicious software such as Trojans or viruses
- Downloaded from phishing emails, illegal websites and ad banners
- Sits quietly in the background until you access a UK bank website

Smishing

- Contact is made by text message
- Sender impersonates well known companies
- Purpose is to get you to click on a link

THINK - does what you're seeing or hearing seem legitimate. DON'T take things at face value.

Social Engineering Type 2

- The art of gaining access to buildings, systems or data by exploiting human psychology.
- Even with the most sophisticated protection technology, processes and policies, a slip of individual concentration can put your business at risk.
- From unknown people accessing your building, to found USB sticks containing damaging data, to emails sent mimicking internal staff. These are just a few threatening scenarios.

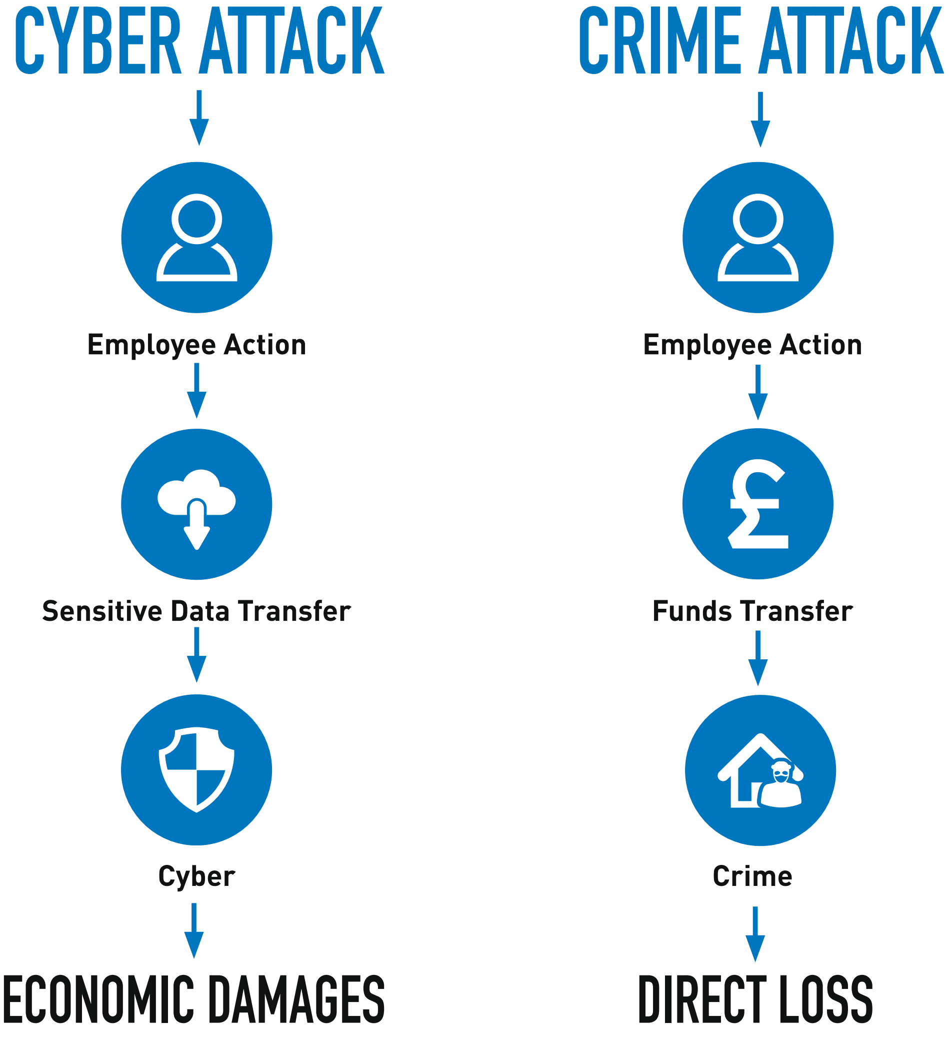
THINK - are you confident that your staff are properly trained to protect your business?

THE DIFFERENCE BETWEEN
CYBER & CRIME

Whilst both originate in a similar way, there are some distinct differences between the effects of cyber and crime on your business. And this means that they need protected differently.

Put simply, crime threats equate to a direct loss of funds whether that is through malicious action, employee dishonesty or social engineering. Cyber threats on the other hand create economic damages arising through a failure of network security or privacy controls which may cause indirect losses.

By far the biggest threat for both cyber and crime attacks, are through social engineering. Employees remain the greatest area of weakness down to human error, negligence or wilful acts. This means that social engineering scams are one of the most effective ways cyber criminals can affect your business.



CYBER ATTACK

Employee Action

Sensitive Data Transfer

Cyber

ECONOMIC DAMAGES

CRIME ATTACK

Employee Action

Funds Transfer

Crime

DIRECT LOSS

HOW CYBER & CRIME INSURANCE CAN HELP

Cyber & crime insurance are fast evolving areas, and policy covers can vary greatly. However, they generally include the following:

Privacy Breach Costs.

