# CYBER RISK INSURANCE – AN EFFECTIVE RISK MANAGEMENT TOOL FOR SMES IN THE UK?

***B. Soyer, * A. Nicholas** and G. Leloudas****

*This article aims to analyse to what extent small and medium sized businesses (SMEs) in the United Kingdom (England, Scotland, Wales and Northern Ireland) utilise cyber risk insurance as a risk mitigation tool in their cyber security management systems. To this end, the authors, by adopting a systematic qualitative analysis, elaborate the nature and scope of cyber risk insurance products on offer for SMEs (the supply side of the cyber insurance market). They then by utilising the data obtained from SMEs randomly but purposively, attempt to gain an understanding of the attitude of SMEs to cyber security generally and to cyber risk insurance. The main conclusion of the article is that the insurance market should consider developing a new cyber risk insurance product that aligns cyber security closely with the principle of indemnity. It is discussed in the article how such a product will enhance SMEs' cyber security resilience (hence providing a social benefit for the society) and at the same time afford new opportunities for insurance providers to expand the size of their business and variety of their products.*

# I. Introduction

Small and medium-sized enterprises (SMEs)[1] make up around 99% of all businesses operating in the United Kingdom (UK)[2] and are often regarded as the backbone of the economy.[3] With an increased reliance on digitalisation, data breaches and security incidents have been commonplace for all businesses; and to a large extent SMEs are more vulnerable to such perils, as they often lack the technical expertise, knowledge and resources to protect their data and business. In a cyber security context, although prevention is often the preferred option for risk managers,[4] there is no denying the fact that cyber risk insurance[5] could prove to be a valuable risk management tool for SMEs, given that it can provide the support they need to get back to business following a cyber breach and/or incident.

The main purpose of this paper is to evaluate how effectively cyber risk insurance is utilised by SMEs as a risk mitigation tool. Accordingly, we aim to focus on the debate from the perspective of providers of cyber risk insurance (risk carriers) and users of such products (SMEs). Therefore, by adopting a systematic qualitative analysis we shall elaborate what losses are normally covered by cyber insurance policies, what losses are excluded and what kind of

*** Professor of Commercial and Maritime Law, Director of Institute of International Shipping and Trade Law, Swansea University**
**** Research Officer, Cyber Risk Insurance- Building Resilience in Wales, Swansea University**
***** Professor of Law, Member of the Institute of International Shipping and Trade Law, Swansea University**
The authors are grateful to **Dr Alicia Mckenzie** and **Ms Nicole Dele-Alufe** (Research Assistants) on the project for data gathering. They are also grateful to **Professor Peter Raynor (Swansea University)** for his comments on an earlier draft of this article especially on methodological issues and two anonymous referees for their useful recommendations.
**The research which this paper is based on is funded by the Research Wales Innovation Fund.**

[1] There is no uniform definition of what constitutes a SME. For example, under the Companies Act 2016, a small company is defined as one that does not have a turnover of more than £6.5 million, a balance sheet of more than £3.26 million and more than 50 employees. A medium-sized company is defined as a business with fewer than 250 employees and a turnover of under £12.9 million. On the other hand, the European Commission defines a SME (2003/361/EC) as a business with less than 250 employees and either a turnover of up to EUR50 million or a balance sheet total up to EUR43 million. Within the SME category, a small enterprise is defined as an enterprise that employs fewer than 50 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR10 million. Similarly, a microenterprise is defined as an enterprise which employs fewer than 10 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR2 million.
The Department for Business, Energy & Industrial Strategy, on the other hand, focuses on the employee number and classifies businesses that have 0 to 49 employees as small and those with 50 to 249 employees as medium-sized. Given that we shall utilise data collated by the Department for Business, Energy & Industrial Strategy, for the purposes of this paper we shall adopt a similar approach.

[2] According to 2021 figures of the Department for Business, Energy & Industrial Strategy, UK had 5.5 million small businesses, 35,600 medium-sized businesses and only 7,700 large businesses. (See, https://www.gov.uk/government/statistics/business-population-estimates-2021/business-population-estimates-for-the-uk-and-regions-2021-statistical-release-html (last accessed on 1 March 2023)).

[3] SMEs account for 99.9% of the business population, in turn employing 16.3 million people, which translates into 61% of total employment. From a revenue perspective, SME's turnover was estimated at £2.3 trillion, which equates to over half (52%) of turnover in the private sector (See, https://www.fsb.org.uk/uk-small-business-statistics.html (last accessed on 1 March 2023)).

[4] L.A. Gordon et al, "A Framework for Using Insurance for Cyber-Risk Management" [2003] Communications of the ACM 81 at 84.

[5] Cyber risk insurance is a broad term used to describe insurance policies that offer indemnity for first and third-party losses resulting from a computer-based attack or malfunction of a firm's informational technology system.

risk control clauses are employed by cyber risk insurers to deal with the risk aggregation problem[6] and moral hazard issue[7] in cyber risk policies. It needs to be stressed at this juncture that the knowledge and experience of the authors of the insurance industry[8] and interviews conducted with those on the supply side of the market (i.e., insurers and insurance brokers) played a significant role in shaping our analysis.

Turning to the other side of the equation, by obtaining data from randomly, but purposively selected SMEs, we aim to acquire an appreciation of the degree of understanding SMEs have of this relatively new insurance product and to what extent they are currently utilising it as a risk mitigation tool. In instances where they are not utilising it, we aim to understand the reasons behind their decision and evaluate what kind of changes in the nature and scope of such insurance products might incentivise SMEs to consider their wider use.

Our research seeks to fill what we perceive to be a critical gap in the design, understanding and purchase of cyber risk insurance for SMEs by subjecting the supply and demand side of this new product to a critical analysis. We hope the outcomes of this study will inform: i) the cyber risk insurers as to how they can tailor their products to enhance their commercial appeal; ii) SMEs as to the need to purchase the right kind of cyber risk insurance product; and iii) policymakers by highlighting the need to provide better training to SMEs as to the role of cyber risk insurance as a risk mitigation tool. To this end, we shall first provide a description of relevant literature, followed by an explanation of our research methodology, data, and results of our content analysis and interactions with various SMEs.

## II. Literature Review

The existing literature almost exclusively focuses on the theoretical examination of asymmetric information, network externalities[9] and insurability of cyber risks in the market.[10] Particular emphasis is often placed in academic literature on information structures that create particular difficulties for cyber risk insurers and problems associated with the cyber insurance cover (i.e., adverse selection and moral hazard).[11] The former is a potential outcome of information imbalance in favour of the assured, and the latter is the risk of the assured taking less than optimal precautions against the insured risk after the attachment of the policy.

---

[6] Most cyber risks are systemic—that is, cascading adverse consequences might arise out of one or more casual events that affect or occur within a network (e.g., an error in a cloud computing service spreading among all users). See, J.E. Scheuermann, "Cyber Risks, Systemic Risks and Cyber Insurance" (2018) Penn State Law Review 613.

[7] Moral hazard is essentially the risk of the assured taking less than optimal precautions against an insured risk after the attachment of the risk. This particular behaviour is commonly referred to as "ex-ante" moral hazard. See, R. Avraham, "The Law and Economics of Insurance Law – A Primer" (2012) 19 Conn Insurance Law Journal 28, at 66.

[8] One of the authors to the article has professional working experience in the insurance sector over a decade.

[9] M. Eling & J. Wirfs, "What Are the Actual Costs of Cyber Risks Events" [2019] European Journal of Operational Research 1109. The issue is also considered by law and economics scholars who often deliberate on the extent to which current cyber insurance contracts contribute to social welfare: B de Waard et al, "The Law and Economics of Cyber Insurance Contracts: A Case Study" (2018) European Review of Private Law 371.

[10] See, for example, J.E. Scheuermann, "Cyber Risks, Systematic Risks and Cyber Insurance" (2018) Penn State Law Review 613. More recently, J.W. Welburn & A.M. Strong "Systemic Cyber Risk and Aggregate Impacts" (2021) Risk Analysis 1.

[11] L.M.D. Bailey "Mitigating Moral Hazard in Cyber-Risk Insurance" (2014) 3 Journal of Law & Cyber Warfare 1.

There is some qualitative research on cyber risk policies but these are restricted to analysing various insurance policies available[12] and examining self-assessment questionnaires provided to potential assureds by insurance companies.[13] Some researchers have also attempted to conduct theoretical modelling of a cyber insurance market by analysing the products offered by various insurers.[14]

Academic work has also been carried out evaluating the role of cyber risk insurance in enhancing cyber security and its benefit to society. For example, some researchers have found that it is hard to achieve a market equilibrium that improves network security without contract discrimination amongst users.[15] Another study concluded that cyber risk insurance is a high-security investment that could potentially have a positive impact on social welfare by making the internet safer for all users.[16] More recently, academic debate has focussed on whether the introduction of compulsory cyber risk insurance is a vital step in improving cyber security standards particularly with regard to SMEs[17] with some commentators arguing that cyber risk insurance should not be extended to cover ransom payments.[18]

To our knowledge, no academic study has been carried out to evaluate the scope of cyber risk insurance cover afforded to SMEs and the suitability of cyber cover on offer, especially in the UK context. Likewise, no study has considered the attitude of SMEs to cyber risks and their willingness to utilise cyber risk insurance as a mitigation tool. This study aims to fill this gap by not only considering the demand side of cyber risk insurance, but also studying the awareness of SMEs of cyber risk exposure and their attitude towards cyber risk products available in the market. We are of the opinion that this approach will provide a sound foundation in understanding how this novel insurance product can be developed and utilised in a more efficient manner to the benefit of SMEs, the insurance industry, and society as a whole.

