Mactavish

MANUFACTURING CONFUSION:

THE DANGERS OF STANDARDISED POLICY WORDINGS

OFF-THE-PEG POLICIES WIDEN THE GULF BETWEEN CLIENT EXPECTATIONS AND INSURER DELIVERY

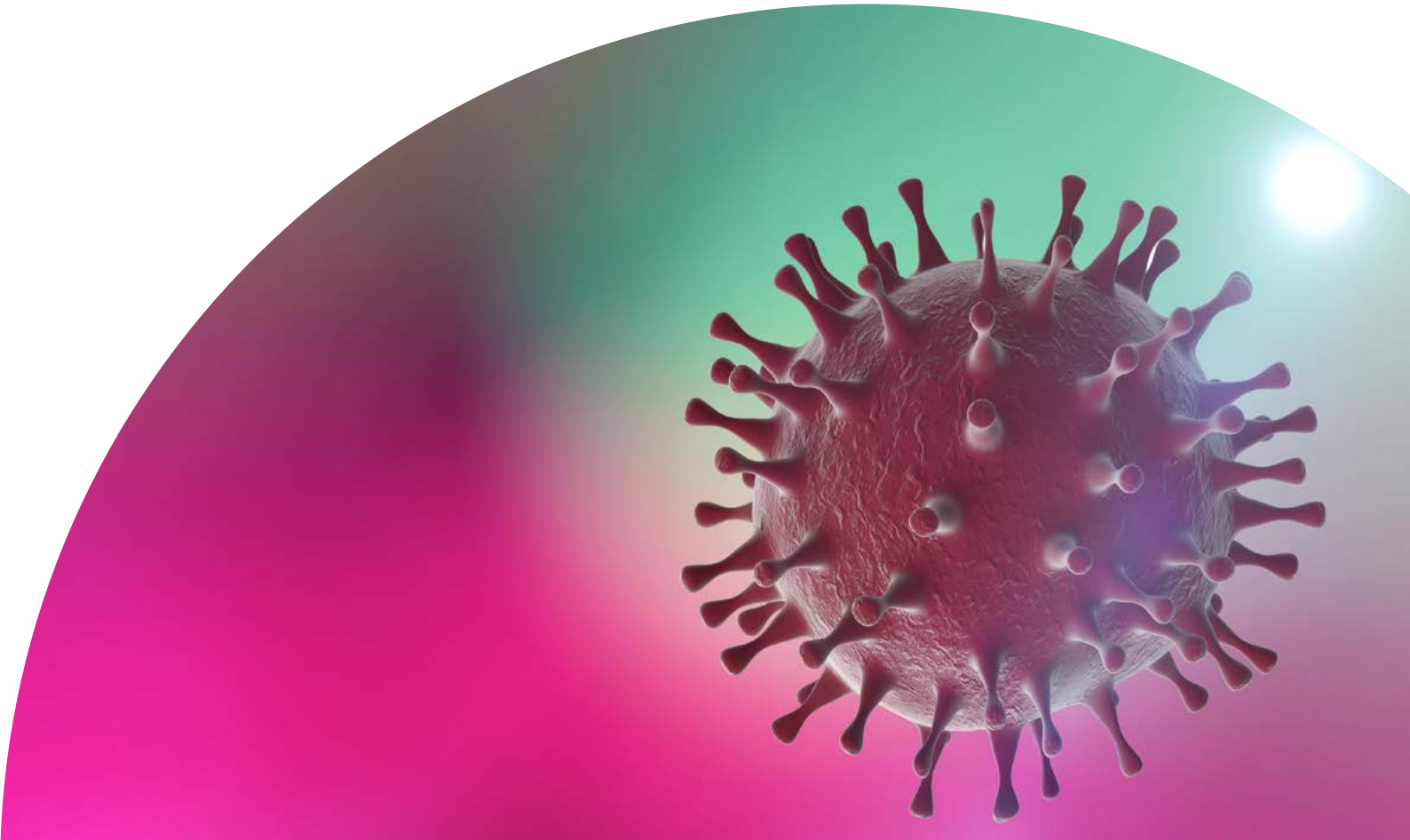
AT-A-GLANCE:

