Mactavish
Expert insurance buyers

Mactavish cyber report

Building corporate resilience.

Cyber-attack is one of the fastest growing problems faced by businesses in the UK and worldwide.

Governmental bodies, multinational corporations and sole traders are all subject to the risk of attack. In just two weeks in September 2022, Uber, Holiday Inn, Revolut and the Government of Albania were all reportedly hit by hackers. The motivations behind these attacks may have been different, some a protest against capitalism, others a simple, if malevolent, desire to extort a ransom, however the effect was the same. Business activity was disrupted, confidence was eroded and costs mounted up.

> **Research shows that UK businesses are 85% more likely to suffer a cyber-attack than they were 4 years ago.**

In this context, it is not surprising that cyber insurance has been about the hottest topic in insurance for the last few years. But despite a growing demand, hard insurance market conditions characterised by high premiums, limited and narrowing capacity, and standardised policies unfit for purpose are failing to meet the client needs. To better understand what was happening in the market, we revisited a survey we initially conducted in 2018, interrogating a panel of UK businesses, to ask them about their experience of cyber-crime and how the insurance industry was performing in response to the threat.

> **At a time of heightened exposure to cyberattacks, our survey unveiled that nearly a quarter (23%) of businesses have no specific cyber insurance cover and that the accessibility and quality of such cover is declining.**

Read on to understand the new cyber risk landscape and best practices to get the best risk placement solutions for your business and minimise your loss exposure.

Research findings

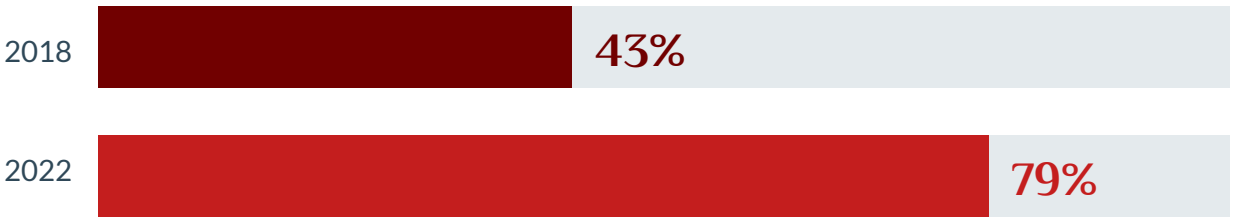
The results of our survey[1] should give UK businesses and the insurance industry pause for thought. Cyber risk is clearly on the rise, and while the take up of cyber insurance has risen, confidence in these products has fallen.

This is a worrying combination and suggests the insurance industry is missing a trick. Demand for these products is growing, however, the provision of insurance is not keeping pace. Cover is being eroded as exclusions and policy terms are tightened, leaving customers feeling dissatisfied and, ultimately, uncertain about what exactly it is they are buying.

Growing exposure –

businesses are 85% more likely to suffer a cyber-attack than they were 4 years ago

Percentage of businesses that experienced a cyber-attack in the previous year



Cyber-attack threats experienced by UK businesses as reported in 2022

70%

of companies perceived a considerable or highly significant threat from cyber attacks over the next 12 months.

36%

around 1/3 have seen a net increase of the volume of cybersecurity incidents in the past 2 years.

34%

another 1/3 have reported increasing threats in the severity of cybersecurity incidents.