## III. Research Methodology and Data Collection

In the following part (IV), we shall share the results of the thematic analysis that we have engaged, with a view to identify and categorise themes and concepts, and derive meaning and insights, across a collection of standard insurance policies used by insurers when underwriting cyber risk insurance for SMEs. We have obtained these policies from several insurance brokers independent of each other, so we are relatively confident that we secured access to a large

[12] W.S. Baer & A. Parkinson "Cyber Insurance in IT Security Management" (2007) 5 IEEE Security & Privacy 50. More recently, a very interesting work has been carried in the US by S. Romanosky et al, "Content Analysis of Cyber Insurance Policies: How Do Carriers Price Cyber Risk?" (2019) Journal of Cybersecurity 1.

[13] D. Woods et al, "Mapping the Coverage of Security Controls in Cyber Insurance Proposal Forms" (2017) 8 J Internet Services App 8.

[14] A. Matotta et al, "Cyber-Insurance Survey" (2017) Computer Science Review 35.

[15] R. Pal et al, "Will Cyber-Insurance Improve Network Security? A Market Analysis" Paper submitted to 104 IEEE Conference on Computer Communications.

[16] D. Kuru & S. Bayraktar, "The Effect of Cyber-Risk Insurance to Social Welfare" (2017) 24 Journal of Financial Crime 329.

[17] L. Miller, "Cyber Insurance: An Incentive Alignment Solution to Corporate Cyber-Insecurity" (2019) Journal of Law and Cyber Warfare.

[18] J.M. Lemnitzer, "Why Cybersecurity Insurance Should Be Regulated and Compulsory?" (2021) Journal of Cyber Policy 118 and A. Shortland, *Kidnap: Inside the Ransom Business* (2019, OUP).

amount of samples commonly used in the market.[19] Also, some large insurance companies make their standard coverage terms available online (such as Hiscox and Travelers); and we have, accordingly, obtained the text for such policies from the websites of these insurance providers.

In order to determine the appropriate number of cyber risk policies to examine, we employed a common form of qualitative non-probabilistic sampling known as "purposive sampling".[20] Sampling size in purposive sampling is determined by a concept called "thematic saturation", which is the point at which "no additional data are being found whereby the researcher can develop properties of the category—the point where no new concepts emerging".[21] We believe we reached that point after analysing 14 policies.

At the beginning of the coding process, a master codebook was created which recorded the following metadata for each docket: the relevant insurance company, the product name, the insurance line, coverage/exclusions, provisions dealing with moral hazard risk, and claim-related issues. Two teams composed of authors (and research assistants) of this article coded the coverage/exclusions, moral hazard, and claim-related issues. Each team developed their own codebook as they examined and processed their respective documents. The codebooks for each section were guided by an inductive approach that enabled investigators to identify themes and patterns within their respective documents. The authors followed common coding practices to first deductively anticipate initial coding variables, and then as each subsequent policy was examined, updated the codebook in order to capture unexpected findings. The themes were adjusted to create new and collapsing redundant themes, as needed. The ultimate data obtained was checked by all contributors at the end. We believe that the coding practice undertaken here was straightforward and less open to interpretation, as it was the direct result of whether a particular provision was present or not in the policy document. It needs to be stressed that we found the format of these policies to be standardised, and this assisted us immensely in the process of coding.

In Part V, you will find the results of the data collected from UK SMEs, with a primary view to determine the effectiveness of cyber risk insurance as a risk mitigation tool. As you will note, the study reveals other important, but relevant information, such as their understanding of coverage provided and significance of various contractual mechanisms employed by cyber insurers to protect themselves against the risk of moral hazard and ensure smooth running of the claims process. For this part, naturally a different research methodology has been employed, namely the method of probability (random) sampling.[22] When selecting our sample group, our purpose was to acquire an accurate representation of the current SME sector in the UK. To this end, we utilised statistics provided by the UK government on SMEs.[23]

---

[19] We estimate (based on our discussions with insurance brokers) there are 40 standard cyber risk policies in the UK market available to SMEs. For the purposes of this research, we have scrutinised 20 of the standard policies on offer. There are certainly more forms designed for specialised markets, such as marine, aviation and transport, but these are often not used and/or suitable for SME market, as such clauses are drafted on the assumption that that the turnover of the assured company is no less than US$1 billion and the assured corporation has appropriate corporate structures to deal with that volume of business.

[20] G. Guest et al, Applied Thematic Analysis, Sage Research Methods, (2014) (See http://antle.iat.sfu.ca/wp-content/uploads/Guest_2012_AppliedThematicAnlaysis_Ch1.pdf (last accessed on 1 March 2023)).

[21] A. Bryman, *Social Research Methods* (4th edn, OUP, 2012) 578–582.

[22] See ch 8 in A. Bryman, *ibid*, and ch 7 in E. Babbie, *The Practice of Social Research* (15th edn CenCage 2021).

[23] See, https://www.gov.uk/government/statistics/business-population-estimates-2021/business-population-estimates-for-the-uk-and-regions-2021-statistical-release-html (last accessed 1 March 2023).

In 2021, in terms of business density rates (numbers of SMEs per 10,000 resident adults) London had 1460, Wales 796, Scotland 752, Northern Ireland 825 and the rest of England (South West, South East, East of England, Yorkshire and the Humber, North West, North East, West Midlands, East Midlands) 974. So that our sample group appropriately represents all parts of the UK proportionately, we strived to gather samples at the following rate from different parts of the UK: 30.5% (London), 11.9% (Wales), 10.16% (Scotland), 9.32% (Northern Ireland) and 38.12 % (rest of England).[24]

The same statistics reveal that the main industries that these SMEs engaged in, in terms of turnover and employment, are the following: Construction, Professional/Scientific and Technical, Manufacturing, and Wholesale/Retail Trade and Repair (see the table below). Also, 98.2% of these businesses are small businesses (employing 1–49 employees) and 0.64% of them are medium-sized businesses employing (50–249 employees).

**Table 1**

**Main Industries in the UK**

| | **2021 – Turnover** | **2021 – Employment** |
|---|---|---|
| Construction | 11% | 11% |
| Professional, Scientific and Technical | 11% | 12% |
| Manufacturing | 9% | 9% |
| Wholesale and Retail Trade and Repair | 35% | 14% |

Again, in order to ensure that our sample group is appropriately representative, we required that at least 60.89% of it is made up from these sectors (Wholesale and Retail 33.4% of the surveys, Manufacturing 12.25%, Professional, Scientific and Technical 9.74%, and Construction 5.50%) and a big proportion of the data (98.8%) comes from small-sized businesses. It needs to be stated that in determining the list of targeted SMEs, we engaged in a consultation with several trade associations (such as the Federation of Small Businesses, SME Alliance and Superfast Business Wales)[25] and we made allowance for the fact that not all SMEs

[24] In total, 236 samples were collected from UK SMEs by the researchers (we have these in file for audit purposes). We noted no statistically significant difference in the responses from different parts of the UK. Thus, it can be suggested that there is no part of the UK where SMEs' attitude towards cyber risks and insurance is significantly different than other parts.

[25] The trade associations assisted us in identifying potential SMEs to approach and also informing and encouraging their members to respond to our survey.

contacted would have responded to our request for information.[26] The data were obtained from SMEs by our research assistants, who requested SMEs to complete a questionnaire prepared by the authors of this article. The coding analysis conducted on cyber policies in Part IV informed the preparation of this questionnaire. For example, when questioning the SMEs on the details of their cyber policies, we asked them questions to appreciate their level of understanding of the scope of cover provided by cyber risk policies, the use of insurance terms by insurers to mitigate moral hazard issues, and the effect of claims provisions on the prospect of recovery.[27] After sending the questionnaire to target SMEs, our research assistants made themselves available for any clarification that might be needed, and around 6% of those who responded to our questionnaire were assisted by our researchers in understanding the meaning and scope of the questions posed. It should be stressed that our researchers ensured that the relevant data were obtained from the person or department of each SME that has authority to make decisions concerning the purchase of insurance. To ensure that this is the case either the data were obtained from the relevant individual by email following a personal phone/skype call, or if the data were obtained by email, a phone/skype call was made later to check the credentials of the individual providing the information. The details of the data obtained from SMEs in line with the parameters set and explained in this part will be presented and discussed in Part V.

# IV. Cyber Risk Policies – Lessons Learned from Our Study in Relation to the Nature of the Cover Provided in the Market

## A) Cyber Insurance Market

The cyber insurance market has not adopted the approach of the marine, transport, energy and aviation insurance markets, which utilise a set of standard terms developed by insurers in consultation with market participants as the basis of cover.[28] Therefore, insurers tend to use their own standard terms to offer cyber risk insurance to SMEs.[29] However, our detailed examination of several cyber insurance policy wordings has revealed that the cover offered

[26] In fact, we failed to get responses from just above 200 SMEs contacted, for various reasons. Most SMEs declined to respond and indicated that they had no interest in the subject (about 27.5 % of those contacted). Some indicated that they had no time and/or resources to engage in the process (about 16.5 of those contacted) and a few of them were suspicious of our motives in collecting this data (around 1.9 % of those contacted).