- The dispute between clients and insurers over Covid-19 claims highlights how the industry is failing business
- Insurers refusal to cover Covid-19 impacts – against the context of ambiguously-worded business interruption policies – echoes wider client experience across all complex insurance classes, notably cyber
- Clients without a legal or technical background now often have no chance of deciphering their own policies. This abuse of trust is a legal disgrace
- Brokers and insurers are increasingly offering inadequate one-size-fits-all policies, rather than bespoke wordings that meet clients' specific needs
- The side-lining of the technical skills base of both broking and underwriting means few in the industry now have the capability to understand over-complex policies or to adapt them to meet client needs
- When policyholders, brokers or underwriters do want to amend wording it is often impossible
- Covid-19, tighter governance and increasing business complexity are increasing the need for bespoke cover – just as standardisation is becoming the industry standard
- Buyers must lead the demand for change. The industry will not reform itself and the FCA will not insist on it
- Flawed policies lead to disputes between insurers and clients, a breakdown in trust, and the further commoditisation of insurance
- This negative cycle must be broken or, as rival centres gain ground, the London market` will decline

INTRODUCTION

The clash between insurers and clients over whether Covid-19 losses should be covered by business interruption policies is further tarnishing the industry's reputation.

In standing against stricken small businesses, as the rest of the nation unites against a common foe, leading insurers have at times, seemed little better than profiteers. The impact on client trust has been immediate. A McKinsey report suggests that 60% of small to medium-sized enterprises surveyed feel their insurers were not transparent over how Covid-19 would affect their policies. One-third say they are likely to stop buying business interruption cover.[1]



INADEQUATE POLICIES

The Covid-19 stand-off highlights a wider, more fundamental problem across the whole sector, most spectacularly with cyber insurance.

Clients are being widely let down by policies that are not fit for purpose. In an age of growing complexity, rather than crafting highly-bespoke wordings designed to meet clients' unique requirements, brokers and insurers are increasingly developing one-size-fits-all approaches. So that, with Covid-19, many companies find they are covered against the unlikely event of bubonic plague but not against emerging diseases, like coronavirus.

These generic policies are rolled out across vast distribution networks, and sold arbitrarily to clients, with little regard to their sector, size or individual characteristics. Such off-the-peg policies may cost less for brokers and insurers to produce but those savings do not translate into a more valuable product for policyholders.

The echoes between the Covid-19 stand-off and disputes around cyber insurance are striking. As with the Covid-19 cases, the complexity of many cyber business interruption policies means it is almost impossible to decipher whether they should or shouldn't pay out on claims – as we explored in our November 2018 publication, the Cyber Risk & Insurance Report.[2] Matters are particularly acute in the cyber arena due to rapidly-evolving risks and the immaturity of cyber insurance products. However, systemic limitations, badly drafted policies, and over-standardisation of widely-marketed policies mean similar problems – and the related mismatch between client expectations and reality – exist across all complex classes of business insurance.

LONG-HELD CONCERNS

We have been highlighting this issue for a decade, with our Cyber Risk & Insurance Report being just the latest expression of our long-held concern.

In 2011, a PwC/Mactavish report flagged up the problems arising from limited technical skills and insufficient adaptation of cover to meet client needs.[3] A few years later, our 2014 submission to the Law Commission[4], which was the largest source of evidence for the 2015 Insurance Act reforms, documented how insurers were "commoditising by default a standard, and by consequence inadequate, insurance product". In our increasingly complex and globalised world, even modest companies can have complicated risk profiles. Evolving business models, changing supplier relationships and burgeoning technology mean organisations want more bespoke insurance products not fewer.

CYBER POLICIES FAIL THE TEST

The global cyber insurance market is projected to be worth £15 billion by 2022. Its growth has been boosted by high profile data breaches and ransomware strikes and data protection regulation and fines, including that heralded by GDPR. The boost in home working and a significant increase in digital crime following the Covid-19 lockdown mean many more companies will be considering protecting themselves with specialist cyber insurances.

Our research shows that – like many Covid-19 claimants – significant numbers of Mactavish clients have found gaping, and costly, holes in their cyber policies.

Our Cyber Risk & Insurance Report and follow-up research revealed that:

- More than one-third (35%) of companies surveyed feel that available cyber insurance cover is unfit for purpose
- Eight common flaws afflict 93% of the policies reviewed
- On average, wordings have an average of 2.5 of these flaws
- The flaw of complex and onerous notification requirements has the highest prevalence – in 61% of all wordings

Counter-intuitively, standardisation does not necessarily lead to simpler and clearer policies. The average D&O policy – one of the shortest contracts – is more than 20 pages long and will involve numerous endorsements and exclusions, all written in very insurance-specific legalese. Such additions are themselves often standardised, meaning the client is left to decipher an over- and under-lapping set of documents – all of which may be inappropriate for the risks for which the policyholder is seeking protection, and commonly fail to dovetail as intended with other parts of the policy.

