Cyber Insurance from the stakeholder's perspective: A qualitative analysis of barriers and facilitators to adoption

Cyber insurance from the stakeholder's perspective

A qualitative analysis of barriers and facilitators to adoption

Dawn Branley-Bell

Northumbria University, dawn.branley-bell@northumbria.ac.uk

Lynne Coventry

Northumbria University, lynne.coventry@northumbria.ac.uk

Pam Briggs

Northumbria University, p.briggs@northumbria.ac.uk

Business disruption from cyber-attacks is a recognized and growing concern, yet the uptake of cyber insurance has been substantially lower than expected. This study aimed to identify what factors may be influencing perceptions and uptake of cyber insurance. In-depth interviews were conducted with two stakeholder groups: those responsible for making cybersecurity decisions within businesses, and those involved in marketing cybersecurity products and/or services including cyber insurance. Thematic analysis generated five themes from the data: *High complexity of company-level decision making, Security investment trade-off, Lack of risk data and immaturity of cyber insurance, Mistrust of insurers,* and *Compliance legislation as a driver for cyber insurance adoption*. The results highlight the importance of recognizing that internal organizational decision making involves a complex eco-system which can make the process of obtaining and renewing cyber insurance an effortful process. Legislation may facilitate insurance uptake, but several external factors represent key barriers. There is a need for clearer policy wording, improved processes for cyber risk assessment, improved trust in insurers and lower policy premiums.

CCS CONCEPTS • **Security and privacy ~Human and societal aspects of security and privacy • Social and professional topics ~Computing / technology policy**

Additional Keywords and Phrases: cyber insurance, cybersecurity, risk assessment, policy, qualitative methods

ACM Reference Format:

First Author's Name, Initials, and Last Name, Second Author's Name, Initials, and Last Name, and Third Author's Name, Initials, and Last Name. 2018. The Title of the Paper: ACM Conference Proceedings Manuscript Submission Template: This is the subtitle of the paper, this document both explains and embodies the submission format for authors using Word. In Woodstock '18: ACM Symposium on Neural Gaze Detection, June 03–05, 2018, Woodstock, NY. ACM, New York, NY, USA, 10 pages. NOTE: This block will be automatically generated when manuscripts are processed after acceptance.

1 INTRODUCTION

Cyber-attacks are a major financial and reputational concern for businesses and other organizations. According to the UK government's latest Cybersecurity Breaches Survey [45], almost 40% of UK businesses report having suffered a cyber breach in the last 12 months. Within these, 31% report having a cyber breach or attack at least once per week. Bearing in mind that this is reported and *detected* breaches, this is likely to be an underestimation of the true frequency of breaches. Awareness of cyber risk has also increased in recent years and with it the perceived importance of enhanced cybersecurity measures [22,36,37,45].

However, even with sophisticated security measures in place (sometimes referred to as self-protection measures, Dou et al., 2020), it is not possible to prevent all cyber-attacks and cyber insurance provides a valuable way for businesses to manage this residual risk [6]. Insurance will generally cover two broad loss categories: first party and third party. First party losses are those directly suffered by the insured business as a direct result of the incident. Third party liability refers to claims from parties external to the insurance contract, who suffer a loss due to the insured's conduct. Cyber insurance can also cover costs related to investigating the cause of an incident, dealing with business interruption and restoring services, notifying affected parties, managing public relations and media communication, and computer forensic investigation costs. A minority of policies also cover extortion and ransom payments demanded as part of the incident – although these are more commonly listed as an exclusion [30]. Other common exclusions include criminal or fraudulent act from the insured, negligent disregard for computer security, loss to systems not owned or controlled by the policyholder, contractual liability, physical bodily harm, acts of terrorism, war or god, IP theft, and fines and penalties related to legislation [30].

Adoption of cyber insurance encourages organisations to think of cyber risk in relation to monetary value, which could have additional benefits including driving increased security and more appropriate budgeting within the organisation [14]. Additionally, adoption has the potential to not only protect individual organisations, but also to increase security at a societal level. The risk faced by one entity can also be dependent upon the exposure of other related entities. Insurance can act as a strong incentive for promoting investment in other self-protection measures, especially as insurance companies often require a specific level of security measures to be in place before coverage will be offered [28,30]. Therefore, cyber insurance has the ability to increase cybersecurity for the internet as a whole [6,23] rather than just compensate for its lack.