[27] The nature and effect of such terms were described in detail in the questionnaire with samples provided. The aim here was to ensure that those engaging in completing the surveys were fully appreciative of the questions posed so that a more accurate response was obtained.

[28] For example, Institute Hull Clauses (1983/1995) and International Hull Clauses (2003) produced by the Joint Hull Committee often used as the basis of hull and machinery cover in London market (especially Lloyd's Market).

[29] The primary reason for this is the fact that cyber risk insurance is a relatively new product which is still in the process of development in the market. It is likely that we shall see standard terms developed in the future which are widely used by market participants. It should be noted that in the marine insurance market, it was not until 1779 that Lloyd's of London produced the first standardised marine insurance policy, commonly known as the SG (Ship and Goods) Policy, after almost three hundred years of underwriting marine risks.

against cyber insurers for SMEs in the UK insurance market is very similar, with few differences identified.

Our discussions with specialist cyber insurance brokers have also revealed that the following issues stand out with respect to the SME market for cyber risks. The uptake of cyber risk insurance is rather low. According to insurers, this is partly due to the average SME failing to meet the minimum criteria for obtaining cover. For example, in order to acquire cover, a cyber insurer might expect the potential assured to have adopted measures such as Multi Factor Authentication (MFA), to provide employee awareness training, and to have a stringent set of remote working controls. Further, it is quite common for SMEs to not fully appreciate the cyber risks they face, even where their business relies on the processing of data.[30] This shortcoming reflects a general lack of understanding of the potential costs resulting from a cyber breach and legal obligations should a data breach occur.

Insurers tend to approach the cover offered to SMEs differently from that offered to corporate businesses. With respect to the latter, the underwriting queries prior to placing the insurance are more stringent, with longer (and in some cases multiple) proposals in the case of larger corporations. Larger organisations are also generally subject to higher excesses and co-insurance clauses, particularly in respect of the risk of extortion. Their policies may also contain total exclusions more frequently than in the case of SME cover. Brokers also report that currently the London insurance market does not have much appetite for SME businesses. This opens the door for smaller (and niche) insurers to operate in the SME cyber insurance market. As a result, we see insurance cover being provided by a single insurer in the SME cyber insurance market rather than multiple insurers subscribing to the same risk, which is rather common in marine, transport, energy and aviation markets.[31]

### B) Coverage Provided by Cyber Risk Policies and Exclusions

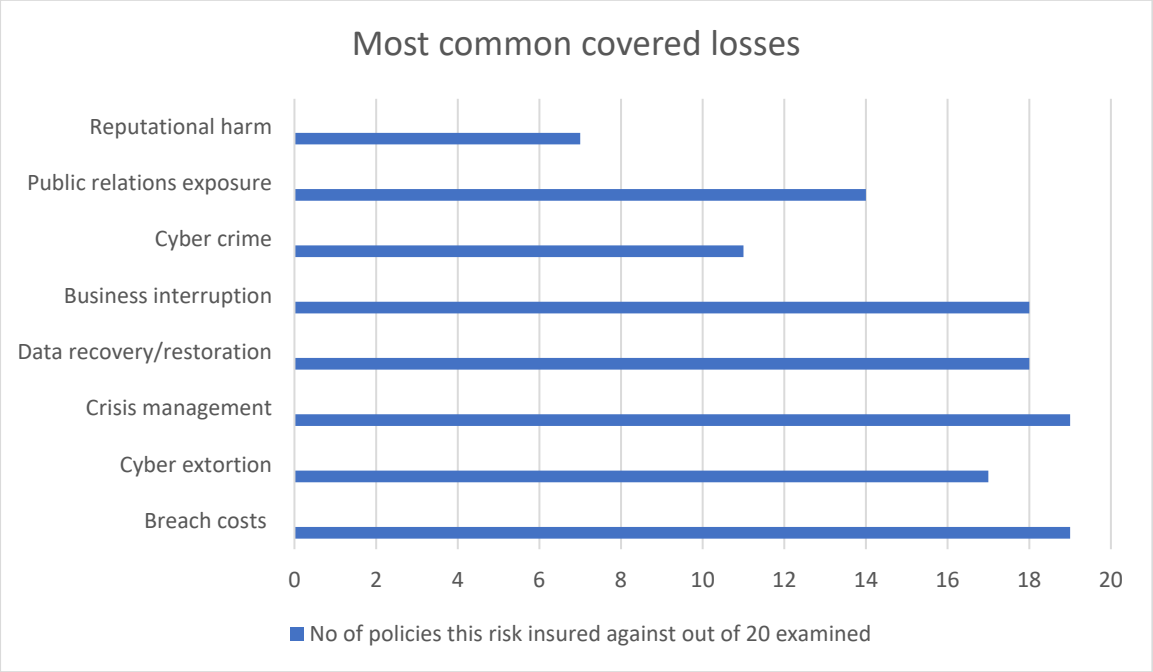
Our study found that the type of covered losses appeared more consistent across the policies examined. For example, after reviewing only 5 policies, 80% of the covered losses had been coded, and by the 14$^{th}$ policy we reached the saturation point, in the sense that we had identified all covered losses from the policies in our dataset. Although there is clearly a significant level of consistency across the policies on offer in the market, we also identified that insurance providers vary the degree of coverage significantly by setting financial limits for certain types of losses. For example, some policies limit the amount of recovery for certain types of losses (i.e., post breach remediation costs, crisis management costs, and data recovery/restoration costs). Similarly, in some policies we observed that cover for some kind of losses has been qualified. For instance, in some policies "data compromise response" is available only for specified expenses arising from a personal data compromise involving information that can identify individuals. Similarly, the peril "computer attack" provided coverage for specified

[30] In fact, our study (Part V) confirms that this is not only the perception of insurers, but most SMEs do not, in fact, appreciate the need to obtain cyber risk insurance.

[31] This, of course, has an adverse impact on risk distribution. We are not informed of the reinsurance arrangements of cyber risk insurers that operate in the SME market, but it is very likely that they would opt to distribute part of the risk through reinsurance.

expenses arising from an attack on the computer system. It needs to be stressed that all policies examined also identified an aggregate liability limit of indemnity and set a sublimit for some type of losses (e.g., for legal fees, crisis management, or incident response).

**Figure 1**




When it comes to cover for third-party liabilities, we found that the scope of cover is more restricted in the sense that cover was provided for only 14 types of potential liabilities that can arise. For insurance lawyers, this is hardly a surprising finding, since insurers are often hesitant in expanding the scope of cover for third-party liabilities concerned with risk aggregation. For example, in the attacks of 9/11 the third-party liabilities (claims from innocent bystanders and property users) that were incurred as a result of the crash of the two aircraft in the Twin Towers caused a long crisis in the aviation insurance market of London that resulted in withdrawal of third-party war risk insurance cover for several years; the crisis was only resolved by the provision of third-party war risk insurance cover for several years by governments.[32]

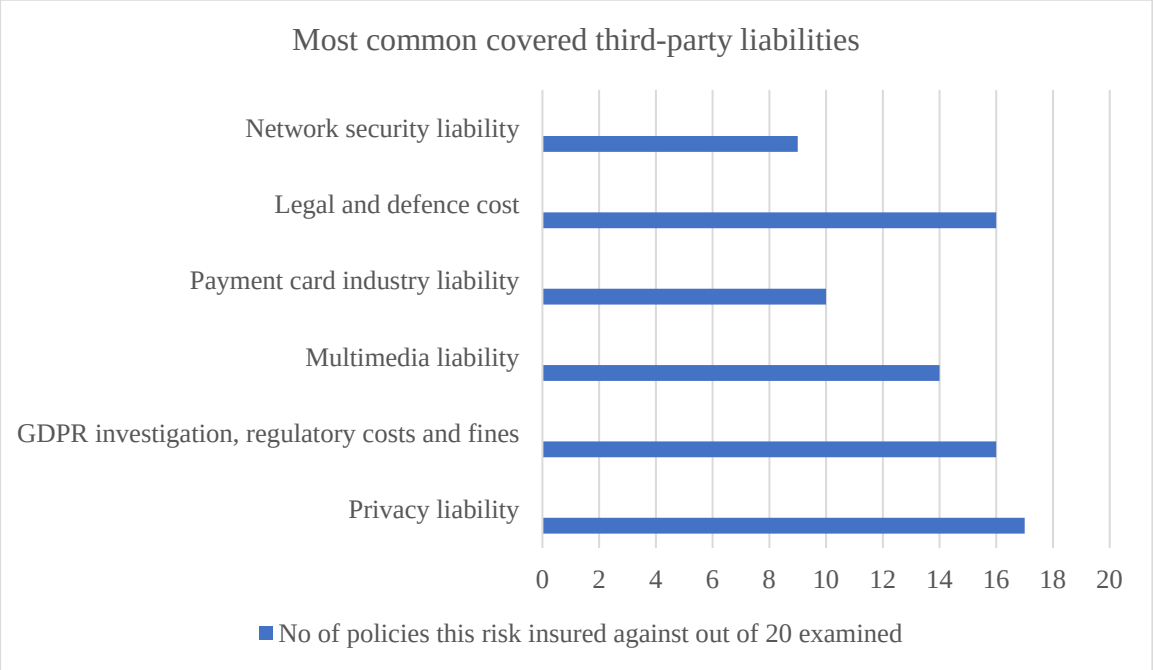
We also found that coverage for third-party liabilities is less consistent throughout the policies that formed our data set. For example, we identified that only two of the policies examined provided cover for director's liability[33] and only one provided cover for online

[32] K. Posner et al, *Margo on Aviation Insurance* (4th edn, LexisNexis 2014) para 19.07 – 19.31 and G. Leloudas et al, *Shawcross and Beaumont on Air Law* (Issue 183, LexisNexis 2022) Division IX, ch 46, [45].