"If you want to ask lots of questions about how our wording works, maybe we're not the right insurer for you."

A leading cyber insurer to a FTSE 250 client at a 2019 meeting.

HOW COMMON POLICY FLAWS UNDERMINE REAL CLIENT COVER

Cyber: Leading UK pension fund

The company's principal cyber risk is a data security breach relating to pension scheme members, all of whom were excluded from key sections of its proposed cyber policy despite being the only significant source of personal data in the business.

Directors' and officers' (D&O) liability: Public sector body

The D&O insurer agreed with around 20 necessary policy clarifications but the underwriter was unable to amend its own wording, offering only a heavily-caveated and legally-inadmissible side letter on aspects of underwriting intention, which failed to satisfy client governance standards.

Professional indemnity (PI): International events business

The firm's broker placed the firm's PI policy into an existing, standard scheme for 'PI', which excluded 100% of the advisory activities actually undertaken by the company via broad exclusions for anything relating to its core business.

Property and casualty: Online travel business

The standard tour operator's policy structure only covers where the policyholder organises trips as a traditional tour operator. No adaptation could be made to reflect the different role of a modern online travel business so that the policy technically provided no cover at all.

A LEGAL DISGRACE

Faced with such complexity, even the most sophisticated buyers are out of their depth. As a result, they are wholly dependent on their broker; yet, as our recent research shows[5], brokers are unused to completing this type of analysis and their incentives are often allied with the insurer. This is a legal disgrace; exposing non-legal specialists to such a morass is unethical and abusive.

Standardisation is not inherently wrong; it is both an economic necessity and a potential way of spreading best practice. A standardised document can quite legitimately be the baseline policy that technically-skilled underwriters and brokers amend to reflect specific client needs. However, too often generic policies are not being adapted – partly due to a relative lack of sufficiently-skilled underwriters and brokers – leaving policy wording ambiguous and with significant gaps in coverage. This enables different inferences to be drawn as to whether a provider should or shouldn't pay out on claims – as seen with the Covid-19, and many other complex class claim, disputes.

Theoretically clients could, of course, point out policy flaws at the point of signing. In reality, as explored above, most clients – and the majority of brokers – could not understand the wording of their policies, and their multiple – and too often contradictory – endorsements, extensions, exclusions, definitions, conditions and 'side letters' if they tried. They are just too complicated. And if they were able to try, they would be among the lucky few; many companies do not receive their policy documents for many months after signing/renewal. Furthermore, our experience shows that when an individual policyholder, broker or underwriter does want to amend a wording they are often told it is not possible. This, in Financial Conduct Authority (FCA) parlance, is not treating customers fairly.

THE ROAD TO STANDARDISATION

The use of standardised policies has rocketed due to significant changes within the insurance industry in the past three decades.

Insurers themselves have been through an extended period of consolidation and were, pre-Covid-19, expected to continue on a similar trajectory. Brokers have also increased their M&A activity, leaving just a handful capable of handling global client programmes. As companies have merged, investment in technical resources (such as wordings experts) has been slashed, with few technically-skilled brokers now in situ.

The relationship between insurers and brokers has also evolved. Traditionally, brokers marketed policyholder risks to a broad range of underwriters and put forward the best offer to their clients. However, while clients might assume this approach endures, brokers are now more likely to place that risk with a pre-arranged panel of insurers, or a facility they have set up. More often than not, as Mactavish explores in its recent Broker Conflicts Report, alongside many other broker remuneration levies, insurers pay a facility management fee to the brokers that manage the panel. This charge is significant – often as high as 10% of the total premium. In return, the insurer – which has essentially outsourced its sales activity to the broker – gains access to a large volume of business.

Panels typically use standardised wordings that have been drafted or approved by the broker. This means there are fewer policies for clients to choose from, making it all the more important that wordings are adapted by technically-competent brokers. But such experts are now very thin on the ground.

"The Covid-19 stand-off highlights a wider, more fundamental problem within the sector: clients are being widely let down by policies that are not fit for purpose."

FACING THE TIPPING POINT

Covid-19 could be the tipping point for UK insurance's position as a global market leader.

The pandemic has transformed the risk landscape and the types of protection which businesses look to insurance to provide. Mass homeworking, facility mothballing, new services, and untested safety practices are just some lockdown facts of life that existing policies did not anticipate. Insurers must respond swiftly to the new environment. And, as the UK returns to work in the shadow of a major recession, the insurance industry will face further challenges. Unprecedented business uncertainty, a huge anticipated spike in claims – particularly in D&O, PI, PPL, and employers' liability insurance – and diminished insurer reserves could lead to massively reduced capacity across some classes and further erode the quality of available cover.

