

Cyber Insurance Potential Buyers Should Act With Care Over The Mid-Term

*The Lack of Skills and Reliable Data are still Key
Market Constraints*

Cyber Insurance : At face value, a good measure for most companies to have in place

- Data is ubiquitous; mobility is becoming an integral part of social and workforce expectations
- Data breaches are hard to avoid
- Scale of impact is hard to predict given media, political and regulatory interest on these matters

But Cyber Insurance has the potential to trigger a range of management reactions, and as such it needs to be handled with care

At one end of the scale, it can be a game changer by triggering adherence to cyber security good practices, so that premiums are not wasted and claims can be made successfully when necessary

At the other end, it can be seen just as an illusory “silver bullet” i.e. something that would make the cyber security problem vanish without “changing anything” to existing practices i.e. while continuing with weak security practices



Cyber Insurance and the Insurance Industry

So far, it seems that the Insurance Industry has been focusing on generic Cyber Insurance products aimed at smaller firms and the mass SME market

- Many larger firms have been self-insuring for years or decades on matters of operational risk and are seen as unlikely to change their approach
- They can afford specialised products from specialised insurance providers (priced on ad-hoc basis) if necessary

There is a vast amount of hype around Cyber Security and Cyber Insurance

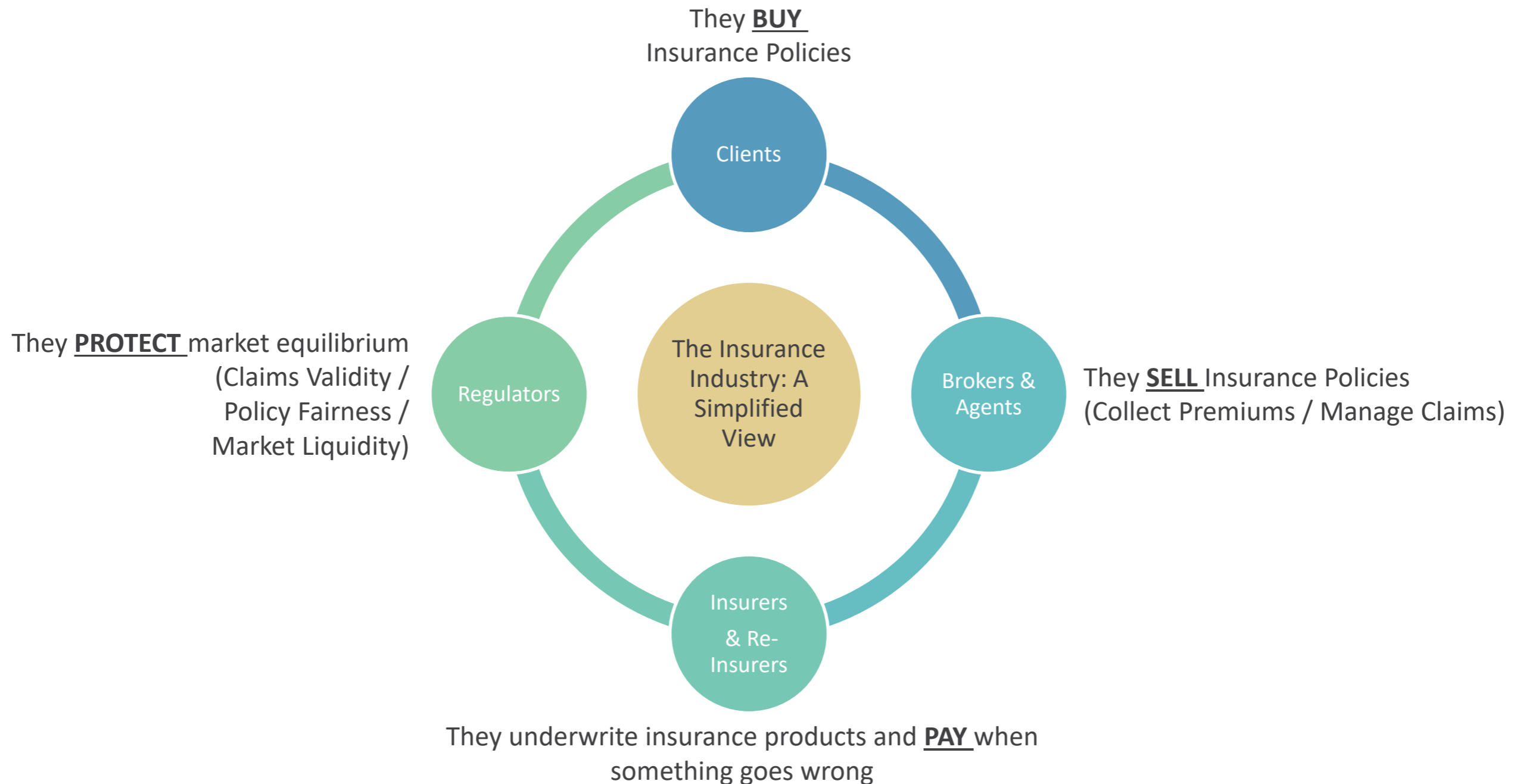
- Whipped up by a string of high profile incidents since 2014 (Sony, Target, Ashley Madison, TalkTalk etc...)
- And pushed by governmental bodies, such as the Cabinet Office in the UK (["UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk"](#) – March 2015 – in partnership with Marsh)