[33] This essentially is designed to cover directors/senior executive officers for claims made against them as a result of a cyber event.

(media) liability. Interestingly, it was noted that most of the policies examined (90%) introduced significant qualifications to indemnity. For example, the peril "electronic media" provides coverage for defence and settlement costs only in the event that a third-party claimant sues the assured alleging that the assured's electronic communications resulted in defamation, violation of a person's right of privacy, interference with a person's right of publicity, or infringement of copyright or trademark. Also, it is worth noting that a sublimit has been set for third-party claims in 11 of the policies examined.

**Figure 2**[34]




Considering the exclusions from cover, a rather different picture emerges. We have particularly identified four points that need to be highlighted. First, the policies examined contained a significant number of exclusions: 76 to be precise (in total). As such, after

[34] In common law, the "*ex trupi causa*" principle prevents a legal action from being enforced by courts when it is founded on "immoral or illegal" conduct. This effectively means that it would be against public policy to allow a person to insure its criminal conduct. Courts have taken the view that the same applies to quasi-criminal conduct and in *Safeway Stores Ltd* v. *Twigger* [2011] EWCA Civ 1472; [2011] 1 Lloyd's Rep. 462, anti-competitive acts in breach of the Competition Act 1998 involved the necessary element of moral reprehensibility and were sufficiently serious to engage the illegality defence (see, also , *Les Laboratoires Servier* v *Apotex Inc & ors* [2014] UKSC 55; [2015] AC 430*).* The type of behaviour which may lead to penalties under the GDPR legislation are varied and they range from failure to maintain a record of processing activities to failure to comply with any of the key principles underpinning GDPR legislation. If the GDPR fine/penalty is imposed for an action of the company which is not deliberate or if the company has fallen victim to a nation state attack, it is plausible that such fine would be insurable and it is the intention of cyber risk policies to provide SMEs cover against this kind of GDPR fines and investigation costs.

analysing 5 policies we reached 56% saturation for exclusions and achieved full saturation by the 16th policy. Second, we came across exclusions that appeared only in a handful of policies examined: losses from unfavourable business conditions, losses emerging while working on travel, and losses emerging from the suspension of domain names. Third, we noted that the scope of some of the exclusion clauses that appear on cyber risk policies is so broad that to a certain extent they do undermine the cover offered to SMEs. For example, several policies contain a "social engineering" exclusion, which provides that:

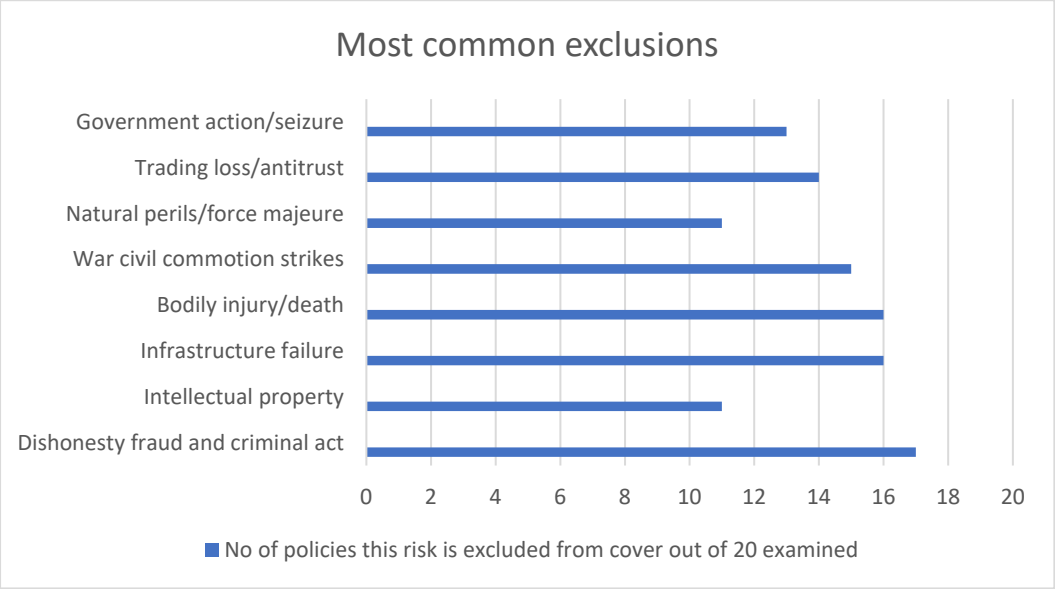
> The Insurer will not cover any claim or any loss under this policy resulting directly or indirectly from the input into or use of Electronic Data by anyone who has express or implied authority by the Insured to have access or to use or operate the Insured's network System, and/or being induced by any dishonest act to voluntarily part with title to or possession of any property and/or may cause any loss to the Insured.

It is submitted that this exclusion is wide enough to deny coverage when a loss arises as result of a spear phishing attack, namely one that leads an employee of the assured to open an email or attachment that contains a virus or malware or other software designed to steal passwords or damage the network system. Similarly, in a case where an employee of the assured becomes victim of a fraudulent email impersonating legitimate sources and gives out financial information or other details that causes a loss, such loss is likely to come under the scope of this exclusion. Also, the exclusion may be wide enough to apply in a case where a USB drive is deliberately contaminated by malicious third parties or hackers and deployed innocently by an employee to spread virus or malware or other damaging software into the network system. Another exclusion clause that dramatically restricts the scope of cyber cover provided is the one that excludes losses arising out of bodily injury or tangible property damage caused by a network security failure or breach. In a case when this exclusion is incorporated into the policy, it will ensure that there is no coverage for mental anguish, emotional distress, and shock due to the publication of private data as a result of a cyber breach.[35]

Lastly, some of the exclusions commonly observed were those not necessarily directly related to the cyber realm, but instead related to criminal, fraudulent, or dishonest acts, errors or omissions, intentional violation of law, any ongoing investigation or proceedings, and payment. We also found that several policies contained exclusions for infringement of patents, disclosure of trade secrets or confidential information or violation of securities laws. As an example, the effect of these clauses is that the loss caused by the passing of confidential information kept in digital records by an employee of the SME to a third party will not be covered by the cyber risk policy; this exclusion is understandable, as this loss is not caused by a cyber risk. Having said that, the loss will be covered if a third party unlawfully gains access to the digital network of the SME and steals or releases to the public confidential information.

[35] We noted that some policies offer to extend cover to such losses provided that additional premium is agreed.

**Figure 3**




## C) Risk Control Mechanisms Used in Cyber Policies

### i) Clauses Dealing with Moral Hazard

Moral hazard is a systemic risk faced by all insurers.[36] It is essentially the risk of the assured taking less than optimal precautions against an insured risk after the commencement of the policy. This particular behaviour is commonly referred to as "ex-ante" moral hazard, and insurance contracts invariably incorporate provisions in the form of warranties, conditions precedent[37] and exclusion clauses to deal with moral hazard issues. All policies we examined contained a provision requiring the assured SMEs to "take all reasonable steps" to maintain and update security software and hardware. A typical clause may provide that:

> The Insurer will not pay any claim or loss under this policy arising out of or relating directly or indirectly to any failure by the Insured to take all reasonable steps and precautions to prevent or reduce loss, damage or any claim, including to maintain, update and test all hardware and software programmes.

[36] R. Avraham, "The Law and Economics of Insurance Law – A Primer" (2012) 19 Conn Insurance law Journal 28, at 66.

[37] In case of breach of an insurance warranty the cover is suspended until the breach is remedied (s. 10 of the Insurance Act 2015). Breach of a condition precedent normally entitles the insurer to elect to discharge from the contract or prevent the assured from claiming for a particular loss depending on the wording adopted (see, *London Guarantee Co v Fearnley* (1880) 5 App Cas 911, at 915, per Lord Blackburn).