Coming in the wake of the major fracture in trust between the real economy and insurers around the Covid-19 dispute, these factors mean the industry can no longer expect to thrive on opaque, standardised polices that are unfit for purpose.

This was becoming clear even before the virus. The pace of technological change, increasing globalisation and connectivity, and the speed with which companies scale up mean that business risks are more complicated than ever. These risks – compounded by future virus shockwaves – just do not fit in generic boxes. And at a time when other sectors are delivering sophisticated bespoke products – from 3D-printed aeronautic parts to personalised pharmaceuticals – it is bizarre that the insurance industry is resolutely marching in the other direction.

"In our increasingly complex and globalised world, organisations want more bespoke insurance products not fewer."

DISADVANTAGED CLIENTS

Our research shows that clients of all sizes and industries have been disadvantaged by standardised complex class policies. In highlighting cyber insurance, with further evidence from PI, PDBI, and D&O, Mactavish is not targeting these lines in isolation nor criticising their products. Insurance as contingent capital is always a complex product, particularly for larger corporate clients. Nor are we failing to understand that standardisation is not in itself a 'bad thing'.

However, brokers and underwriters absolutely must adapt generic policies to the specific situations faced by their clients. That is a major component of the value of insurance and, from the evidence before us, this work is too often not being carried out. Risk needs to be carefully analysed and bought with care, with policies being duly negotiated to fit. Wherever the current insurance market model impedes that process, coverage 'flaws' will arise for any complex class.

The flaws identified in this report came from a broad range of policies sourced from some of the largest and most sophisticated risk buyers in the UK. If even companies with that level of purchasing power cannot push for the policy adaptations they need, there is a serious problem in the way the market functions.

"Exposing non-legal specialists to such a morass is unethical and abusive."

BUYERS MUST ACT

The extent of this ‘serious problem’ means buyers must act. They need to challenge the insurance industry for selling it products that not only do not meet their needs, but are sold in an incomprehensible and misleading way that would be unacceptable for any other complex financial product.

Only buyers have the muscle to achieve the necessary change in practices and products; the industry will not reform itself and – despite the extent of this legal disgrace – the regulator is unwilling to demand it. With recent corporate governance regulation meaning boards have a greater responsibility for managing risk, executive directors – rather than lower-level employees – now effectively oversee corporate insurance arrangements. Their louder voice and greater clout might finally get brokers and insurers to sit up and listen.

“Clients of all sizes and from all industries have been disadvantaged by standardised complex class policies.”

BREAKING THE NEGATIVE CYCLE

If the industry does listen to buyers and, rising to the challenge, crafts clear, bespoke policies that meet clients' precise needs, there could be great opportunities ahead. Companies could gain a greater sense of the value provided by brokers, specialist legal advisors and other professional services in the insurance eco-system.

Rather than being cost-focused vendors of an interchangeable commodity, they could be seen as technical and financial experts with highly valuable expertise. This, in turn, might allow them to wean themselves off the non-transparent insurer-derived income we discuss at length in our recent Broker Conflicts Report.

If brokers cannot rise to the challenge, it will be a long-term problem for us all. The London market does not have a divine right to business: the UK has already slipped from being the world's third-largest non-life insurance market in 2008 to the fifth, with Asia-Pacific set to account for 42% of global premiums within a decade.[6] The UK cannot compete on cost with rival emerging markets. It must, instead, provide a top quality product and contract: it is currently failing on this.

If things continue as they are, and more policyholders experience the shock of a denied claim for one of the very loss scenarios they bought cover for, trust in the industry and its practitioners will further decline. In turn, this will lead more end-clients to see insurance as a mere commodity – creating additional cost pressures and further reducing the level of resources the UK industry needs to work effectively. The extraordinary mismatch in expectations between policyholders and insurers over infectious disease cover in relation to Covid-19 – and its echoes across all complex class insurance – is a wake-up call to all those with an interest in the future of the UK's once world-leading insurance industry.

"The flaws identified in this paper came from a broad range of policies sourced from some of the largest and most sophisticated risk buyers in the UK."

APPENDIX I

CYBER INSURANCE: CLIENTS STRUGGLE WITH FLAWED POLICIES

Cyber insurance was only born 30 years ago, when early ecommerce companies sought protection against hackers. The relative immaturity of the market means it provides a largely untested product. However, despite the dynamism of the sector, insurers and brokers have adopted largely inflexible and imprecise models for cyber policies and extensions. These are proving inadequate in responding to the rate of risk evolution and the variety of company models.