Two common concerns in the insurance industry also address societal level cybersecurity issues: Adverse selection and 'moral hazard'. Adverse selection refers to an asymmetry in information between the insured and the insurer, i.e., the insured has information about their risk profile that is not made available to the insurer. This can result in a policy holder obtaining coverage at a lower premium than the insurance company would charge if it were aware of the applicant's actual risk level. Adverse selection also means that high-risk parties may be more likely to adopt insurance in the first place, compared to low-risk parties. Moral hazard refers to a change in behaviour following adoption of the insurance policy, i.e., the insured behaving less securely and/or investing less in security once insurance coverage is in place [31,33]. Adverse selection and moral hazard have been linked to a range of insurance products including motor insurance [11], health insurance [19] and crop insurance [12]. However, it is worth noting that this is becoming a contentious subject with many suggesting that the threats of adverse selection and moral hazard may have been exaggerated [32,34]. There is also little evidence to suggest that moral hazard is a significant concern for cyber insurance. In fact, recent research suggests that cybersecurity measures and cyber insurance appear to show advantageous selection [7] . Advantageous selection occurs when individuals with insurance are highly risk averse and therefore also seek to reduce risk by acting securely even when coverage is in place [26].

Despite significant benefits associated with cyber insurance adoption, it is estimated that only 3 in 10 organisations are explicitly insured against cyber risk (Cybersecurity Breaches Survey, 2020); with estimates even lower for Small and Medium-Sized Enterprises [17]. Factors which have been suggested as potential barriers to uptake include: a lack of cybersecurity awareness (AON, 2017; although as aforementioned there is evidence that awareness has increased), confusion around availability of policies [29], policy coverage and a lack of standardisation [5,22], uncertainty relating to "silent" cyber coverage within traditional insurance policies [40], expensive premiums driven by a lack of actuarial data and the correlated properties of cyber-attacks enabling numerous businesses to be hit simultaneously [2,15,18], concerns over actual coverage and exclusions [2,5], difficulty in predicting the likelihood of future cyber incidents [5] makes it difficult to calculate premiums, and a lack of broker knowledge [16]. However, there is a lack of empirical research in this area [20,22,30], particularly in relation to in-depth investigation of stakeholder perceptions of cyber insurance [28]. Weishäupl et al. [38] conducted a series of case studies with stakeholders. However, their study focused on information security from a technological solution viewpoint, rather than cyber insurance. Processes for technological solutions may vary from those involved in insurance adoption, therefore our study applies similar empirical approaches to the investigation of perceptions of cyber insurance specifically.

Woods and Simpson [39] identified the need for further insight into stakeholder perceptions within this field. They conducted a stakeholder analysis with policymakers and those in the cyber insurance industry, with a focus on providing a roadmap of the roles governments and the insurance industry can play in increasing uptake. Consumers of cyber insurance were 'out of scope' for their research (p. 210). Our study expands upon this work, using one-to-one interviews with stakeholders (including potential buyers) to further explore and identify facilitators and barriers to adoption at the organisational level.

2 MATERIALS AND METHODS

We conducted a series of in-depth qualitative interviews with companies and consulting partners such as insurance brokers. This combination of different interview partners was chosen to address concerns that companies may sometimes be reluctant to disclose security-related inadequacies due to concerns around potential attacks and/or damage to reputation [35]; and is in alignment with other studies using a similar approach (e.g., [38]). This approach also allows us to benefit from the brokers experience of decision making across many organizations, and compliment it with the first-hand, comprehensive information provided by the organizations themselves.

2.1 Sample

Eleven interviewees were recruited via e-mail invitation to existing business contacts, networking events, and mailing lists. Of the sample, six individuals were responsible for making cybersecurity decisions within a company (1 with experience in an SME, 2 within a large company, and 3 with experience in both SMEs and large companies), and five individuals were involved in the marketing and/or sale of cybersecurity related products or services as an insurer, broker or consultant.