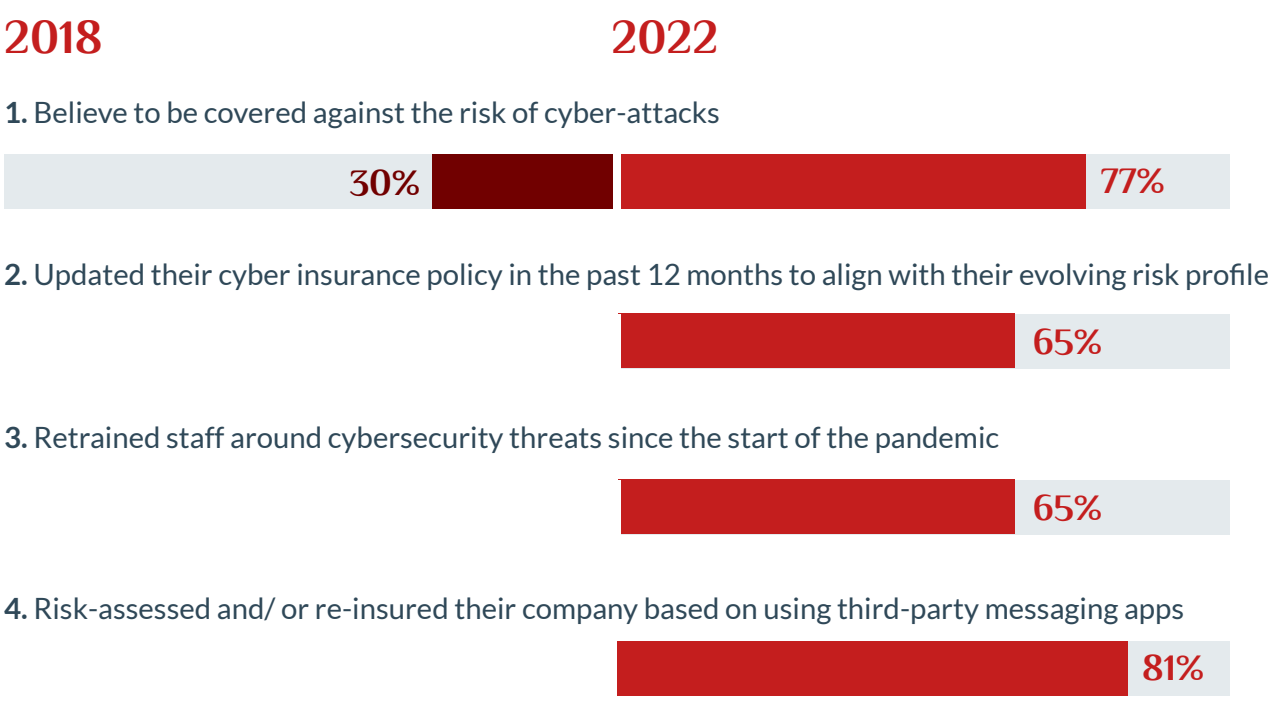
50%

have suffered a loss of revenue or data in the previous year due to cyber-at-tacks.

1. Insights based on two surveys conducted by Mactavish respectively in October 2018 with 700 UK senior managers and reconducted in May 2022 with 202 risk professionals and senior managers in companies with over £5m turnover, across all sectors of the industry.

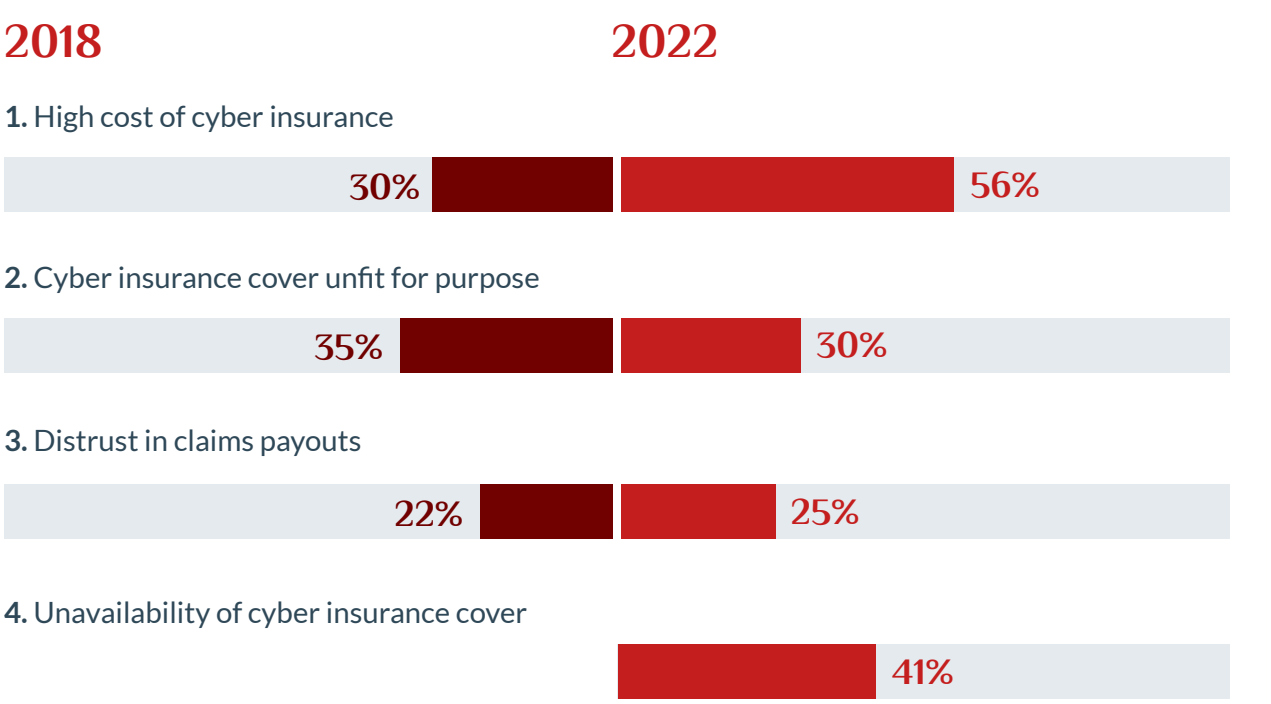
Growing protective measures against cyber-attacks