Many Insurance players are jumping on the band-wagon because they perceive the segment as a lucrative niche

- But in reality the Cyber Insurance market is still maturing
- And presents significant blockages which limit the value clients can get from products

The Insurance Industry Ecosystem

- A regulated industry with a variety of players



The Cyber Insurance Blockers

■ Insurers and Re-insurers (Underwriters)

Most are confused because traditional actuarial models cannot be applied. They have no choice over the short-term but to protect themselves through exclusions & favourable contract wording to avoid pushing premiums into un-sellable brackets

- Demonstrable adherence to cyber security good practices and standards is seen as essential and key in accepting applications (Source: [SANS/Advisen 2016 Cyber Insurance Survey](#) – June 2016)
- But, at the same time, threats morph very quickly and nobody can predict with any degree of reliability what attack vectors will be used for data breaches in 12-24-36 months
- The cyber problem is relatively recent (in the scale of issues covered by insurance policies) and, as a result, actuarial and modelling data related to breaches either does not exist, or does not exist in sufficient quantity, or cannot be trusted
 - Firms affected by data breaches do not necessarily report full reality (knowingly or not)
 - Threats can remain silent and breaches can stay undetected for long periods of time
- In addition, there are structural blockers preventing that situation from changing over the short-term (e.g. reputation protection) and the global economy is nowhere near a realistic reporting obligation (globally) that could be trusted
 - GDPR in the EU might have an impact but won't come into play until 2018
- Many re-insurers still do not re-insure Cyber Insurance products, and for those who do, it is still unclear how they may aggregate events (multi-events vs. single events), with too few cases to base decisions on, and significant industry sector differences can be expected.

The Cyber Insurance Blockers

■ Brokers & Agents

Many have jumped on the Cyber Insurance band-wagon attracted by the hype around the topic and the perception of a lucrative niche

- They sense the Cyber Insurance market for Small & Medium Firms could be significant and are rushing to position themselves while the niche is still young
- At the same time, it is becoming clearer and clearer that their potential clients in that space are at low levels of maturity in terms of security controls (evidenced by a non stop avalanche of data breaches and associated media coverage), and that cyber claims can be very diverse; in addition, many might be already covered by existing policies (or deemed so in the future by courts or regulators)
- Underwriters are hesitant due to the lack of reliable actuarial and modelling data: They insist on good cyber-hygiene before accepting applications but tend to push towards large exclusion lists and complex contract wording as threats morph quickly and they cannot know what a breach will be like in 12-24-36 months. They are perceived as having inconsistent and fast changing criteria for accepting applications, which creates frustration with Brokers and Agents (Source: [SANS/Advisen 2016 Cyber Insurance Survey](#) – June 2016)
- Brokers and Agents themselves lack key specialist field expertise around cyber threats and the controls required to ensure adequate cyber protection, that would avoid them being misled by their potential clients
- Many products are turning into value-added “data breach / incident response managed services” more than proper insurance products (i.e. services putting clients in contact with PR, legal experts etc... in the event of a data breach)
- This could be in response to Client’s demands but also a way of protection against mis-selling concerns otherwise related to abusive exclusions or abusive policy duplications (e.g. selling cyber insurance for something so restricted that courts or regulators could rule in the future that nobody could claim or that the risk was covered in standard Professional Indemnity policies ; a situation the industry encountered in the past around PPI in the UK)