2.2 Procedure

Ethical approval was obtained from the University Ethics Board prior to data collection. Semi-structured interviews (lasting on average 45 minutes) were conducted with each interviewee independently; either in person or via video call. Each interviewee was asked about the processes behind cybersecurity decisions within their company(s) – this included discussing general perceptions of cyber insurance, which staff roles and teams would be involved in a decision around purchasing cyber insurance, how long this process would take, any common barriers to the process, the type of information

required by potential insurers and whether they had any experience of a cyber insurance claim within their company(s). Interviews were recorded and transcribed prior to analysis.

2.3 Analytical Approach

The interview transcripts were analysed using inductive thematic analysis [8] using NVivo. The first author coded the dataset independently using an inductive approach, whereby codes were generated from the data rather than a-priori. Codes were collated to identify initial themes. To increase rigor, a team approach was taken with the other authors providing critical feedback on themes and coding. Amendments were made where appropriate. The finalised themes were then generated and agreed upon by all authors.

3 RESULTS

Analysis generated five key themes: *High complexity of company-level decision making, Security investment trade-off, Lack of risk data and immaturity of cyber insurance, Mistrust of insurers*, and *Compliance legislation as a driver for cyber insurance adoption*.

3.1 High Complexity of Company-level Decision Making

Many interviewees commented that decisions around cybersecurity are not made by one person but involve numerous staff members within the business. For example, these decisions may involve the Chief Information Security Officer (CISO), security board, Chief Operating Officer (COO), Financial Director (FD), IT team, various committees and panels, and the executive board. This is particularly true for larger companies, with the decision-making process increasing in complexity with the company size.

> "I doubt whether you'd get one single person, you might do, in a medium to smaller organization […] But I think you now get panels, like a risk committee and get someone from the security discipline, someone from the IT discipline, you get an auditor, you get compliance and those type of people…"

The number of individuals involved can stretch into the hundreds:

> *"We have a security operations team, security engineers, security architects, government risk compliance team (for internal and external audits), security awareness staff, third party and supplier insurance, and a team that worries about email and end point security, a forensics team and an identity management team. The last team is a security platforms team that run a lot of the systems we run on. The team is about 140 people. […] We also have a risk committee".*

This highlights the importance of recognising that internal decision making involves a complex eco-system. Unsurprisingly, given the complexity of these systems and the number of parties involved, cybersecurity decisions at company level can be time-consuming and complex:

> "It can take months, particularly in a complicated organization with so many markets and people so in order to put something proactive in place it takes months of embedding. So, it is a challenge"

Participants reflected on delays occurring across numerous stages of the decision-making process. For example, although the final process of 'signing off' a security-related purchase may be quick and efficient, there can be significant delays

involved prior to reaching this final stage. One of the most time-consuming processes can be the identification and testing of potential products:

> "We'd go to procurement with details on what we have done, what we want, how much it is to buy. The CPO then signs it off based on my team's work. My team would probably have worked on this over a 6-month period (meeting about 6-10 times for an hour or so each) the meeting with the CPO then takes about 15 minutes. […] It is always a much longer process than I've been willing to accept. […]

In addition to lengthy processes, further delays can be experienced due to restricted periods or 'windows' when purchasing decisions can be made. For example, this may be restricted by the dates of quarterly committee meetings or annual windows for budget allocation. There can then be additional delays due to negotiating contracts with product providers and contractors:

> "Even just another 3 months to get contracts into place. Getting contracts into place always involves a lot of negotiation and back and forth with the contractors"

When talking about cyber insurance adoption specifically, interviewees often described a slightly different process compared to other cybersecurity decisions (e.g., the purchasing of anti-virus software or firewalls). One of the most striking differences is that cyber insurance adoption is often driven by departments outside of the technology or cybersecurity departments, such as finance departments and risk committees.

