British Insurance Brokers' Association

CYBER INSURANCE GUIDE

cfcunderwriting.com

As we become increasingly reliant on technology, the potential impact of cyber-related incidents continues to grow. Yet the cyber insurance market is relatively new in comparison with other lines of cover.

This straightforward guide, brought to you by CFC Underwriting on behalf of BIBA, explains how cyber risk and insurance has evolved and how a good cyber policy addresses these modern exposures.

CONTENTS

WHAT "CYBER" MEANS

"Cyber" is one of the most talked about topics in business, insurance and media but also seems to be one of the most misunderstood. And with good reason – it is an area associated with jargon, buzz words and what feels like a whole lot of complexity.

This is largely down to the fact that the development of cyber insurance has historically been driven by the litigious US market, and therefore focused primarily on third party privacy exposures. At the same time, traditional insurance policies have tried, but rarely succeeded, at addressing cyber risks; this has left clients believing many exposures are covered when they actually aren't.

WHILE THE TECHNOLOGY REVOLUTION HAS BROUGHT WITH IT UNPARALLELED LEVELS OF CONVENIENCE AND CHOICE TO MILLIONS OF PEOPLE ACROSS THE GLOBE, IT HAS DONE THE SAME FOR THE CRIMINAL UNDERWORLD

So what should we mean when we talk about cyber risk? What do clients need to protect themselves against? The real answer is crime.

Technology has revolutionised the world for businesses and individuals alike and the past twenty years in particular have seen monumental shifts in human behaviour directly linked to technological advancements. From the way we shop to the way we access bank accounts and book holidays, everyday life has changed fundamentally.

However, while the technology revolution has brought with it unparalleled levels of convenience and choice to millions of people across the globe, it has done the same for the criminal underworld. It is now far easier and far more lucrative for criminals to ply their trade digitally rather than physically. Cyberattacks are the modern crime and cyber insurance is the way to protect against them.

HOW CYBER RISK HAS EVOLVED

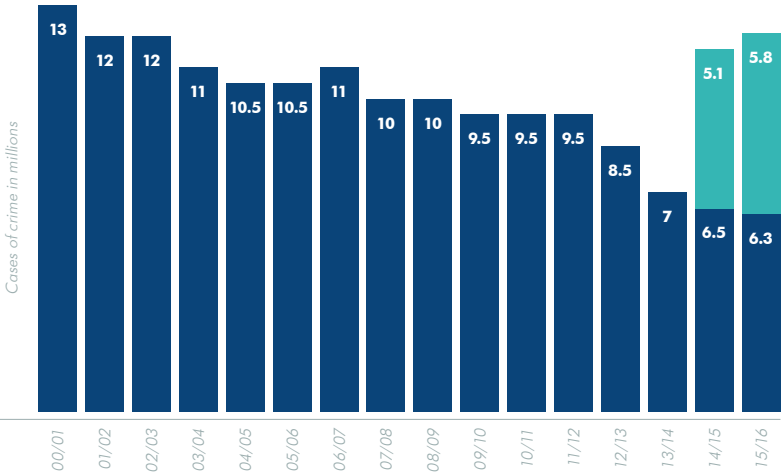
The technology revolution has irreversibly changed the way that businesses operate: the ability to send electronic mail rather than physical mail; the ability to store information electronically rather than physically; and the ability to move money remotely rather than in person has brought speed and efficiency allowing businesses to reach levels of productivity that were never before imaginable.

But technology has also fundamentally changed the nature of assets. The shift from the physical (post, paper records and bank cheques) to the digital (email, data and electronic funds) means that some of our most valuable business assets are now accessible by anyone in the world from anywhere in the world.

This fact fundamentally changes the nature of the risk of them being lost, stolen or destroyed. And that's what cyber insurance is there to protect against – the loss, theft or destruction of a company's digital assets.

RISE OF CRIME

The inclusion of cybercrime in the 2014/15 ONS report on crime in England and Wales put the crime rate back up to levels not seen since the beginning of the millennium.



Figures available from the Office for National Statistics (ONS) website: www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice

THE NEED FOR A NEW TYPE OF INSURANCE POLICY

Cyber insurance is necessary because traditional insurance policies were not designed to handle 21st century threats. Many standard first party insurance policies such as property and traditional crime were designed to deal with threats to a company's physical assets – their buildings, machinery, office equipment and tangible money only.

There has historically been little to no protection offered under these policies for loss of, theft of or damage to data, systems and electronic funds.