Our Cyber Risk & Insurance Report[7] highlights eight significant common 'flaws' in dozens of standalone cyber policy wordings that were either in place or being negotiated with medium-to-large sized companies, including a significant proportion of the FTSE 100 and 250. These eight flaws – drawn from a much larger pool of limitations/ambiguities that we routinely encounter within cyber wordings – range from excluding cover for loss following accidental error or omissions, meaning clients are only covered for events initiated by attacks or unauthorised activity, to curbs on cover for data breaches, leaving clients merely protected for expenses they are legally obliged to incur, rather than the far greater costs incurred in practice.

As discussed further below (see Industry dialogue box), our analysis excluded outright any flaws that had been discussed with the client. That is, the identified flaws were a bolt from the blue. Neither the broker nor insurer had brought them to the client's attention, and the client had not said they were happy to exclude them from the policy.

	COMMON FLAWS IN CYBER POLICIES	PERCENTAGE OF POLICIES WHERE THE FLAW APPLIES
1	Cover can be limited to events triggered by attacks or unauthorised activity – excluding cover for losses caused by accidental errors or omissions	25%
2	Data breach costs can be limited – for example, only covering costs that the business is legally required to incur (as opposed to the much greater costs incurred in practice)	25%
3	Systems interruption cover can be limited to the brief period of actual network interruption, providing no protection for the more significant knock-on revenue impact after IT systems are restored but the business is still disrupted	18%
4	Cover for systems delivered by outsourced service providers (many businesses' most significant exposure) varies significantly and is often limited or excluded	46%
5	Exclusions for software in development or systems being rolled out are common and can be unclear or, in the worst cases, exclude events relating to recently updated systems	18%
6	Where contractors cause issues, such as a data breach, for which the business is legally responsible, policies will sometimes not respond	18%
7	Notification requirements are often complex and onerous	61%
8	Businesses can often not choose their own IT, PR or legal specialists during a cyber incident, as the policy only covers insurer-appointed advisors.	36%

THE CORE OF THE MARKET

We took care to ensure our research sample was representative of UK business and the core cyber insurance arena. The wordings assessed came from insurers and brokers in the specialist end of the market, servicing larger, more complex risks. The surveyed companies and policies represent a broad range of sectors, from telecoms to construction, with insurance limits ranging from £1m to £100m. Around one-third are in the FTSE 100, a similar number are in the FTSE 250, and the remainder are private businesses with turnovers between £20m and £2bn.

The breadth of the sample shows clients are being let down across the entire cyber insurance market, not just in isolated pockets.

MANAGING UNUSUAL RISKS

Organisations with unusual risks or exposures find cyber policy flaws create particular problems. For example, the extent and type of business interruption cover is often found to be inappropriate once a company's most likely loss scenarios are explored, while cover focused on personal data breaches can be insufficient for organisations with a wider set of commercial concerns around data security. In such cases – as in many others – off-the-shelf cyber cover is not fit for purpose. Digital exposures are complex, varied and evolving, thus cyber insurance is inevitably a complex product. Bespoke cover is often essential.

Even where bespoke cover is provided it is often fatally undermined by the lack of technical wordings skills in the industry. For example, a FTSE 250 had been purchasing bespoke cyber cover for several years to cover a very specific risk agreed with insurers. Specialist cover had been written in, but all other standard policy definitions and exclusions had not been amended, so, as both the broker and insurer had to subsequently admit, the bespoke policy was not in fact providing any of the cover that was intended.

INDUSTRY DIALOGUE

Our 2018 Cyber Risk & Insurance Report was attacked by some industry members, with the Director General of the Association of British Insurers (ABI) arguing we had "fundamentally misinterpreted" the sector.

We fully understand this sector and contend that, rather than exaggerating the problems in the cyber insurance sector as claimed, the flaws we highlighted are the tip of the iceberg. To illustrate this point, this report provides more cyber evidence and extends and updates previous data.

Below we expand on areas queried by our critics:

- It was suggested that our findings were skewed because we were looking at cyber add-ons, rather than standalone policies, and at old policies rather than current ones. In reality, our analysis was based entirely on pure cyber policies now in use. In all respects, the report was driven by current data not subjective opinion.
- It was argued the flaws we identified are irrelevant because they could be fixed by an add-on or extension. However, our analysis explicitly excludes flaws that were discussed with the client and for which supplementary cover was suggested. Where clients knowingly decided not to purchase such additional cover, we did not record a flaw.