Sometimes separated into Breach Costs and Privacy Liability. Breach Costs will cover you for costs to deal with a security breach such as notifying clientele of a cyber breach, costs of a call centre to answer queries, public relation advice costs, the costs of engaging IT forensics, resultant legal fees and costs of responding to regulatory bodies. Privacy Liability will cover you against claims of infringement of privacy and legal costs in the event of a cyber breach.

Cyber Business Interruption

Should an IT failure or cyber attack affect your business, the policy will cover your loss of income whilst you are unable to trade normally. Cover can also include increased costs of carrying on your business in the aftermath of an attack.

Cyber Extortion

This cover protects your business from Ransomware and other malicious attempts to take control of and stop you accessing your operational or personal data until a 'ransom' has been paid. It can also cover consultants fees to negotiate and facilitate the payment of the ransom and reinstate the access to your data.

Hacker Damage

Cover is provided for the costs incurred in connection with a cyber event in order to repair and restore data, media and application components of your system that have been damaged as a direct result of the cyber event.

Cyber Media Liability

This covers your business should a claim be brought against you due to your digital media presence for libel, slander, defamation and infringement of intellectual property rights.

Cyber Forensic Support

The costs involved of cyber forensic investigation specialists (usually appointed by your insurer) following a hack or data breach.

Social Engineering / Cyber Crime

Cover with certain insurers can include social engineering and/or cyber crime events such as invoice fraud and 'bogus boss' scenarios. However be aware that not all policies include this cover.

DO YOU NEED IT?

Put simply, yes.

Whilst both originate in a similar way, there are some distinct differences between the effects of cyber and crime on your business. And this means that they need protected differently.

Whilst you may have some coverage for certain scenarios under existing D&O or Computer policies, it's important to remember that they often will not cover actual losses you experience in the wake of a cyber or crime attack, due to low inner policy limits.

Take a look at the scenarios below and you'll see how feasible it is that they could happen to you. And why dedicated Crime & Cyber policies will be invaluable protection for your business should the worst happen.

SCENARIO	CRIME POLICY	CYBER POLICY
An employee finds a USB drive in the car park and picks it up on the assumption that another employee has dropped it. To find out who it belongs to, the USB drive is inserted into the computer introducing malware to the network causing disruption.	NO	YES
A senior employee leaves a laptop on a train which contains hundreds of customer records.	NO	YES
You find that your system has been hacked and your files have been encrypted. The criminals have demanded the payment of a ransom to release a decryption key to restore your system.	NO	YES
During their notice period, a disgruntled employee steals the records of customers and employees.	NO	YES
A ransomware attack by criminals encrypts the data files of a company who relies totally on their IT systems to operate their business. The client decided not to pay the ransom to the hackers and the loss of business income due to the extended system outage was £250,000.	NO	YES
An employee receives an email from what they believe to be a genuine contractor noting a change in their bank details and enclosing an invoice for recent work carried out. The payment is made to the new bank account which later is found out to be a fraudulent account.	YES	NO MAY BE AVAILABLE WITH SOME INSURERS & SUBJECT TO INNER LIMITS
An employee receives email instructions from who they believe to be the CEO to make an urgent and confidential payment to a bank account for an important business transaction. The payment is made but it transpires that the email instructions came from a fake email account created by criminals.	YES	NO MAY BE AVAILABLE WITH SOME INSURERS & SUBJECT TO INNER LIMITS
In collusion with a third party, an employee in your accounts department sets up a number of fictitious accounts to syphon money to.	YES	NO

STEPS YOU CAN TAKE TO PROTECT YOUR BUSINESS: BE AWARE

Let's start with the basics.

Ask yourself a few simple questions about your cyber security processes:

1) Where's your latest backup and do you regularly test them? Testing should involve a FULL system recovery, not just a random spreadsheet. If your backup is contained on a USB memory stick and/or on-site, then consider what would happen if the media is corrupted and your build has burnt down.

2) Windows updates are free. Ensure that you are installing on a regular basis and that your software is still current and supported.

3) Ensure your passwords are strong and changed on a regular basis. Mobile devices should use either a pin code and/or finger print recognition.

That's the easy bit.

As human beings, we are eternally optimistic by nature. We are happy in our belief that bad things happen to other people, not us.

The same is true in IT in that 50% of businesses do not have an IT Business Continuity Plan. And of those that do have one, only 28% have tested it.

Disasters can, and do happen.

They come in many forms. There are the ones that are obvious, like fires, storms and floods. But they also come from other directions such as hardware failure, malware, data corruption and even actions of a rogue employee.

In the last few years, there has definitely been a noticeable increase in the latter kinds of events happening. Much of this is due to issues such as ransomware and other types of malware. But also in some cases, just due to the general increase in system complexity and good old human error.