The Cyber Insurance Blockers

■ Regulators

They are in a conflicting situation which limits their ability to act decisively

- They recognise that the current market dynamics create the potential for mis-selling
- But are also concerned about a potential mis-appreciation of the systemic risk (e.g. a cyber breach at a major provider leading to large numbers of valid claims and requiring more liquidity than what the market can offer at the time) in absence of valid actuarial data
- This does not create the right context for decisive action as the 2 risk aspects are obviously dynamically opposed (i.e if cyber insurance policies have been largely mis-sold then clients will not be able to claim irrespective of the type of event that happens)
- They seem to lack key specialist field expertise around cyber threats and the controls required to ensure adequate cyber protection, that would avoid them being misled by other players
- Rating Agencies could play a part but are rarely mentioned
- In the meantime, the evolution in the market is likely to be driven by court cases and precedents in particular in the US, but for now, there are too few of those to judge accurately the way it could go on a case by case basis (Source: [SANS/Advisen 2016 Cyber Insurance Survey](#) – June 2016)
- It has to be expected that the true enforceability of some policy exclusions and other contractual aspects will have to be tested in court and that the only form of market regulation around Cyber Insurance for the short to mid-term will come from the courts

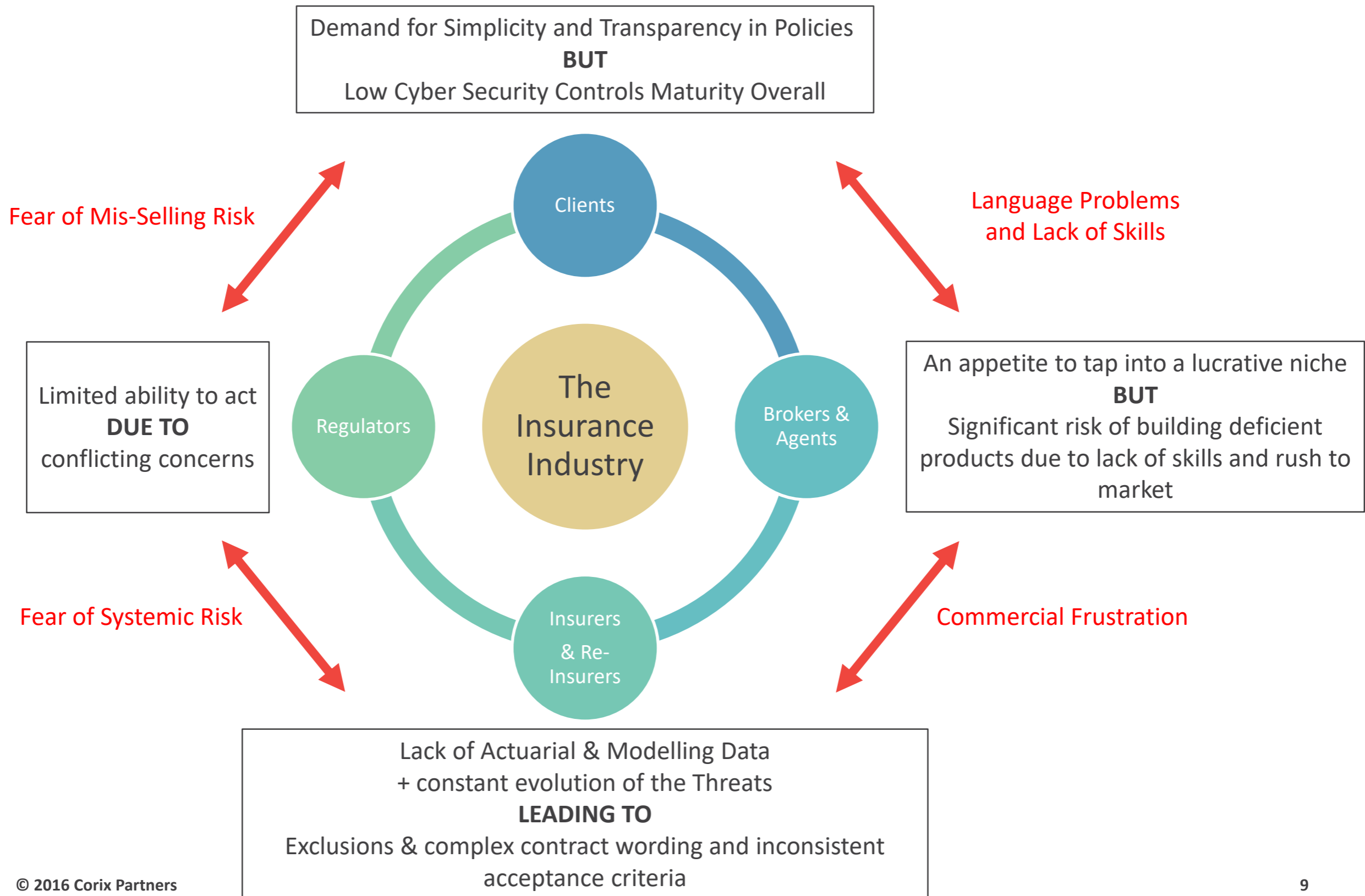
The Cyber Insurance Blockers


■ Clients

How many are engaged in a mature risk transfer approach, and how many are simply look for a “silver bullet” to make cyber security problems disappear without changing anything ?

- A mature risk transfer approach has to imply some understanding of threats and controls across the organisation which may be difficult and expensive to establish and maintain for small firms; many are not likely to have adequate expertise in that space
- Making the problem vanish without “changing anything” to existing practices (i.e. while continuing with weak security practices) obviously does not make any sense from a cyber insurance perspective i.e. common sense dictates that evidence of good practices being in place will always be required for applications to be accepted and for claims to be successfully processed (you can’t insure against regulatory fines)
- It is not likely that self-certification (e.g. UK Cyber Essentials scheme) will continue to be seen as a factor in the calculation of premiums, if & when it emerges that the appreciation of threats and controls by senior execs – in Small and Medium Firms in particular – is not necessarily as strong as it should be (in the end, the costs of those certification schemes – when offered as part of Cyber Insurance products – are simply factored into the premiums and push them up)