It is clear that under a clause of this nature those in charge of day to day operations of the assured company and its senior management are expected to take reasonable steps required to maintain, update and test all hardware and software programmes, and failure by an employee in discharging such duties would not suffice.[38] However, what is less clear is who sets the standards in maintaining, updating and testing the hardware and software programmes that the assured must conform to, and equally, what these standards include. As it is worded, the clause is vague and thus has the potential to create disputes between parties.[39] It will certainly be an improvement if it makes reference to current (or prevailing) industry standards requiring the assured to operate at that level.[40]

We also observed that some policies impose more stringent requirements on the assured in an attempt to mitigate moral hazard. In some policies the obligation to maintain and update software, and even to take other security measures, has been extended to the employees of the assured rather than only senior executives. Accordingly, a clause worded in the following fashion[41] appeared in 4 policies we examined:

> The Insurer will not pay any claim or loss under this policy arising out of or relating directly or indirectly to any accidental, negligent or unintentional act or failure to act by an employee by the Insured, or an employee of a service provider, to protect the network system by anti-virus and firewall software programme or to undertake other network security measure.

Given the recent trend in construing exclusion clauses, it is possible that an exclusion clause of this nature might be construed narrowly[42] but there is no escaping the fact that the wording is rather well-defined and this is intended to be a very broad exclusion.

We also encountered in some policies (only 5 from the data set) that insurers combined a "reasonable precautions" exclusion with a "prior knowledge of circumstances" exclusion clause. The primary focus of the latter is to deny coverage in cases where a loss is discovered during the policy period,[43] but is due to an event which the assured "ought to have known", "ought reasonably to have known", "ought to have suspected" or "ought to have reasonably

---

[38] See, *Fraser* v. *Furman (Productions) Ltd* [1967] 1 WLR 998, at 905, per Diplock, LJ. A similar issue of imputation of knowledge might arise in the context of the duty of fair presentation on the part of the assured at the pre-contractual stage (s. 3 of the Insurance Act (IA) 2015). However, in that context the statute expressly stipulates that for the purposes of this duty, the knowledge of the assured company's senior management or those responsible for the assured's insurance would amount to the knowledge of the assured (s. 4(3) of the IA 2015).

[39] For such a dispute before courts in the United States see, *Columbia Casualty Co. v. Cottage Health System, No. 2:16-cv-3759 (C.D. Ca.).*

[40] We must stress that some of the clauses we examined made explicit reference to prevailing industry standards. And in one policy we noted that the assured is expected to follow the insurer's requirements with regard to firewalls and antivirus protection.

[41] The wording was slightly different in 4 policies we encountered regarding this requirement, but the essence of the requirement was the same.

[42] See particularly the Supreme Court judgment in *Impact Funding Solutions Ltd* v. *AIG Europe Ltd* [2016] UKSC 57; [2017] Lloyd's Rep IR 60. See also, *Transocean Drilling UK Ltd* v. *Providence Resources plc* [2016] EWCA Civ 372; [2016] 2 Lloyd's Rep 51 and *Presimmon Homes Ltd* v. *Ove Arup & Partners Ltd* [2017] EWCA Civ 373; [2017] 2 C.L.C 28.

[43] Cyber attacks or breach events are usually discovered by the assured after a certain period of time from the date on which they have first occurred.

been discovered" before the start of the policy period.[44] When both clauses appear in the same policy for the purpose of mitigating moral hazard, the result could be catastrophic for the assured. By way of example, an assured is likely to fail to recover under such a cyber policy if a claim arises out of a breach event occurring prior to the policy period, for example due to a software update failure on the part of the assured.

### ii) Claim Arising Basis

All policies we examined offer cyber risk insurance cover on a "claims made" basis. This essentially means that cover under a cyber liability policy is triggered as long as a "claim" arises during the policy period regardless of when the cause (e.g., network security failure or breach event) or circumstances giving rise to the claim have taken place. However, this could create a serious problem for cyber risk insurers. Unlike claims made under commercial general liability policies, where the date of the incident giving rise to the liability is easy to identify (e.g., the day of fire), in the case of cyber security breach, this can be much harder to identify as in many cases such breaches can go undiscovered for weeks or even months. Therefore, in the absence of any additional clause in the policy, a cyber liability insurer must indemnify the assured for any third-party claims arising from a network security failure as long as that claim is made during the policy period, even if the network security failure occurred long before the policy inception period. To deal with this eventuality, cyber risk insurers could incorporate into their policies a "retroactive date" which attempts to place a limit on or deny coverage for breaches that occur prior to a specified date, even if the claim is made during the policy period. In fact, we found that 4 of the policies examined contained a "retroactive date" provision. A typical clause of this nature would provide:

> The policy shall not cover any claim first made during the policy period and arising from any breach event, act, fact, circumstance or cause which was committed or occurred on or before the Retroactive Date.

The default position for insurers is to set the inception date of cyber cover as the retroactive date. Obviously, this has the effect of restricting the coverage provided by the policy significantly and might not be suitable for SMEs in certain sectors, such as those that possess significant amount of personal data or those that rely heavily on their databases as part of their daily business (e.g., accounting firms). We understand that insurers would not be adverse to setting a retroactive date six or twelve months before the inception date. However, that usually requires negotiation at the underwriting stage. Obviously, the longer the length of time between the retroactive date and the policy inception date, the broader the coverage.

To deal with the fact that cyber security breaches that occur before the inception date might give rise to claims by third parties during the policy period, a clause known as "discovery trigger" is incorporated into some policies. Five of the policies examined contained such a clause. The objective of this clause is to restrict the right of the assured to claim under the

[44] For the purposes of such clauses, it will be vital to determine whose knowledge within the assured's corporation will be imputed to the company. Naturally, this would vary from company to company but in light of the principles emerging from the seminal case of *Meridian Global Funds Management Asia Ltd*. v. *Securities* [1995] 2 AC 500- especially taking into account the language of such clauses, their content and policy considerations- it can safely be suggested that the knowledge of such breaches by those in the higher levels of management is likely to be attributed to the assured company.

policy for a third-party claim if it arises from a cause or circumstance or act which must first have been discovered (and reported) to the insurer within the policy period (or if there is a retroactive date after that date). In some policies, the relevant claims notification clauses require the assured to notify the security breach or event to the insurer "as soon as possible" or "immediately".[45] Disputes as to how long a period is allowed for notification under such clauses could arise as well as what the consequence for the breach of such clause will be[46] unless these issues are specified in the clause in a precise fashion.

## V) Lessons Learned from SMEs in relation to Their Understanding of Cyber Risk Insurance and Approach to Risk Management

Our primary objectives in conducting this survey were to understand:

i) how common it is for SMEs to purchase cyber risk insurance cover;
ii) the degree of knowledge SMEs have on the scope of cover provided by such policies;
iii) the role that cyber risk insurance and other measures play in the cyber risk management structures of SMEs;
iv) the reasons for those SMEs opting not to purchase this product; and
v) how SMEs can be incentivised to use cyber risk insurance as a risk mitigation tool.

The results of the survey were both interesting and revealing. The number of SMEs that indicated they had cyber risk insurance cover in place was rather low: only 18.5% of those who took part in the survey stated that they had cyber risk insurance in place purchased from a UK insurer. The rest (81.5%), however, indicated that they did not have cyber risk insurance, but expected their commercial insurance products (e.g., professional indemnity insurance, public liability insurance, employers' liability insurance and business equipment and contents insurance) to provide adequate degree of cover against cyber risks. This is obviously an erroneous presumption, as most (if not all) commercial insurance policies exclude losses caused by or contributed to by the malicious use or operation of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system.[47]

---

[45] In a different context, Cockburn, CJ, in *R v Berkshire Justices* (I878) 4 LR QBD 469, at 476, said the word "immediately" implies "prompt, vigorous action, without any delay", after learning of the relevant facts. See also, *Re Coleman's Depositories* [1907] 2 KB 798, at 807.

[46] See, *Friends Provident Life & Pensions Ltd.* v. *Sirius International Insurance* [2005] EWCA Civ 601; [2005] 2 Lloyd's Rep 517. Cf *Alfred McAlpine plc* v. *BAI (Run-Off) Ltd. [*2000] 1 Lloyd's Rep 437 and *K/S Merc-Skandia XXXXII* v. *Certain Lloyd's Underwriters (The Mercandian Continent)* [2001] EWCA Civ 1275; [2001] Lloyd's Rep IR 802.