> "I have only ever seen insurance requirements come from finance you know the FD is effectively responsible for insuring the business against risk. […] I have never been in a position where the security person has gone to the finance person to say I think we need insurance"

Unfortunately, this can lead to internal conflict around these decisions. Many of the interviewees described a disconnect between the various influencers and decision-makers. Some stated that they would not have personally opted for insurance, despite their company doing so. For example, one interviewee in his role as technical director stated that he may not have chosen to purchase cyber insurance for his company, but that this decision came from outside of the cybersecurity team:

> "We have a cyber insurance policy at the moment. I must admit it wasn't me that made this decision. As I'm not sure I would have bought one, if I'm honest. The decision came from the risk committee. […] It feels like it is boards outside of cybersecurity teams that make decisions to buy cyber insurance."

Other interviewees described differences in priorities between committees, the board, and other staff involved in the decision-making process:

> "The board owned the purse strings but it's interesting – they made the decisions because they owned the budget, I suppose but they weren't very interested. […] We [the IT team] would be setting out the risks and the threats trying to explain to them why they need to spend more and there would be certain threats they would get very excited about and others that maybe they would be less interested"

> "I think they [the board] expected us to be creating a basic level of security the things they got excited about was if something came to bail on them or they would become personally liable."

These findings demonstrate that the responsibility for cyber insurance uptake is not likely to lie with one person, particularly in larger organisations. This adds complexity for insurers and other bodies aiming to target specific staff roles to boost insurance uptake. There may also be internal conflicts that further complicate the process.

3.2 Security Investment Trade-off

It was clear from our interviews that the decision to adopt cyber insurance was part of a bigger security investment trade-off, whereby the people involved weighed up the perceived costs and benefits associated with adoption. For instance, interviewees referred to the weighing up of insurance against investing in other security measures, with some individuals perceiving insurance as unnecessary if good security measures were in place:

> "I suppose when you're actually putting controls in, there is a form of insurance. So, all you are really doing is, do you pay out some more money for some other controls which you understand, or do you transfer that risk out? […] I suppose the counter argument is the individual risk is, and you put additional controls and pay for it that way"

> "I think there is probably a sweet spot because of the cost of controls you probably get to a size where you can't afford all the controls you know you need to protect your business and that's probably where insurance kicks in where you know the cost to get up and running and having an issue and we can't afford all the controls to avoid that issue therefore insurance is the way to go for the damage."

These findings suggest that individuals do understand that security controls and insurance are interdependent, but that they do not necessarily have a good mental model of how this interdependency works and/or an accurate perception of cyber risk. Individuals can approach cyber insurance from three positions. Firstly, they may see security and insurance as alternatives, with strong security measures negating the need for insurance coverage (and vice versa – raising concerns about moral hazard). Secondly, the relationship may be viewed as a trade-off with the level of security balanced against the level of insurance coverage, or thirdly, security and insurance may be seen as complimentary goods which both contribute to a strong cybersecurity position.

Some businesses, particularly SMEs, may not perceive cyber risk to be a significant issue for their business; often justified by statements about the business not being "mature enough" or "big enough to merit cyber insurance". Perceived self-efficacy also appears to play a role, with those who perceived themselves as knowledgeable and technologically 'savvy' reporting that they would be unlikely to take out cyber insurance. This suggests that greater awareness of cybersecurity may not necessarily lead to greater uptake of cyber insurance. Instead perceived self-efficacy could lead to a false belief that insurance is not necessary (i.e., they feel able to protect themselves).

> "Businesses just see it as a cost because they don't think any of these risks are ever going to materialise"

> "As a small business and being able to use the cloud, if we back up our data and rely on standard office-based stuff there is not that much to us, there is not a big attack area"

This could relate back to the potential for adverse selection and concerns that those who invest in cyber insurance may be those who perceive themselves as 'high risk'.

Financial constraints also influence the security investment trade-off, with limited budgets resulting in SMEs feeling 'priced out' of the insurance market by high policy premiums:

> "At the end of the day if you're paying out so much premium you just take the risk."

Some interviewees regarded this risk as a forced choice and necessity to get their small business off the ground:

> "[If] the cost of the controls exceeds the profit you're going to make and the cost of the insurance premium you know, you haven't got a business. I think a lot of people must arrive at that decision"

Recently, the UK National Cybersecurity Centre (NCSC) released technical guidance around cyber insurance, in a bid to "encourages organisations of all sizes to think about how insurance might help in the wake of a cyber-attack and contribute to existing risk management strategies" [27]. However, our findings suggest that adoption of cyber insurance is likely to occur at a later stage in business maturity and size, rather than being something that businesses adopt from the start. Policy premiums must be affordable for SMEs if initiatives to boost insurance adoption are going to be successful.