- For the short-term, cyber insurance products are likely to remain complex and contain numerous exclusions, and it is not realistic to expect an insurance policy to cover you 12-24-36 months down the line against threats that were not know at time of signing
- There is a considerable amount of language confusion between the parties and language inconsistencies between policies (Source: [SANS/Advisen 2016 Cyber Insurance Survey](#) – June 2016)
- There is also a risk for some products to be flawed as many Brokers and Agents might have simply jumped on the Cyber Insurance band-wagon without an adequate appreciation of the market dynamics and the technical aspects involved
- Generally, this goes against an ongoing customer demand for more policy simplicity and transparency in the market

The Cyber Insurance Dilemma





Mid Term View > An Immature and Slow-Evolving Market Constrained by Lack of Skills and Reliable Data, and Likely to be Driven by Court Cases

The Cyber Insurance market is not mature, market blockers are strong and they won't move over the short-to-medium term

- Lack of actuarial and modelling data due to constant threat evolution, as well as structural sharing and reliability issues
- Fundamental and generalised lack of specialised cyber security field expertise at key points in the market

Legal Precedents will drive the evolution of the market

- There are too few court cases at this stage to predict how litigation could go
- Legal precedents are in the process of being established on a case by case basis
- They are likely to be the only force driving a slow evolution and maturing of the Cyber Insurance market over the short to medium term
- Regulators are unlikely to act quickly to address this due to conflicting concerns

Conclusion and Recommendations

Potential buyers of Cyber Insurance products should act with care over the mid-term

- Paying full attention to the terms being offered, exclusion clauses and the level of coverage they may already have through existing policies
- The enforceability of exclusion clauses may have to be tested in court
- Value-added products should be seen as what they are and paid for through premiums, and not as insurance products

The lack of skills is a key constraint and all market players should invest in developing a specific expertise around cyber threats

- Working with specialised cyber security firms and academia to build dedicated cyber units staffed or supported by experts

Contact

For further information please contact:

Ben Churney

Business Development Manager

Sequel Business Solutions

+44 (0)20 7655 3021

bchurney@sequel.com

www.sequel.com

Jean-Christophe Gaillard

Managing Director

Corix Partners

+44 (0)7733 001 530

jcgaillard@corixpartners.com

Neil Cordell

Director

Corix Partners

+44 (0)7701 015 275

neilcordell@corixpartners.com

www.corixpartners.com

Many thanks to our focus
group members,
contributors & reviewers

Contributors

Robert Davies, Global-DTC

Nick Simms, Cornwood

Peter Wenham, Trusted Management

Reviewers

Ray Stanton