Most flaws are actually rooted in the detail of the policy wording – not whether an add-on has or has not been purchased.

- Some commentators said the common provision of provider helplines invalidated the flaw of onerous notification requirements. However, compulsory notification via helplines, within unrealistic timeframes alongside strict requirements to notify insurers in writing, is part of the problem. Helplines cease to be useful if they conflict with the policy or create a legal obligation which the client – preoccupied with managing an unexpected workplace disaster – is likely to breach, giving an insurer the option to reject a claim.

Parts of the industry were not only mistaken in suggesting that our data was unreliable, they missed the real point of our findings: that systemic limitations and a lack of will and capability to adapt policy wordings to meet buyer needs was failing clients across all insurance classes.

"Clients are being let down across the entire cyber insurance market, not just in isolated pockets."

2020 UPDATE

In response to industry requests for more evidence, we have updated our cyber analysis to include more recent wordings. We also provide more detail on the frequency with which the flaws occur and examples of how they apply in practice.

In addition, we revisited our 2018 cyber research to assess industry progress, identifying positive movement in some areas. We found fewer incidences of legally required notifications only cover (flaw 2), network interruption period only cover (flaw 3), exclusions for software in development (flaw 5), and policies structured to respond only where the company itself causes an issue (flaw 6).

However, despite such advances, there was no radical improvement. We continued to see wordings in place, or being proposed to companies, with these flaws in 2020. And additional cyber hurdles keep cropping up. One current example, which we brought to public attention in February 2020, follows a Lloyd's of London 'silent cyber' mandate that insurers be explicit about the extent of digital cover in their general policies. While this aim was positive, it has had the unintended consequence of many providers removing swathes of cover for even loosely technology-related losses – much of which would traditionally be covered under property policies – from their wordings. Use of broad, standardised, exclusions has left many clients missing cover from other classes which cannot be bought from the cyber market either, with many unaware of the change.[8]

HOW COMMON FLAWS UNDERMINE CYBER COVER

Numerous Mactavish clients have found the cyber insurance they bought through major or specialist brokers from leading UK insurers does not protect them as intended. Here are a few examples:

- **Private company, left uninsured for operational errors due to broker and insurer error**
  The company's principal cyber risk is a data security breach relating to pension scheme members, all of whom were excluded from key sections of the proposed cyber policy despite being the only significant source of personal data in the business.
- **Leading UK pension fund, left uninsured for data relating to all current or past employees**
  The company's principal cyber risk is a data security breach relating to pension scheme members, all of whom were excluded from key sections of the proposed cyber policy despite being the only significant source of personal data in the business.
- **FTSE 100 business, left uncovered for systems interruptions caused by operational errors**
  The business has significant systems interruption exposure, but its cyber policy only provided cover for interruptions caused by unauthorised activity or malicious attacks – not for those caused by operational errors. The client flagged up this omission but was simply told the cover was of the highest standard.
- **FTSE 250 company, broker recommended cover with substantial flaws**
  The company was buying a cyber policy for the first time. The broker proposed a wording from a leading cyber insurer which included several of the most common flaws: systems interruption cover only applied to live programmes (systems in development or being rolled out/tested were excluded); the network definition excluded outsourced service provider systems' interruption cover; and the company had to notify claims "immediately" staff became aware of them – an onerous standard they were likely to breach.

"Despite the dynamism of the sector, insurers and brokers have adopted largely inflexible and imprecise models for cyber policies and extensions."

APPENDIX II

OTHER COMPLEX CLASSES: CLIENTS FACE GENERIC POLICY CHALLENGES

Complex clients, both large and SMEs, across all lines are suffering from policy flaws and claims disputes. Complex cases are, by definition, not straightforward. Clients may face significantly different risks, even within the same sector, as operational and management decisions and the quality of risk management activity affects the level and type of exposure.

This is where fuller risk analysis and better disclosure demand bespoke policy wording requirements – to clarify exactly what is covered by insurance, as opposed to waiting and seeing once a large claim occurs.

As with the cyber 'flaws' above, we do not provide a long checklist for each class but a small selection of common examples where inability to adapt coverage to risk detail causes problems. In our experience, any real-life wording review and negotiation exercise raises more than 50 problem areas which need to be amended and negotiated for each client.