3.3 Lack of Risk Data and Immaturity of Cyber insurance

The lack of data on cyber risk makes it difficult for businesses to be able to measure and quantify their own risk. A general lack of awareness around cyber risk was articulated, and none of our interviewees had experienced a cyber insurance claim within their company(s) – indicating a lack of learned experience.

> "I have had conversations with the marketing people around what happens if we suffer a cyber-attack and… those were interesting and not conclusive they basically said we have no idea we have never had one. We can't get data from people who have had one"

Brokers and consultants perceived a lack of awareness as a particularly strong concern for smaller businesses as they felt SMEs were unable to accurately assess their cyber risk.

> "The threats are difficult to measure. […] generally speaking, the data is not available in organizations to make accurate decisions"

Reluctance to invest in cyber insurance may be linked to the immaturity of the insurance market itself. This concern was twofold: firstly, our interviewees queried how insurers are calculating premiums.

> The insurer will know how much a liability premium will be for a scaffolder because that might be 30 or 40 years of stats, cyber is a bit different because they haven't got the claims"

> "My observation is that people in insurance are not used to quantifying the risk that people are running and there's very little evidential base from an actuary point of view to justify what a premium is"

This supports recent research that suggests that, unlike other insurance sectors where risk assessment is based on quantitative actuarial data, cybersecurity risks currently rely upon qualitative risk matrices and subjective expert opinion [13]. Immature and subjective risk assessments also raise the potential for adverse selection if applicants withhold risk information from insurers (whether intentionally or accidentally).

Secondly, interviewees commented upon a lack of clarity around what cyber insurance policies include and exclude; further confounded by a 'grey area' between what is silently covered by traditional insurance and what falls under the remit of cyber insurance.

> "I mean insurance can't insure you against the GDPR fines you get. Or the fines wouldn't have any effect. So, I wonder whether people have looked at it [cyber insurance] and thought "well what are they going to pay for?" because I must admit, I did"

> "There is theoretically £500m [in electronic vouchers] there waiting for someone to steal it. When I asked if we were covered for that, the answer was that we would be covered under our crime insurance [not the cyber insurance]. Because it is a cash equivalent it is not covered under the cyber insurance policy."

> "I think there is an argument that the insurance industry needs to consult and make sure they know what a cyber risk is and what is a traditional risk. The only way I think they could do that is to put exclusions into the property damage but it's still a grey area."

There was also uncertainty around what insurers expect from insured parties, particularly what would constitute an acceptable level of cybersecurity within the business.

> "I'm definitely getting the impression that they expect us to get better and better and better at protecting our systems and data. Because the world is getting more dangerous, and hackers are getting more sophisticated. I'm not even sure if that's true to be honest. [...] I never get any affirmative whether this [security measures in the company] is good, or not enough. I am never clear, it's like a moving target and they are not capable of being transparent about it in a way that helps."

> "She [company lawyer] had it [cyber insurance policy] independently checked from an outside law firm and what she discovered – which we should have noticed but we didn't – is that we are not covered for any foreseeable risk. Unless we've disclosed it. So literally, if I thought that I had out of support operating systems that I was worried about and I have a plan in place to address this, but it wasn't finished yet. And we had a breach which was shown to have been caused by an intrusion on one of those out of support operating systems – we would not be covered for the breach. […] It's a complete minefield"

Interestingly, one business felt that even insurers are unsure what is an acceptable baseline for cybersecurity.

> "They [the insurance underwriters], the feeling I get is that as they've talking to the different companies […], nobody is doing everything that they wish they were doing. Everybody can describe all the things you should be doing. But I think they are probably struggling to establish what an acceptable baseline is. Everyone's different, and everyone's environment is different. […] So, I think they really struggle to know whether what you say you are doing is enough. And when you say, 'these are all the plans for what I'm going to do', I think they struggle to work out if that's acceptable and whether you are going fast enough."