However, most businesses these days now have a much greater reliance on their digital assets than they do on their physical ones, which makes a new kind of policy essential.

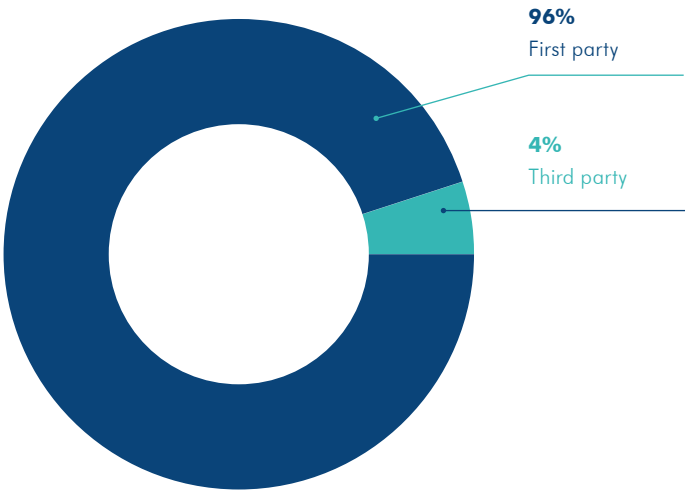
FIRST PARTY RISK AND THE HISTORY OF CYBER "LIABILITY"

Cyber insurance for a long time was (and still is) referred to as cyber "liability" which is really a by-product of where it came from. The first cyber insurance products were developed by professional indemnity underwriters, which naturally meant they were focused on third party exposures, such as passing on a computer virus to a third party and being sued for it.

However, today it's clear that the vast majority of cyber events tend to cause financial loss to the insured themselves as opposed to third parties that they deal with. In fact, cyber claims figures show that less than 5% of cyber claims by volume involve third party legal action.

Given that cyber is predominately a first party exposure, cyber policies are actually much more akin to traditional property and crime policies than they are to liability policies, making cyber "liability" a misnomer.

FIRST PARTY V THIRD PARTY CLAIMS



CFC Underwriting cyber claims statistics, 2017

TYPES OF CYBER CLAIMS

More than 95% of cyber claims are for first party losses only and they fall into three broad categories:

1. *THEFT OF FUNDS* – this is straight forward theft of money from a company's bank account. The fact that nearly every business can now move its money around electronically and remotely means that it is much easier to steal. Criminals no longer target physical banks – they target online accounts. And if a business has somehow been negligent in allowing this to happen, the bank will not reimburse them.

2. *THEFT OF DATA* – data is valuable, and if something has value, it is worth stealing. Identity theft has reached record levels in the UK and in order to commit identity theft, criminals need data. Seemingly innocuous information such as names and addresses stored on a computer network can be worth more money than you think.

3. *DAMAGE TO DIGITAL ASSETS* – in order to operate, businesses now have an incredibly high dependency on their systems, and criminals know that. By either damaging or threatening to damage a firm's digital assets, attackers know that they can extort money from their victims who might prefer to pay a ransom rather than see their business grind to a halt. And even after paying up, the victim is often left with systems that are unusable and costly to fix.

In some cases, there may be no financial incentive for the attacker at all. In the same way that criminal damage to property doesn't always have a financial incentive, damage to digital assets doesn't need to either.

Claims for theft of funds are actually very easy and quick to quantify, but for theft of data claims, the financial impact can vary depending on the nature of the data compromised and how much of it was stolen.

The costliest part of a cyber event is often responding to the incident. For example, if an attack has managed to compromise a company's computer network, then IT specialists are going to be needed to stop the attack, protect against further immediate threats, and work out what has been stolen. There is then a financial cost associated with limiting reputational damage, notifying clients or customers whose data has been stolen, and offering them identity theft protection solutions if necessary.

Damage to digital assets claims can be easy to determine especially if there is an extortion demand which the victim has paid (the amount of the claim is the cost of the ransom) but more difficult if we're talking about the cost of using IT specialists to rebuild systems or data – which might only be calculated after the work is completed.

The key point underpinning each of these types of claim is that there is a direct financial loss to the victim business which can be transferred with a cyber insurance policy.

HOT TOPIC

THEFT OF FUNDS

It is worth noting that whilst this is one of the biggest issues facing businesses in the UK today, not every cyber policy includes cover for theft of funds and those that do can vary in how broad the cover offered is. Please see the "More About Cybercrime" section on page 14 for more details.