Main measures implemented by UK businesses to mitigate the risk of cyber incidents



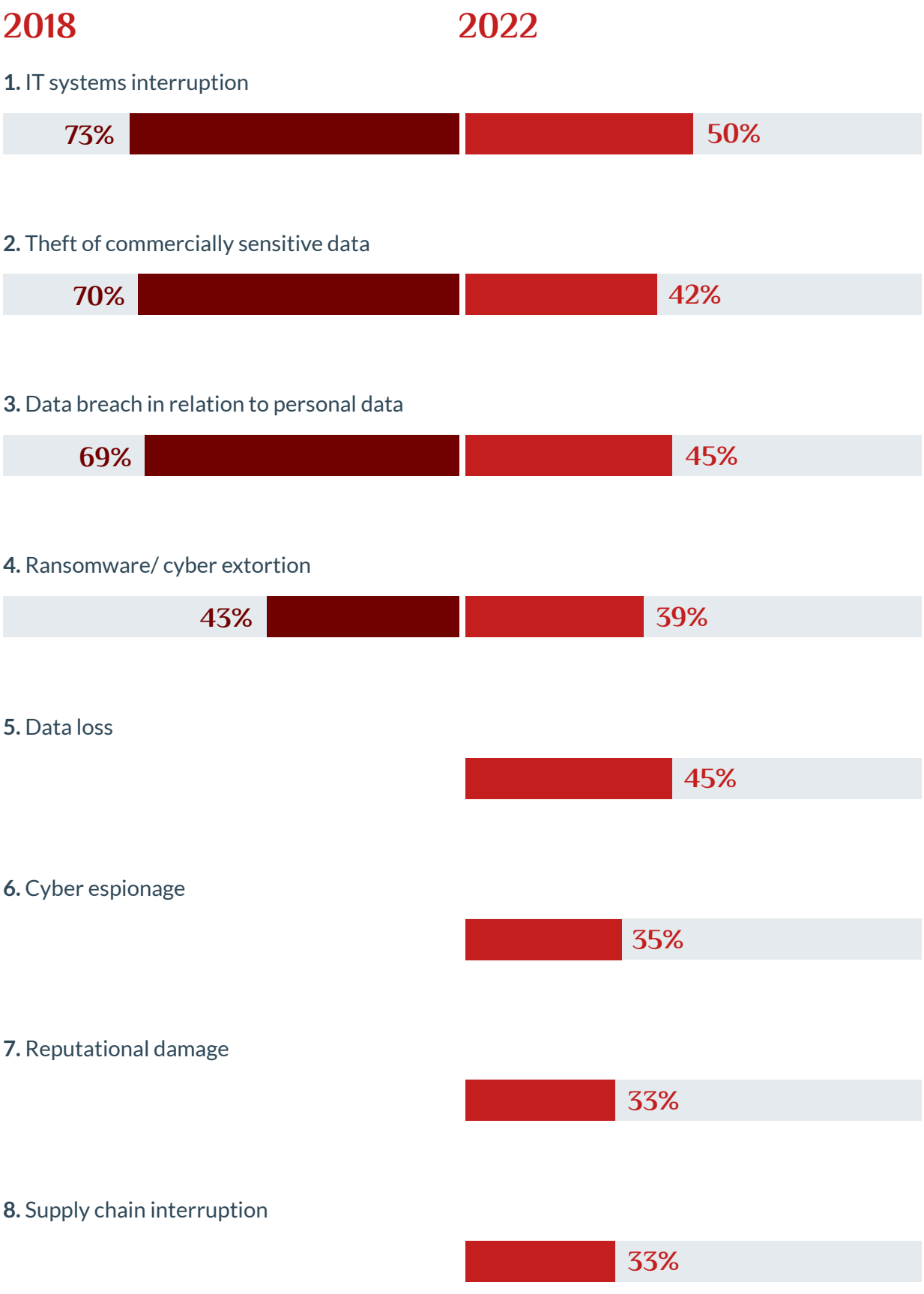
Barriers to adoption of cybersecurity protective measures