DIRECTORS' AND OFFICERS' LIABILITY (D&O) INSURANCE

Common D&O 'flaws' – or incidences of coverage uncertainty or mismatch – experienced recently by Mactavish clients include:

Professional indemnity (PI) exclusions:
PI exclusions were introduced for the reasonable purpose of delineating D&O cover from that of PI. However, the blanket use of some broadly-worded exclusions leaves D&O cover essentially worthless for professional services sector clients.

Environmental exclusions:
These exclusions also had a sound objective – delineating D&O cover from environmental impairment liability (EIL) cover. However, broadly-worded exclusions for some clients (such as those responsible for buying or managing land) exclude consequential claims against directors for failures in supervision or management – areas that an EIL policy would also rule out.

Conduct exclusions:
Standard wording aims quite fairly to avoid underwriting deliberate fraudulent or criminal activity. However, many wordings inadvertently go further to exclude cover for an innocent party who has gained indirectly as a result of third-party dishonesty. This would be particularly problematic for certain financial services firms where the scope for indirect gain by directors may be more complex.

HOW COMMON FLAWS UNDERMINE D&O POLICIES

Standardisation problems on recent Mactavish D&O client placements include:

- **Public sector body**
  The D&O insurer agreed with around 20 necessary policy clarifications but the underwriter was unable to amend its own wording, offering only a heavily-caveated and legally-inadmissible side letter on aspects of underwriting intention, which failed to satisfy client governance standards.whom were excluded from the cyber policy despite being the only significant source of personal data in the business.

- **FTSE 250**
  The broker proposed switching to its own new D&O wording but refused the client's request to provide analysis of cover detail against the expiring policy, on the basis that this analysis was the broker's intellectual property.

- **Large investment group**
  The broker proposed moving PI, Crime and D&O policies to its own 'best in class' scheme wordings without accommodating more than 30 key amendments negotiated against the previous insurer's wordings. The broker's view was that the scheme had been negotiated with insurers at a portfolio level and no changes were possible for an individual client, even where standard terms technically excluded swathes of cover the insurer did in fact intend to insure.

PROFESSIONAL INDEMNITY (PI) INSURANCE

Common PI 'flaws' – or incidences of coverage uncertainty or mismatch – experienced recently by Mactavish clients include:

Narrow standard definitions of 'professional activities':
These inadvertently restrict cover for complex services businesses with a mix of technical and advisory work delivered in diverse sectors by employees with traditional and non-traditional qualifications.

Contractual liability exclusions:
These aim to prevent automatic cover for non-tortious liability arising through unusual contracting arrangements, or atypical liquidated damages, unless by underwriter agreement. However, problems arise when clients disclose such details but cannot amend the wording, or in sectors where all liability arises by virtue of a contract. In these circumstances some current wordings provide almost no cover.

Interface between PI and product liability:
Standard policy wordings can create gaps or overlaps for clients that buy both PI and PL. This is particularly the case in sectors where 'advice' is bundled, incidental and/or delivered through non-traditional channels. In one recent case, this would have led to neither policy responding to several critical loss scenarios.

HOW COMMON FLAWS UNDERMINE PI POLICIES

Standardisation problems on recent Mactavish PI client placements include:

- **High-growth international catering and events business**
  Broker placed the firm's PI policy into an existing, standard scheme for 'PI', which excluded 100% of the advisory activities actually undertaken by the company via broad exclusions.

- **Professional services Covid-19 exclusions PI**
  Standard, broad exclusions introduced just before many 2020 PI renewals (covering anything directly or indirectly related to Covid-19) effectively exclude cover for most ongoing 2020 advisory work, given the scale of the current economic crisis.

PROPERTY DAMAGE AND BUSINESS INTERRUPTION (PDBI) INSURANCE

Common PDBI 'flaws' – or incidences of coverage uncertainty or mismatch – experienced recently by Mactavish clients include:

Unclear delineation of what is covered under BI:
A high degree of uncertainty remains in many PDBI wordings on what type of costs are insured following property damage. Areas where specific client expectations should be agreed in advance might include uneconomic short-term workarounds (such as freight costs for low-value goods), customer compensation to retain long-term business, the level of cover for supply chain penalties, and the scope to reinstate damaged property on a non-'like for like' basis.

Broadly-formulated exclusions implemented inconsistently by insurers:
Some PDBI policies contain broad standard introductions excluding anything "caused by/contributing to or consisting of" numerous matters. Given the breadth of issues commonly covered in such exclusions, and the use of vague terms such as 'operational errors' or 'wear and tear', this leaves wide scope for insurers to argue a different interpretation of exclusion – or to suggest one thing when selling the policy and another when disputing a claim.