THE THREE PILLARS OF CYBER SECURITY

Cyber security can be split into three distinct areas. Only by being aware and actioning protection in each of these areas do you best increase your level of protection and reduce the risk of a catastrophic loss.

PEOPLE

The biggest threat to any business is you and your employees. One small mistake could cost you and your business time, money and your reputation.

Human error remains the leading cause of data breaches. It's very important that all staff are able to identify and report all types of cyber threats. You are only as strong as your least informed employee.

PROCESS

Every company needs to communicate their organisations cyber security policy. Computer systems should have defined roles and departments follow documented procedures.

Businesses need to determine what rights and privileges users need to perform their duties, making sure higher-level system privileges are carefully controlled and managed. As well as individual logins for employees whenever possible, redundant accounts (including those of former staff members) should be removed immediately.

A strong cyber leadership is needed to establish and enforce processes. Management must be prepared to invest in cyber security resources.

Cyber threats are not just online - think physical. Unauthorised visitors, removable media, unsecured IT equipment are all examples where data can go missing.

THE THREE PILLARS OF CYBER SECURITY

TECHNOLOGY

You need the help of external hardware and software. This may come in the form of a Firewall, Antivirus or Spam filter. All help to mitigate cyber risks.

Your main business system may be current and supported, but when paired with another solutions, vulnerabilities usually appear.

It's a good idea to hire an external expert to evaluate your risks. Periodic cybersecurity assessments are a central element in any good security programme because it highlights the strengths you can amplify and the weaknesses you can improve. An external penetration test will provide a comprehensive report of your company's exposure.

THINGS TO DO NEXT:

CREATE AN INCIDENT RESPONSE PLAN

For all of the protections and defensive capabilities that you implement, anticipating that they will never be 100% effective is part of a comprehensive strategy.

A well thought out and thorough incident response plan will pave the way for a swift and effective reaction if your organisation does experience a successful attack.

A good incident response plan will spell out the right escalation path, so the most equipped team members are notified immediately if there is a problem. It will ensure that everyone understands the steps that need to be taken, who is responsible for which part of the response an even how to communicate to organisation leadership, external stakeholders and the public when necessary.

As a business, you need to understand what disaster scenarios you are likely to face and exactly how you will invoke. This should also include a decision making process in deciding *IF* disaster recovery should be invoked. There may be easier options, or this may be a minor transient glitch. This will usually become apparent very early on.

THE GOLDEN RULES OF CYBER SECURITY

KEEP YOUR SECRETS, SECRET

Don't share your personal information online unless you are certain that you're dealing with a safe website. The best way to tell if the site is safe or not is to look for an 's' in the URL (or web address), for the site you're visiting. An unsafe site will start with http://, whereas a safe site will start with https://

JUST. DON'T. CLICK

Do not click links in emails. Even if you think you know who the email is from. Also, don't download files. The only exception to the rule is if you are expecting someone to send you a link or a file. If you have spoken with them in the real world and know where the link will lead or what the file will contain, then it's okay.

TESTING, TESTING, 1, 2, 3.

When major incidents happen, it's important that you have a plan. There is nothing that can make bad things worse than decision making on the fly. You need to be absolutely sure you have a plan and that said plan is up-to-date, taking into account any changes made since the plan was last tested.

HOW WE CAN SUPPORT YOU

Let us see if you're properly protected and insured against potential cyber threats.

It's our philosophy, that no two businesses are the same, therefore their insurance products shouldn't all be the same. Lots of brokers will give you off the shelf products making an easy life for them. But what about you?

We're dedicated to making sure you have cover that is unique to you. We'll explore any potential risk you may be exposed to, and make sure that you're protected against it. Whatever sector you work in, whatever cover you need, we've got the experience and skill to keep you safe. And with the benefit of being truly independent, we can approach multiple markets to make sure we're getting the very best cover at a competitive price for you.

Confidential review

Whether you're due for renewal or just not sure you're getting the best deal from your current broker, let us know. We'll work completely confidentially, to review your potential exposure and let you know if we can help you any better.

We've seen businesses of all shapes and sizes with every risk imaginable, so you can rest assured that whoever you are, we'll be able to find the best insurance for you.

Award winning service

People are at the heart of our business. From our customers, to our staff, to the insurers we work with. We care about doing the best for every individual, and treat everyone as part of our family. It's our belief, that only by treating our teams well and creating a positive environment, will you get the exceptional service you deserve.

We're proudly independent, which lets us dedicate the time to really get to know everyone we work with and do what's right for them. And we're thrilled that this dedication has been recognised time and again from the people around us, and an impressive trophy cabinet!

ROMERO

INSURANCE BROKERS

For any questions or to see how we can support your cyber & crime insurance needs, get in touch with us today.

0113 281 8110
romeroinsurance.co.uk
enquiry@romeroinsurance.co.uk

Authorised & regulated by the Financial Conduct Authority
Registered in England & Wales no. 3362483