Main reasons why companies are not covered against the risk of cyber-attacks



Main cyber-risk concerns and exposure

Cyber-risk concerns continue to be high across all common cyber-attacks in 2022



Main cyber-attacks experienced by UK businesses as reported in 2022

34%
Malware attacks

29%
Data loss

26%
Theft of commercially sensitive data

25%
Cyber espionage

24%
Data breach/Privacy regulation issues

21%
Ransomware/ cyber extortion

The new cyber risk landscape

Our survey clearly demonstrates that it is not just the threat of cyber-attack that is on the rise, actual losses have also nearly doubled over the last four years.

Looking at the previous twelve months, 79% of respondents revealed that they had experienced a loss from a cyberattack, with 50% of those attacks resulting in a loss of data and/or revenue.

This is 84% more cyber incidents than registered 4 years ago.

As a response to increased security threats, cyber risks are becoming a central business preoccupation, and a growing part of business continuity plans across all sectors not just those traditionally considered attractive cyber "targets".

Encouragingly, our survey revealed there is 61% more cyber insurance cover in place in 2022 compared to 4 years ago. Businesses are taking a more proactive position towards cyber protection. What's more, cyber-security is no longer the preserve of larger businesses, but a threat taken seriously by SMEs alike. The growing understanding of the threat has been prompted by increased external geopolitical threats, as well as new internal dynamics and widespread working practices in response to the Covid-19 pandemic.

External geopolitical tensions

Perhaps the most obvious change in the international business environment to have taken place since our last survey, is the start of the Russian war in Ukraine. While the headlines quite understandably focus on the physical threats posed by the war, another conflict is taking place behind the scenes. Since the start of the year, scores of largely Ukrainian sites have been targeted by malware attacks, according to Microsoft Threat Intelligence Center. Experts, including the National Cyber Security Centre in the UK, the FBI and National Security Agency in the USA have warned that such attacks may spread as Russian state-sponsored actors attempt to escalate the economic war that is being pursued alongside the military offensive. To date, the only attacks to have been identified were against Ukrainian companies, however, their impact has spread internationally. In a statement issued on 10 May 2022, the UK's then Foreign Secretary, Liz Truss, described one such attack as "… clear and shocking evidence of a deliberate and malicious attack by Russia against Ukraine which had significant consequences on ordinary people and businesses in Ukraine and across Europe."

While the evidence to date suggests that state-sponsored hacking of the type seen in Ukraine has political goals, there is growing concern that countries with the cyber capability and economic problems of Russia may look to cyber-crime as a way of generating foreign currency. North Korea's Lazarus Group, with its attacks on Sony, AstraZeneca and various cryptocurrency exchanges, is the obvious case study for this kind of cyber-crime. Furthermore, there are concerns that Russia is using Ukraine as a testing ground to enhance its offensive capabilities in the cyber realm.

Against this background, the response of the insurance market has been disappointing and self-defending. Since the start of the war in Ukraine, insurers have been accelerating the rewriting of insurance contracts.

Cyber Insurance contracts have broadly defined exclusions for war and terrorism which include events such as State or Government actions. These exclusions are intended to protect insurers in the event of a large scale cyber conflict causing losses across the country more widely. However, they often leave individual businesses exposed while believing that their cyber insurance will cover them in an increasingly perilous landscape. Such exclusions have led to very large claims being denied and litigated, as occurred following the NotPetya attacks in 2017 whereby large, cyber claims of up to $1bn and above, were denied by insurers on the grounds that they were warlike actions by the Russian state.

The ambiguous definition of these events continue to undermine the reliability of cyber wordings; for instance, do State or Government actions relate to warlike acts and if so, how are these defined? Is any act of state classed as a warlike act? What is even more problematic is that such clauses often make it incumbent on the insured to prove that a war/terrorism exclusion does not apply.