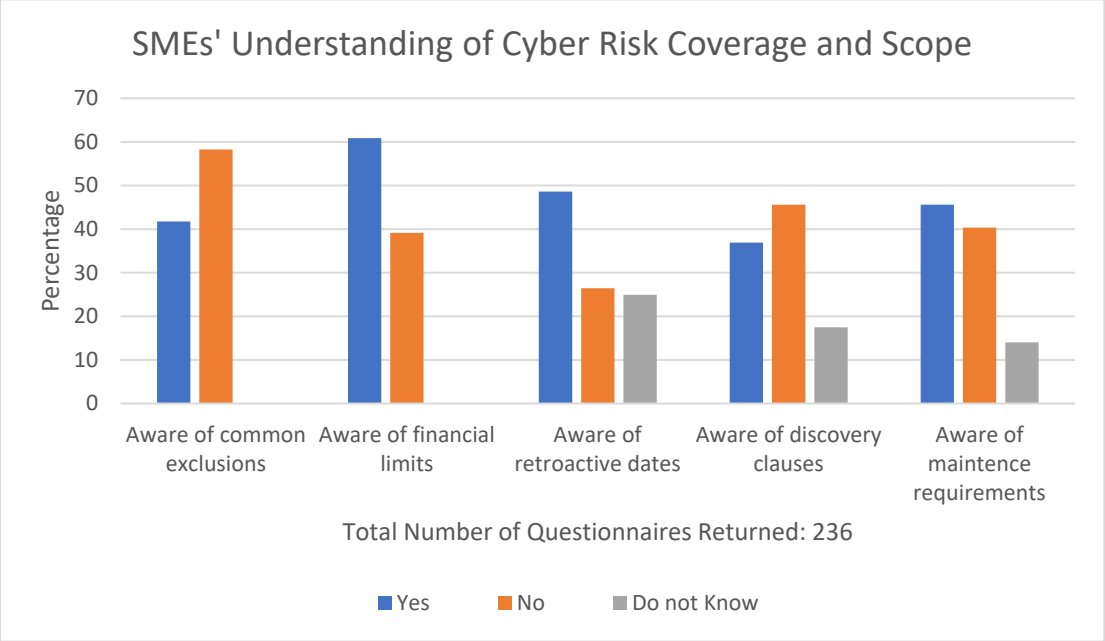
[47] The following is a typical exclusion clause that often appears in commercial insurance policies:
This Policy does not cover:

**Computer Virus and Hacking**

In the following part of the survey, we wanted to test the knowledge and understanding of SMEs on the scope of cover provided by cyber risk policies. We put this question not only to those who have cyber risk insurance cover but also to those who indicated that they preferred to rely on their commercial insurance coverage against cyber risks. In particular, we wanted to find out whether they were aware that cyber risk policies often include common exclusions (such as social engineering, dishonesty, fraud and criminal acts), impose financial limits on cover, and contain "retroactive dates" and "discovery clauses" that could reduce the scope of cover significantly and might impose demanding "maintenance requirements" that could jeopardise the cover in case of their breach.[48]

The results for this part of the survey could be found in Figure 4.

**Figure 4**




It was not, for example, surprising that most SMEs were not aware of the use of discovery clauses in cyber policies and their potential impact. This is a rather technical clause

1. Damage to any computer or other equipment or component or system or item which processes stores transmits or retrieves data or any part thereof whether tangible or intangible (including but without limitation any information or programs or software) and whether Your Property or not where such Damage is caused by Virus or Similar Mechanism or Hacking

2. financial loss directly or indirectly caused by or arising from Virus or Similar Mechanism or Hacking…

[48] In the survey, the meaning of these terms and their effect were clearly set out and, as indicated above, our researchers were prepared to explain what those terms meant to those who needed further clarification.

but might significantly restrict the right of the assured to claim under the policy as it would prevent the assured from submitting a claim in cases where the cyber security breach giving rise to the claim is not discovered within the policy period (or if there is a retroactive date after that date). In a similar vein, researchers were not surprised that most SMEs were aware of the fact that cyber policies often impose a financial limit on recovery. In fact, setting a top ceiling for indemnity is very common in most commercial business insurance policies and is effectively something that most SMEs expect to encounter when purchasing a new insurance product. Similarly, it was not unexpected to see that most SMEs were not fully aware of the common exclusions that are incorporated into cyber risk policies. In particular, these who completed the survey were genuinely surprised to find out that most cyber polices contained a broadly worded social engineering exclusion that excludes loss caused as a result of the voluntary actions of those who have express or implied authority by the SME to have access to use or operate the SME's network system when they are induced by any dishonest act to voluntarily part with title to or possession of any property and/or may cause any loss to the SME.

On the other hand, it was somehow surprising for researchers to find that a majority of SMEs did not know or appreciate that cyber risk policies might contain retroactive dates (essentially giving the insurer the right to deny coverage for cyber breaches that occur prior to a specified date). Insurers in the cyber risk insurance context make use of such clauses since without such clauses a cyber insurer would be expected to pay any claim presented during the policy period regardless of when the breach occurred. It is the nature of cyber risks that a breach might go undetected for weeks and there could be a significant gap in terms of time between the breach occurring and any loss being identified. It is this nature of cyber risks that often leads insurers to utilise retroactive dates, which limits the ability of the assured to seek indemnity for losses that arise as a result of a network security failure that occurred prior to the inception of the policy.

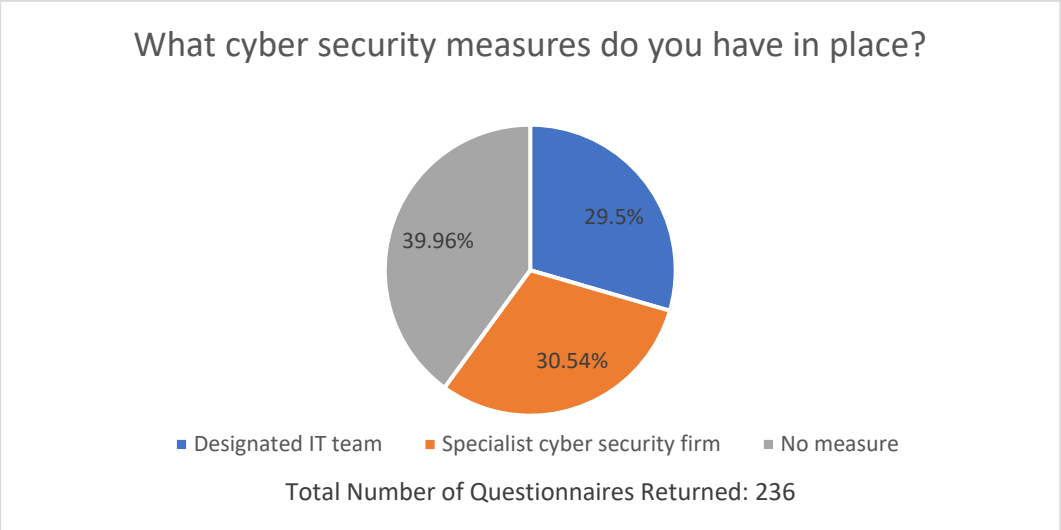
Another interesting finding is that slightly more than half of the SMEs surveyed were not aware that cyber risk policies impose a duty on the SMEs to take "all reasonable steps" to maintain and update security software and hardware. In fact, we found such clauses (with varying degree of severity)[49] in all policies we examined, but the worrying finding is that most of the SMEs surveyed do not appreciate the fact that there is an expectation for them to take steps to ensure that cyber resilience measures are in place and such measures are maintained throughout the policy period.

There is no denying of the fact that there is a correlation between robustness of cyber security measures adopted by an SME and the manner in which cyber risk insurers rate the riskiness of that particular business. This correlation led us to seek an understanding from the SMEs as to how they manage cyber risks within their organisation and how they perceive becoming a target of a cyber attack, as these factors could certainly be key when considering putting in place robust cyber security measures. The purpose here was to identify what cyber security measures (if any) they have in place and identify how common it is to employ a specialist cyber security firm. The results (Figure 5) indicate a patchy approach to cyber

[49] As indicated above, some of the maintenance clauses are designed to operate as a "warranty"—i.e., in case of breach the cover is suspended until the breach is remedied. Some, on the other hand, are "conditions precedent" to liability, meaning that in case of their breach the insurer is not liable for any loss emerging as a result of the breach.

security amongst the SMEs surveyed: only 29.5% of them indicated that they have a designated IT person/team in place who deals with cyber security issues of their business, while 30.54% indicated that they rely on the services of cyber security firms; but the majority (39.96%) stressed that they had no cyber security measure in place.

**Figure 5**



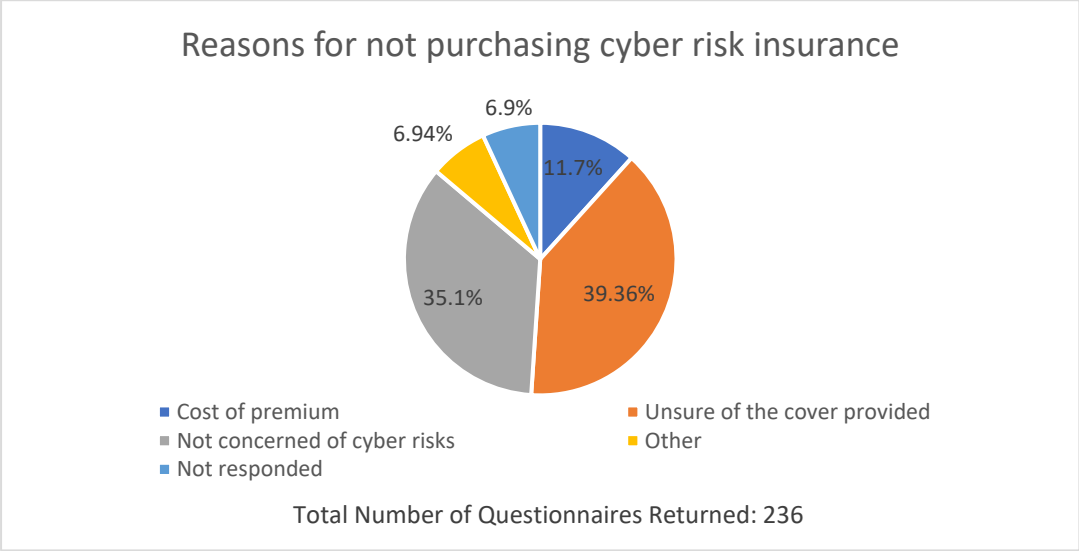

When we asked those who do not have any cyber security measures why they do not consider utilizing a specialised cyber security firm that can help them reduce their cyber exposure, the results indicated that a large majority of them (68.9%) were unsure as to what services a cyber security firm could offer them in that regard. We found this interesting as it shows that there are still many unknowns for SMEs when it comes to cyber threats and security measures that can be employed to reduce such threats.