Concurrent or subsequent causes:
Many policies are unclear or punitive in the event of multiple causes of loss; with one event (such as wind damage to a supplier site) being insured while another (such as 'wide area' damage to a port) is not. This can lead to the unexpected exclusion of a loss which seemingly fitted within the policy cover. The policy position should be clarified for key scenarios in advance.

PRODUCT AND PUBLIC LIABILITY (PPL) INSURANCE

Common PPL 'flaws' – or incidences of coverage uncertainty or mismatch – experienced recently by Mactavish clients include:

Unclear definition of 'product':
Some policies are unclear as to what phases or activities relating to a product are insured as product liability. For example, does a particular policy cover damage to third parties during the transport of the product – or should this be covered by a separate policy?

Unclear basis of cover for injury/damage:
If a company is not sued directly, but via a retailer or intermediary following damage/injury, it can be unclear whether the policy should respond. The debate centres on whether the liability is for the damage/injury, or if it is a financial liability to the retailer/intermediary. While most industry commentators and clients would assume the former, the latter was asserted in a recent dispute. This new position would fundamentally undermine insurance cover for any business that provides products or services to end-customers via intermediaries.

Unclear cover limitations to 'accidental' events only:
It is a fair and common principle in insurance that deliberate acts cannot be insured: from an owner torching a factory to the publication of a known libellous untruth. However, many PPL wordings are not clear if this means losses caused by certain 'deliberate' acts – such as that of a rogue junior employee or JV partner – are excluded, or if the exclusion is limited more reasonably to acts by the insured's 'controlling mind'.

HOW COMMON FLAWS UNDERMINE PROPERTY AND CASUALTY COVER

Standardisation problems on recent Mactavish client placements include:

- **Public sector body**
  A property and casualty insurer argued that no changes to its standard 'sector-leading' wording were feasible. Instead it proposed further changes to a patchwork of around 50 endorsements, where there were many points of unresolved conflict, leaving the whole basis of cover unclear for many key client risks.
- **Speciality manufacturing business**
  Standard liability policy contained all the 'normal' exclusions for offshore/airside cover, despite such applications making up 60% of the client's business. When queried, the broker argued that the exclusions would not be applied in the event of loss but could not be amended.
- **Online travel business**
  Standard tour operator's policy structure covers only where the policyholder organises trips as a traditional tour operator. No adaptation could be made to reflect the more limited role of a modern online travel business so that the policy technically provided no cover at all.
- **Retail business**
  The company purchased an excess liability policy to cover claims relating to higher risk products, but the standard excess policy wording excluded all liability for the type of products concerned as it had not been scrutinised or amended by the broker. The policy was therefore worthless.

"If a company is not sued directly, but via a retailer or intermediary following damage/injury, it can be unclear whether the policy should respond."

"A high degree of uncertainty remains in many wordings on what type of costs are insured following property damage."

REFERENCES

1 'UK companies to shun business interruption insurance', Financial Times, May 4 2020; www.ft.com/content/ba7b8321-73a0-442d-ac85-74ad09019223

2 'Cyber Risk & Insurance Report, Mactavish, November 2018, www.mactavishgroup.com/wp-content/uploads/2018/11/Mactavish-Cyber-Risk-Insurance-Report-November-2018.pdf

3 'Corporate Risk & Insurance: The Case for Placement Reform, Mactavish, 2011

4 'Mactavish evidence to Law Commission & HM Treasury on insurance contract law; business disclosure; warranties; insurers remedies for fraudulent claims; and late payment, Mactavish Group, July 2014; www.mactavishgroup.com/insights/mactavish-evidence-to-law-commission-hm-treasury-enquiries

5 'Broker Conflicts Report, Mactavish, May 2020; https://www.mactavishgroup.com/insights/broker-conflict-report

6 World Insurance: the great pivot east continues, Swiss Re Institute, July 2019; www.swissre.com/institute/research/sigma-research/sigma-2019-03.html

7 Cyber Risk & Insurance Report, Mactavish, November 2018, www.mactavishgroup.com/wp-content/uploads/2018/11/Mactavish-Cyber-Risk-Insurance-Report-November-2018.pdf

8 'Firms forced to pay extra for cyber cover after insurer policy change', The Telegraph, 10 February 2020; www.telegraph.co.uk/business/2020/02/07/businesses-forced-pay-extra-cyber-cover-insurers-accused-gaming/

Mactavish

To find out more, please contact:

Telephone: +44 (0)207 993 0662
Email: mail@mactavishgroup.com

www.mactavishgroup.com