HOW A CYBER POLICY WORKS

Cyber insurance policies tend to be modular in nature, meaning that they consist of a variety of different coverage areas and, for many, that has led to confusion around what exactly they cover and how they work.

Broadly speaking, most cyber policies can be divided into two areas – first party covers and third party covers.

The first party sections cover the insured's own financial loss arising from a cyber event, which is defined as any actual or suspected unauthorised system access, electronic attack or privacy breach. The third party sections cover the insured for liability actions against them arising out of a cyber event.

Typical "first party" cyber policy covers include:

INCIDENT RESPONSE

This section of cover will generally pick up all of the costs involved in responding to a cyber incident in real time, including IT security and forensic specialist support, gaining legal advice in relation to breaches of data security, and the cost associated with having to notify any individuals that have had their data stolen. One of the most important aspects of a cyber policy is that it provides access to the right specialists as well as paying for their services.

CYBER EXTORTION

As the name suggests, this section covers costs incurred in responding to fraudsters attempting to extort money out of an insured by either threatening to carry out a cyberattack or by threatening to expose or destroy data after having already compromised the victim's network. Ransomware, where the victim's data is encrypted (converted into an unreadable format) and only made accessible again by the payment of a ransom demand to the attacker, is one of the fastest growing forms of cybercrime.

SYSTEM DAMAGE

This section covers the costs for an insured's data and applications to be repaired and restored in the event that their computer systems are damaged as a result of a cyber event. This is often critical in getting a company back up and running.

SYSTEM BUSINESS INTERRUPTION

This cover aims to reimburse loss of profits and increased costs of working as a result of interruption to a business' operations caused by a cyber event. It works in a very similar way to traditional business interruption insurance except the trigger is a non-physical peril as opposed to a physical one.

Whilst third party liability claims tend to be less common in cyber insurance, it is still important to have cover for them.

Typical third party (liability) cyber policy covers include:

NETWORK SECURITY AND PRIVACY LIABILITY

This covers third party claims arising out of a cyber event, be it transmission of harmful malware to a third party's systems or failing to prevent an individual's data from being breached.

REGULATORY FINES

If permitted to be included under a policy, this will cover the cost of certain fines and penalties that a regulatory body might enforce on an organisation as a result of them having suffered a data breach.

MEDIA LIABILITY

This covers any third party claims arising out of defamation or infringement of intellectual property rights. Media cover started out in cyber policies to offer protection in respect of online content only, but as policies have broadened over the years, it's not uncommon for full media cover to be provided.

HOT TOPIC

CYBER IN TRADITIONAL POLICIES

It is very common for any one cyber claim to trigger multiple sections of cover within a cyber policy. It is also important to note that while many traditional policies may claim to include some element of cyber cover, they often miss some of the key coverage items mentioned above, namely incident response, system damage and system business interruption.

MORE ABOUT CYBERCRIME

Most cyberattacks are criminal acts and so technically can be labelled "cybercrime". Within the context of a cyber insurance policy, however, cybercrime usually refers to attacks that involve theft of funds from the victim as opposed to theft of data or other digital assets. Theft of funds generally occurs in one of three ways:

1. EXTORTION – as mentioned earlier in this guide, the attackers use the threat of a cyberattack or the threat to expose or destroy data that they have already compromised, to extort money out of the victim;

2. ELECTRONIC COMPROMISE – the attackers manage to hack into the insured's network, gain access to their online accounting or banking platforms and start wiring money out of the victim's account;

3. SOCIAL ENGINEERING – the attackers imitate a third party (e.g. a vendor or supplier of the victim business) and trick the victim into wiring money to the wrong bank account. The victim believes they are wiring funds to a third party they know but in actual fact it is going to the fraudsters.

Whilst extortion, in the form of ransomware, has been one of the fastest growing forms of cybercrime in recent years, social engineering scams have also increased dramatically, and they tend to be more severe. So called "CEO fraud", where fraudsters impersonate the CEO of a company (or other senior executives) and email instructions to staff in the accounts department to transfer funds to criminals' bank accounts, has been incredibly successful and a huge source of claims by UK businesses.

It is critical to note that not all cyber insurance policies include cover for the above types of loss. Many will include extortion as the bare minimum but no theft of funds from a victim's bank account. Some will extend to cover for theft arising from electronic compromise but not from social engineering. Some will cover all of them. It is also worth noting that some of these covers can be found in a traditional crime policy too but the cover varies widely.