Due to the covert nature of such attacks, it remains fiendishly difficult to establish and prove perpetrators, motives and intent, much less for an insured to prove what such an attack was not.

Recently, Mactavish has seen even more broad sanctions exclusions added to a wider range of insurance contracts. Sanction clauses arising from events in Russia and Ukraine can impact further insurance lines such as D&O. In the most extreme cases, Mactavish has found client exclusions that have the effect of removing cover for any activity involving interaction with anyone of Russian origin (even if not dealing with any party within Russia itself).

Pandemic and remote working

The rapid adoption of remote working practices forced on companies by the Covid pandemic has introduced a whole new dimension of risk into almost all business operations. Amongst them are: the use of home networks with potentially more varied and less secure hardware characterised by looser privacy policies and procedures; remote connection to central networks; increase in staff turnover in many sectors; and difficulties remotely managing system updates and protection. It was perhaps no surprise that cyber-criminals responded to the pandemic and lockdowns by increasing the number of scams and phishing attacks targeted against private individuals. All of these changes present their own challenges, requiring complex and sometimes expensive responses if they are not to leave companies open to increased cyber-attack risks.

Widespread adoption of video & messaging technologies

Alongside the increase in home working and associated device proliferation, we have also seen a spike in the use of instant messaging as well as the growing adoption of a range of videoconferencing technology. All of these should force companies to reconsider their protection measures against cyber threats.

As soon as companies and their employees start to rely on the use of third-party hosted platforms, they lose an element of control over their security. Such risks can be mitigated but it requires careful thought and, normally, the imposition of additional risk management measures on how staff work in these higher risk environments. Many cyber insurers are refusing to underwrite cyber risks if the insured does not have defined levels of security measures in place such as Multi Factor Authentication (MFA), tightened device and network access, and cyber-awareness training for staff.

Cyber insurance requires tailoring to meet market needs

Cyber market shifts are also happening in the context of the longest insurance hard market in living memory, with 19 consecutive quarters of pricing increases and commercial premiums on average now 2-3 times the price they were pre-pandemic, and a 102% increase on cyber insurance alone in the first quarter of 2022[2].

This sharp cost rise is allied to reduced cover and a heightened frequency and severity of claims activity as reported in Marsh' Global Insurance Market Index[2]. Cyber insurance is at the most difficult end of a difficult market: whether in terms of pricing increases, contractions in cover available, more demanding and inflexible information requirements to be able to buy cover, and relatively low buyer confidence in the reliability of what remains a relatively new and untested product.

At a time of heightened exposure to cyberattacks, the survey unveiled that nearly a quarter (23%) of businesses have no specific cyber insurance cover.

The main blockers remain high costs of cyber insurance; distrust in claims paybacks and perceived inadequacy of the cover on offer.

The survey revealed that:

- For over half (56%) who have prioritised cyber protection, the rising cyber insurance policy costs have prompted cutbacks to other parts of the business
- The most affected business areas reported include cutbacks to office premises (55%) and staff bonuses (43%)
- Other insurance policies (25%) have also been deprioritised, indicating a wider impact on the risk profile of UK businesses.

Hardened market conditions

Cyber remains perhaps the most harshly affected class in the ongoing insurance 'hard market'. In addition to cost increases, most insureds are finding the information requirements and minimum IT security standards increasingly stringent when buying insurance cover. Where supported by a meaningful discussion of IT security, this is a very positive role that insurers can play to encourage risk management best practice.

However, many insureds complain that too often cyber requirements are not well-explained and can be inflexible in accommodating non-standard solutions and approaches, e.g. convincing insurers that whilst automated MFA can be adopted for most systems, occasionally circumstances and technical restrictions can make other workarounds necessary and, if properly implemented,

2. https://www.marsh.com/us/services/international-placement-services/insights/global_insurance_market_index.html

at least as effective. Insurers need to balance technical support and risk engineering objectives with flexibility around implementation for different client circumstances.

By far the most insidious effect of hard market conditions is neither price nor information, but narrowing coverage. Sometimes, this is obvious (such as reduced limits or outright unavailability of cyber business interruption cover for some sectors), but can take many forms: shortened "indemnity periods", multiple reduced sublimits, narrowing definitions of covered acts and/or systems, widened exclusions such as for legacy or 'in development' systems or software, co-insurance clauses for certain types of loss. All of this leaves the corporate paying more premium at the same time as retaining a far greater share of their financial risk.