However, perhaps the most striking response was to the question as to how likely they feel that their business may become a target of a cyber attack. A large majority (72.8%) of those surveyed indicated that they regard the prospect of an attack to their organisation as "not likely". This is staggering considering that a fair majority of SMEs surveyed seem to rely on their IT systems as an integral part of their day-to-day business (taking orders, storing data, online sales, etc.).

In the final part of the survey we tried to evaluate i) why most SMEs do not view cyber risk insurance as an integral part of their risk mitigation strategy, and ii) how cyber risk insurance products could be tailored so that they are more attractive to SMEs.

Regarding point (i), we asked SMEs that do not purchase cyber risk insurance what are the reasons for not using cyber risk insurance as part of their risk mitigation strategy. Figure 6 below shows the results.

**Figure 6**



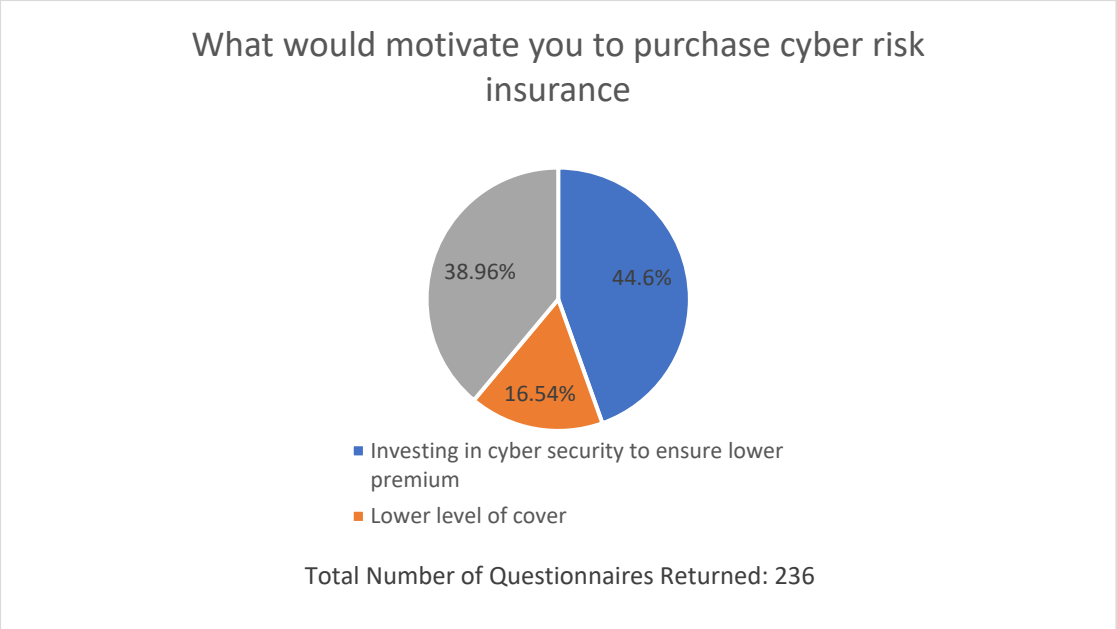

This makes clear to us that SMEs are not shying away from this product simply due to the cost of such products; only 11.70% indicated that the cost of cyber risk insurance is the main reason. More than one third of the surveyed SMEs are simply unaware of the scope of cover that this product provides, and another significant group (35.10%) does not believe that their business is likely to be adversely affected by cyber risks. These are staggering findings, which clearly indicate that there is lack of appreciation of the magnitude of cyber threats facings SMEs, and that the insurance sector has not managed yet to communicate to its potential customers the nature of their product and how it can help SMEs.

Regarding point (ii) we put two questions to those surveyed. In an attempt to measure the degree of knowledge that SMEs possess with regard to different types of cyber insurance products available in the market, we asked all those surveyed whether they were aware of cyber risk insurance products that instead of indemnity offer assureds cover for restoration of their IT systems following a cyber attack and provide them with services such as legal assistance, crisis management, and public relation support following a cyber attack. This kind of product might be cheaper to purchase, but equally it might be more suitable for many SMEs, especially those that do not rely on their IT systems as an integral part of their commercial activity. Obviously, this product will not have much value for those who rely on their IT systems for bookings, logistics and data processing, given that a security breach for such businesses would lead mainly to loss of business opportunities and/or income. Interestingly, 67.37% of those surveyed were not aware of the availability of such cyber risk coverage.

Lastly, we asked those who indicated that they had no cyber risk insurance what might motivate them to consider purchasing it going forward. The results can be seen in Figure 7. It was very interesting to note that more than half of the SMEs who responded to this question indicated that they would be prepared to invest more in cyber resilience tools if that would help them to pay a lower premium (44.60%). Almost one third indicated that they would be tempted to purchase an insurance policy that offers them cover against a reduced variety of risks, and

16.54% indicated that they would be prepared to have a cyber risk insurance policy that offers a lower financial limit of coverage if that would be the cheaper option.

**Figure 7**




## VI) Lessons Emerging and Our Recommendations

It is clear to us that on the supply side, the fact that this is a new line of business with limited historical data on claims makes insurers rather cautious. There is an apparent tendency to qualify the insurance product offered to SMEs by relying perhaps excessively on exclusion clauses and other risk-control mechanisms (such as retroactive dates and discovery clauses).[50] This is not unexpected, especially in the context of an emerging risk, but it is also evident that it will not be possible to scale this product up unless some adjustments to it are made (which will be discussed below).

Turning to the demand side of the market, our survey of SMEs clearly demonstrates that not many SMEs see cyber risk insurance as a necessary risk mitigation tool. This is, unfortunately, not due to the fact that they have sound cyber security measures in place. In fact, most do not see cyber risks as a problem for their businesses at all, including ones that heavily rely on data stored on their systems for their business (i.e., SMEs involved in technical and scientific endeavours) and those that rely on online bookings and sales (i.e., those in the hospitality sector). The survey also demonstrates that there is a lack of appreciation of the

[50] Given that cyber risk insurance contracts to SMEs are essentially commercial insurance products, their terms and exclusions would not be subject to any statutory control under the Consumer Act 2015 (s. 61). Also, such contracts do not come under the scope of the Unfair Contract Terms Act (UCTA) 1977 (s. 15(3)(a)(i)).

potential impact of various risk-control clauses (e.g., maintenance warranties, exclusions) and claim control clauses (discovery clauses and retrospective dates) often used in cyber risk insurance policies. This is not entirely surprising, as some of the terms used in cyber risk policies are rather technical, but it was concerning to see that most of the SMEs surveyed did not know that there was an expectation on them to maintain and update security software and hardware. It was also evident that a large majority of those surveyed did not appreciate the fact that there are different types of cyber risk insurance products in the market. It is worth noting, for example, that a cyber product that pays for restoration costs rather than providing indemnity might be more suitable for many small-sized businesses, especially given that they do not have expertise or IT experts to restore their service quickly and safely following a cyber attack.

Bringing it all together—our understanding of the insurance market (especially the legal effect of the cyber risk policies on offer to SMEs), results of the surveys presented in Part V, and discussions with insurance brokers/SME representatives—our main recommendation is that the insurance market should consider designing a new cyber risk insurance product that aligns cyber security with the principle of indemnity. More specifically, we recommend that for SMEs a new insurance product that offers not only indemnity (first and third party) in case of a cyber attack, but also cyber security services (a cyber risk assessment at the outset and interim security checks) as part of the cover, will be ideal.[51] This kind of new insurance product is likely to be attractive given that our survey clearly demonstrates that SMEs are prepared to invest in cyber resilience, especially if this is likely to yield them benefits in terms of acquiring cyber risk insurance. As we see it, the benefits of such a product are several, not only for SMEs but also for risk carriers (insurance providers):

i) It is clear that most SMEs lack technical support and knowhow to enhance cyber security of the systems that they use as part of their business.[52] An insurance product that provides a cyber security element is important as it will provide a continuous check on the vulnerabilities of the digital network of SMEs, update its defences by reference to the most current cyber threats and effectively create a cyberworthy ecosystem that has a strong proactive risk management approach. We believe that securing the cyber dimension this way is more important for SMEs than for large corporations. This is because SMEs, due to their size and financial resources, are prone to be more adversely affected by the "ripple effects" of successful cyber attacks, for example by permanently losing clientele due to adverse publicity—a risk that cannot be mitigated by insurance but can be managed better with preventive measures.

ii) Making a cyber security firm an integral part of a SME's cyber reliance strategy will have an additional benefit in the form of providing essential training for SME

[51] This product could be sold by insurers in partnership with cyber security firms. It is also plausible that cyber security firms consider providing a new product to their clients offering cyber insurance as a feature of their cyber security service contracts. The latter could be more suitable for larger corporations which rely on computer systems and data networks as part of their daily operations.