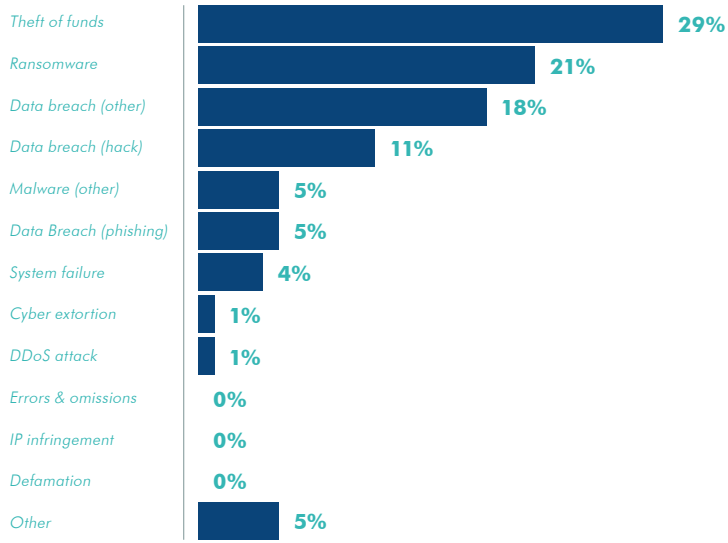
GENERAL DATA PROTECTION REGULATION (GDPR)

The EU General Data Protection Regulation (GDPR) brings with it new rules around how entities collect, process, store and transmit personal data including the security they have in place and this has created lots of discussion around how this may change the cyber exposure faced by UK businesses.

Given the complexity of the topic, BIBA has produced separate guidance on the GDPR which should be referred to for further information. Within the context of cyber insurance in general, however, it is worth noting that other territories, such as the USA, have had much more stringent data protection regulation than the UK for many years and the claims trends still show that the vast majority of claims are first party losses. Consequently, we shouldn't expect the situation in the UK to alter much either.

Please contact BIBA for further information about the GDPR.

KEY 2017 CYBER STATISTICS



CFC Underwriting cyber claims statistics, 2017

POLICIES IN ACTION: CLAIMS EXAMPLES

SOCIAL ENGINEERING

A financial controller in a high street law firm received a call from someone purporting to be from the firm's bank, explaining that some suspicious wire transfers had been flagged on the business account. The caller insisted that, in all likelihood, funds had been stolen and the business was in immediate danger of the remaining funds being drained unless they put a freeze on the account; a password and pin code would be required to do so.

Not wanting to cause any further loss, the financial controller confirmed the pin code and password to the caller, and the caller confirmed that the freeze had been successfully applied and that they would be in contact once the situation was resolved. Upon calling the bank the next day, however, the financial controller was told that the bank had not in fact been in contact and that £89,900 had been wired to three overseas accounts in nine separate transactions, all of which were too late to recall. Because the transactions had seemingly been authorised, no reimbursement was offered by the bank.

Fortunately, the law firm had purchased a cyber insurance policy containing cybercrime cover with social engineering and was able to recover the full amount from insurers less their policy deductible.

DATA BREACH

A private healthcare clinic based in London was the victim of a cyberattack where patient information had been stolen. Hackers were threatening to post the data on a public website unless they received a ransom payment of £10,000 in Bitcoin. The owner of the clinic immediately contacted their IT team, but as this was outside their usual remit, the team was unsure how to help.

Next, they called their cyber insurers. Within thirty minutes they received a callback from the insurer's in-house incident response team who was able to advise the insured's IT team what to do in order to fix the immediate vulnerability. The insurer also engaged with a local IT forensics specialist who was able to visit the business in question and start the process of verifying the attackers' claim. After an investigation of the insured's network, the forensic specialist was able to advise that data relating to 3,000 patients had been compromised, but it was a database containing names and addresses only – no sensitive medical data had been accessed.

Consequently, the decision was made not to pay the ransom demand. Instead, the insurer connected the company with a crisis communications consultant. This consultant advised them that it would still be good to notify affected patients to prevent any adverse reputational impact and assisted with the construction of a notification notice that was quickly and discretely emailed out.

They have heard nothing further from the hackers to date. The clinic's cyber insurance policy covered costs of engaging the IT forensics company (£10,000) and the crisis communications company (£5,000) for a total claim of £15,000 less the small policy deductible.