Not only is this unwelcome, coming at a time of widespread cost increases and huge inflationary pressures, it compounds the increase in operational risks being retained by UK plc.

The compound effects of Brexit, the pandemic, the Russia-Ukraine conflict and widespread supply chain disruptions have drastically altered operational risks as companies respond, redesign and adapt their processes accordingly. As a result, they need adequate insurance and they need to invest in resilience across their business system; at the very time of highest necessity, this is exactly where forced cutbacks are being made as companies have to allocate a finite insurance budget to competing categories - where the world is now a riskier place.

25% do not trust their cyber insurance to pay out in case of a cyber attack

What steps should you take?

Buying off the peg insurance products is rarely a good idea in any market. When that product is designed to protect against a rapidly evolving threat such as cyber, the need for careful consideration of what is required and what is on offer is even more crucial.

We have set out below the 4 steps we consider to be key in obtaining cover that is cost effective and meets the needs of any company.

1. Evaluate in detail what your risk concerns are and what the effects would be on your business. Make a detailed list of the cover your company requires and critically assess what is less relevant to your business, so that money can be saved.

2. Seek out pragmatic, independent advice on the information you will need to provide to your insurer in order to place cyber cover. In doing so, you should be able to cut through standardised proposal forms and endless 'checkbox' questions.

3. Get specialist advice so policy wordings are adapted to your business needs and make sure such wording is explained to your IT and operational teams so they know what they need to do to maintain cover – avoiding the common flaws besetting many cyber insurance policies.

4. Start this process early and take control of the process of placing your risk in the market to maximise competition for your business and ensuring you get the right cover at a fair price.

Avoid Common cyber insurance pitfalls

Co-insurance
Cyber insurance is designed to limit the financial risk relating to any loss of information and disruption caused by activity disrupting IT systems or networks. Co-insurance clauses, however, can seriously limit your cover by requiring you to pay (in addition to the policy deductible) a proportion of all losses of a specific stated type, such as ransomware (where limiting cover to as little as 50% of your loss is increasingly common).

More demanding policy conditions
In addition to requiring more information to place than before the hard market, cyber policies are also more likely to include more demanding conditions which need to be reviewed carefully. Often these can deal with risk management subjects such as enabling Multi-Factor Authentication, software updates, device controls etc, in addition to technical matters such as notifying incidents rapidly (including before they are even known to have caused a loss). Whilst the objective of such conditions is often reasonable, it is important to review how flexibly they are framed and be wary of any alternative or 'non-standard' solutions your business may rely on. These may be equally or more effective at managing your risk but still constitute a breach of your policy that will undermine cover.

Limited cover for systems interruptions
Cover for systems interruptions can be subject to varying restrictions; it may be limited only to a subset of relevant IT systems (excluding external providers or systems in development), or only to loss of income rather than the wider costs of the interruption. It may only cover the period of interruption and not cover ongoing costs incurred after the IT system is restored. All of these mean that only a fraction of the costs arising from some interruptions may be covered and scenarios should be clarified up front.

War/Terrorism exclusions
These exclusions were introduced for the reasonable purpose of delineating more general Terrorism cover from that of cyber-specific insurance and limiting systemic exposures arising if part of a wider political conflict between states. However, given the potential for many cyber-attacks to be interpreted as acts of cyber terrorism, and an increasingly complex landscape of so-called "hybrid" warfare whose underlying perpetrators and intentions can be hard to establish, such exclusions can exclude a significant section of cover and put an unfair onus of proof on you to determine perpetrators' motives. Even where an exclusion carves back cover for Cyber Terrorism, it may still exclude 'hostile' or 'warlike activities' which, if interpreted broadly, still compromise cover. It is key to review these wordings and definitions very carefully if they are introduced to your cyber programme.

What to do next

Contact the Mactavish team

Email: mail@mactavishgroup.com **Tel: 0203 4796 875**

A member of our technical team will be delighted to talk you through any of the issues we have mentioned here or any other concerns you may have about your insurance programme.

If you'd like to find out more about our mission to create a fairer market for policyholders, visit **www.mactavishgroup.com**. In times of uncertainties and change, planning for the future and building resilient risk transfer is more important than ever.

Mactavish
Expert insurance buyers

Building corporate resilience.

22a St. James's Square London SW1Y 4JH | COMPANY NO. 4099451