[52] Apart from our survey, this has also been pointed out by M. Heidt et al. "Investigating the Security Divide between SME and Large Companies: How SME Characteristics Influence Organizational IT Security Investments" (2019) 21 Inf. Syst. Front 21 at 1285

employees in cyber hygiene. It will be in the interest of the insurance provider to require its partner (the cyber security firm) to provide such training, especially on how to react upon a cyber breach—in terms of operational steps to be taken to mitigate the impact of the attack also in terms of legal responses, such as regulatory notifications and collection of evidence. Having such training will enable the relevant employees of the SME to have a clear path of action in the first few hours after the attack, which are among the most critical.

iii) The benefits of such a product for risk carriers are several. Most importantly, having cyber security screening undertaken by a trusted cyber security firm will not only enable an insurance carrier to rate the risk correctly at the outset, it will also ensure that the risk is maintained at an acceptable level throughout the insurance period. The continuous monitoring of the network by a trusted partner will operate as an audit of the network's health. Put differently, the insurers will not be relying solely on the assured to maintain the cyber resilience systems in good order. This will be done by cyber security experts, and if additional instructions are given to the assured SMEs by the cyber security firm, this will be documented. This kind of paper trail will also be very useful for insurance providers if at a later stage they would like to raise any potential breach of insurance terms by the assured.

iv) We also believe that one of the main reasons leading cyber risk insurers to introduce an extensive list of exclusions into cyber risk insurance products, and technical terms as a risk control mechanism, is the fact that they do not have adequate means of obtaining reliable information concerning the approach of SMEs in managing cyber security threats during the policy period. In physical risks insurance (e.g., when insuring a building or warehouse), insurers will have different ways of ensuring that the risk is maintained by the assured at an acceptable level. They often require the setup of security cameras and physical security controls; they will pre-approve certain types of locks/doors; and they will require the establishment of security procedures for accessing the insured locations. This new product will achieve a similar outcome for cyber risk insurers. The cyber security firm's regular checks and maintenance advice will ensure that the SMEs do not inadvertently increase the risk of loss by failing to take adequate or necessary security measures. There is every reason to believe that this will enhance the confidence of insurers in the risk and attitude of the assured to the risk and might lead to a reduction in the number of exclusions or risk control mechanisms used in cyber insurance policies.

v) An additional benefit of such a product for insurers is that they can incentivise the assured SMEs to ensure that they adopt better cyber resilience systems internally. One feature of this new product will be that reports will be produced by the cyber security firm at the outset and in the middle of the insurance period, which will give insurers an in-depth, ongoing knowledge of the security ecosystem of the SME, and also confirmation that the SME in question employs best security practices that

reduce its overall cyber risk exposure.[53] This arrangement can be formalised by introducing a premium return mechanism in the policy, whereby a bonus at the end of the current policy year or a reduction in next year's premium will be given to the SME, provided certain predetermined cyber security milestones have been achieved as verified in the cyber security reports and no claims have been made under the policy.[54] Such arrangements are also quite popular with physical risks insurances whereby a certain percentage of the premium is to be returned to the insured upon the end of the policy period provided that there are no claims under this policy or their quantum is below a certain financial threshold.

vi) It is also worth mentioning that this product, while compatible with the Cyber Essentials scheme of the UK Government,[55] will provide much more, as it gives a real-time evaluation of the risk profile of the SME's digital network and provides remedial actions and tailor-made training of the SME's employees, in addition to the insurance indemnity cover. The Cyber Essentials Scheme provides a minimum level of protection, yet this is not sufficient for achieving a significant reduction in the premium, which requires an ongoing evaluation of the risk profile of the SME and the taking of remedial actions when gaps are discovered. As such, the suggested product aims to provide tailor-made protection that is above the protection offered by the Cyber Essentials scheme and aims to satisfy the requirements of the insurance industry.[56]

Having set the details and justification for our main conclusion (i.e., the need to develop a new integrated product that provides cyber security assistance to SMEs in addition to indemnity), we would like to clarify a few related issues at the end of our analysis.

First, our suggested solution presupposes that cyber security companies would be interested in working with insurance providers in partnership in providing this new product. During the course of the project, we worked closely with several cyber security firms, and it is our understanding that they would see this as a great business expansion opportunity. Many of their clients are larger companies and expanding their reach to SME market is something they are

[53] Such audits are not uncommon in insurance, with several insurance policies covering the risk of theft of warehoused items requiring regular audits of the security systems employed in warehouses, as well as the regular taking of inventory.

[54] The converse may also be true; where a business does not perform well from a cyber security perspective, there is potential that the insurer may increase the renewal premium, or alternatively decline to offer cover at all. This brings the mid-term cyber report into sharp focus, whereby the SME may have the opportunity to address any shortcomings before renewal.

[55] Cyber Essentials is a certification scheme designed to show an organisation has a minimum level of protection in cyber security through annual assessments to maintain certification. The scheme is backed by the UK government and overseen by the National Cyber Security Centre. Its primary aim is to encourage organisations to adopt good practice in information security. SMEs are actively encouraged to obtain this certification, and cyber insurers would expect a potential assured to have this certificate.

[56] As pointed out by J. M. Such et al, "Basic Cyber Hygiene: Does It Work?" in (2019) Computer, vol 52, no.4 at 30. Whilst the Cyber Essentials scheme goes a long way in mitigating risk, it does not guarantee that an SME will maintain adherence to the guidelines set out.

actively working on, so this new product will undoubtedly present a great opportunity to them.[57]

Second, a legitimate question can be asked as to whether a product that offers cyber security services and indemnity at the same time would be more expensive, effectively pricing most of the SMEs out. It is beyond the scope of this article (and expertise of its authors) to engage in such an actuarial study to test this hypothesis, but it is our belief that this will not be the case due to the fact that losses that need to be paid out by insurers should be reduced dramatically as a result of the work that cyber security firms do (at the outset and during the currency of the policy). Put differently, we believe that under the assumption that cyber insurance claims will be reduced in the light of stringent cyber security measures introduced, insurers will not lose out as a result of sharing part of their premium with their partner cyber security firm and thus they will not have to resort to increasing the premium.

Third, it is our opinion that introduction of such a new product might lead to changes in the way cyber insurance products are sold to SMEs in the future. Today, cyber risk insurance business is usually sold on a fixed time basis. This requires insurers to assess the risk at the outset and determine the premium payable during the period of insurance. The premium payable is fixed and reflects the risk assessment carried out at the outset based on data presented to the insurer and obtained by the insurer from other sources at its disposal. Inevitably, data relied on by insurers for risk rating would be historical—that is, reflecting how efficiently the cyber security systems operated in the past, and the previous claim history of the assured. However, if insurers are presented with up-to data regularly by their partner cyber security firm on the manner in which the relevant SME's cyber resilience systems are functioning, along with the SME's approach to cyber security, this might enable cyber risk insurers to offer a new product to SMEs known as "usage-based insurance" that will utilise this dynamic data made available to insurers to determine the premium rate at different stages of the policy period. Put differently, the insurers might be able to utilise the massive amount of data and be in a position to offer a new type of insurance—one that charges a different premium rate based on the most recent cyber security performance of the SME in question.

Fourth, we believe that such an integrated approach will not only enhance cyber security but will do in a sustainable way.. Some commentators believe that making cyber insurance compulsory, especially for SMEs, is the right way to enhance cyber security.[58] We have serious doubts about this approach. There is no doubt that cyber risk insurance is one of the main risk management tools against cyber threats, but making it the first line of defence (and making it compulsory) will increase operational costs for SMEs and it is rather doubtful that in the current economic climate SMEs (without subsidies from the government) will be able to cover such additional costs. Also, apart from the economic aspects of this matter, establishing a compulsory insurance regime would require the preparation of a legal framework which is unlikely to be in the agenda of the government at present. Hence, our main recommendation in this paper is the development of a new product where insurance could be utilised as a catalyst for enhancing cyber security for SMEs.

---

[57] As indicated above, it is also possible that cyber security companies might see this as an opportunity to incorporate insurance into the service contracts they have with their clients.

[58] J.M. Lemnitzer, "Why Cybersecurity Insurance Should Be Regulated and Compulsory?" (2021) Journal of Cyber Policy 118.

Last but not least, given the fact that most of the SMEs we surveyed seemed to be not fully alert to the fact that their businesses are vulnerable to cyber attacks, it is clear to us that more training needs to be offered to SMEs, and this should be a priority for the Government.[59] Given the cost of cyber attacks to the UK economy, there is vast social benefit in providing such training. That said, we believe that introduction of an integrated insurance product along the lines described in this paper will certainly help to reduce the number of successful cyber-attacks to SMEs and hence make a huge contribution to the UK economy at the same time, yielding a significant social benefit.

[59] It is one of the objectives of the National Cyber Security Centre to provide information and training on cyber security threats for individuals and businesses. Ensuring staff are trained to a reasonable standard can go a long way to preventing ransomware and phishing attacks, with the National Cyber Security Centre advocating the importance of this step: https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks (last accessed on 1 March 2023) and https://www.ncsc.gov.uk/guidance/phishing (last accessed on 1 March 2023).