BUSINESS INTERRUPTION

A food trucking company suffered a ransomware attack where cybercriminals encrypted all of their data files and requested a ransom of £7,500 in exchange for the decryption key. Like many modern companies, their entire business was run via their systems and hackers had encrypted every single piece of data that they required to run their operations – their routes, logistical information, key contacts, and how much stock they had and needed to order – as well as shutting down their payment card processing capabilities.

Even though business had come to a halt, the CEO refused to give in and pay the demand. Instead, the company immediately set about reconstituting data from a collection of paper records and their employees' knowledge of day-to-day operations, resulting in a large amount of overtime costs right away. What was worse, however, was the loss of business income that resulted from the extended outage of their systems and the consequential impact on operations.

For the month of November, the insured had forecast that they would complete 220,000 sales transactions but, due to the system outage, they were only able to process around 140,000. With an average transaction value of more than £9, that was a loss in revenue of nearly £780,000. After adjustment by their cyber insurance provider, the insured was able to recover nearly all of the financial loss suffered under their policy.

SELLING CYBER INSURANCE

Objections to a new insurance product that a business has never before invested money in is natural. But it's important to overcome these objections to ensure that clients have relevant cover in place. Here are some of the most common objections we've seen raised and the reason why it's important that they are countered:

"CYBERATTACKS ONLY AFFECT BIG COMPANIES. I'M NOT A TARGET... "
This is wrong. While blockbuster data breaches against household names tend to make the news, attacks against smaller organisations are now so frequent that they are no longer newsworthy. More than 50% of UK SME's have reported being the victim of some sort of cyberattack and the increasing frequency is being matched by increasingly high levels of severity.

"WE ARE A "TRADITIONAL" BUSINESS THAT DOESN'T COLLECT SENSITIVE DATA SO WE HAVE NO EXPOSURE..."
Cyber risk is not just about data breaches. Any business that makes wire transfers from a bank account is at risk of funds transfer fraud, and social engineering scams have made victims of businesses ranging from building contractors to beauticians. First party business interruption losses do not require a business to collect sensitive data to be exposed – merely being unable to access their systems puts businesses at risk of financial loss, particularly where technology is increasingly utilised in day-to-day operations.

"WE ALREADY SPEND MONEY TO SECURE OUR NETWORKS SO WE DON'T NEED CYBER INSURANCE..."
It's important that businesses are conscious of IT security and take steps to protect themselves from threats, but no one can ever be 100% secure. Cyber threats are rapidly evolving and there are a plethora of ways in which attackers can access networks. Additionally, strong IT security controls don't always protect against events which don't necessarily involve a third party accessing the network such as social engineering attacks or the actions of a rogue employee. Refusing to purchase cyber insurance because you have IT security controls is akin to refusing to buy property insurance because you have physical security controls – the two should not be mutually exclusive.

"WE USE A THIRD PARTY CLOUD PROVIDER TO HOST ALL OF OUR DATA AND NETWORKS SO THE RISK IS WITH THEM, NOT US..."

Incorrect. If the cloud service provider suffers an attack and goes down, meaning you cannot operate, it is your business that will potentially suffer first party business interruption and the additional costs incurred in attempting to continue trading. It can prove extremely difficult, potentially impossible, to recoup these losses from your IT provider.

Additionally, if a breach of data that you are responsible for occurs at a third party provider, it is still you that is responsible and your reputation that will suffer.

"DON'T THE BANK HAVE A DUTY TO REIMBURSE THEFT OF FUNDS FROM MY ACCOUNT?..."

Not if you were negligent in allowing access to a fraudster and not if you or an employee of yours were duped into wiring the funds themselves. If the bank is not at fault, they will not reimburse.

All information in this booklet is correct as of 01 May 2018. We take great pride in our professional expertise on cyber insurance and as such would like to state that certain content within this guide is liable to become outdated due to the fast-paced nature of the cyber security and insurance market.

CFC is a specialist insurance provider with a track record of pioneering emerging risks and disrupting inefficient insurance markets. Today, CFC has over 30,000 cyber clients in more than 60 countries globally and the largest team of dedicated cyber and technology underwriters in the London market.

We are a proud BIBA scheme provider for both cyber insurance and product recall.

To contact us, please email enquiries@cfcunderwriting.com or dial 0207 220 8500. Our cyber team can be reached via email on cyber@cfcunderwriting.com.

The British Insurance Brokers' Association represents the interests of insurance brokers, intermediaries and their customers and has nearly 2000 firms in membership. To reach them, please call 0344 770 0266, email enquiries@biba.org.uk, or visit www.biba.org.uk.

cfcunderwriting.com