This combined uncertainty can help to explain a reluctance to adopt insurance policies, and/or why businesses would rather spend their money on tangible security measures which they feel personally in control of, and/or feel they understand more:

> "That [security] control could last all you wanted to, or you could change that control as it's under your direct management"

Despite fundamental difficulties in quantifying cyber risk, companies reflected on being asked to do exactly that to obtain an insurance policy, i.e., to answer the various questions posed to them by insurers. This led to anxiety on behalf of the businesses and concerns around whether the insurance would be adequate and appropriate. Answering the questions on the policy form was even described as another 'risk'.

> "The questions they ask on the policy form it was difficult to quantify the impact of that, it could have been three million it could have been fifty million... So, it's an interesting one, yeah that was a risk to me"

> "At the moment I don't think people are confident they understand how to value their assets, therefore being able to have a robust conversation with the insurer."

Risk assessments were perceived as undoubtedly difficult (supporting recent findings by [28]), with one interviewee describing the yearly renewal process as "painful". It was suggested that risk assessments could be improved by focusing on how risk is measured. For example, by asking about risk in less technical terms. This was raised as particularly relevant for SMEs:

> "I don't think they [SMEs] would understand the technical risks, I think they would understand if you spoke about what assets you have got – I think if you spoke to people about trying to do a business continuity plan then saying what applications do you need back up – it's always quite hard to have that conversation with them […] If you structure the questions right you can [ask]... what are the systems you absolutely need – what is the biggest risk"

> "So, I think that is the thing for SMEs is how can they quantify the impact it's going to have on their business, I would use impact assessments rather than just risk assessments because it is far easier. What happens if you don't open your shop today – you know your shop could be online, well that's easy I lose business, how much business do you lose each day? You know, you can do that quite easily. But if you say what is the risk of your website going down, that is really hard to quantify"

These findings highlight how cyber insurance is currently a double-edged sword due to a lack of data and tools to enable accurate risk assessment. This leads to increased premiums by the insurers, and doubt and anxiety for businesses. Despite fundamental difficulties in accurately quantifying cyber risk, this information is demanded from businesses to obtain a policy. Improved access to cyber risk data is a necessity.

3.4 Mistrust of Insurers

Some interviewees expressed negative views of insurance companies including doubts around the intention of insurers and the likelihood of paying out. Interviewees perceived insurers as using complicated policy wording and exclusions to their advantage, i.e., to find a way to not pay claims:

> "One of the key reasons I am not an advocate of insurance policies is there is always a way of not paying out"

> "I feel like – anybody that I talk to in the cybersecurity industry feels that cyber insurance is a joke and that it never pays out"

> "I mean the most important factors for me would be being transparent about what they cover and not having lots of caveats, so you can have confidence.

One interviewee described how there can be confusion over whether some crimes are covered by cyber insurance, for example Phishing attacks.

> "They [some insurers] see fishing and social engineering is more traditional fraud it's just undertaken by electronic means. […] They'll cover it but under the crime policy not the cyber policy"

This aligns with recent findings by Wrede et al. [40], who carried out a content analysis of cyber insurance terms and conditions and conducted a qualitative study with German insurance experts to investigate silent cyber coverage. This refers to risks arising "from implicit cyber exposure within 'all risks' and other liability insurance policies that do not explicitly exclude cyber risks" [41]. Therefore, silent cyber coverage can result in claims being made that insurers have not underwritten. Wrede et al. concluded that policy wording was imprecise and failed to include sufficient descriptions of the contractually specified insurance coverage.

Despite these concerns, a recent report by the Association of British Insurers (ABI) conducted a survey of 207 insurance claims made in 2018 and found 99% (205) had received a pay-out [1]. One interviewee explained that they perceive insurers to use vague wording in policies as a method of future proofing, rather than to purposefully mislead or provide potential loopholes to deny a pay-out. As the cyber industry and technology evolves so quickly, insurers may avoid being too specific in their policy wording as this would require almost constant updates as technology progressed. A degree of 'vagueness' enables policies to be more long-lasting. However, there needs to be a level of specificity to provide some clarification, and reassurance, for insured parties. This is an interesting tension to be addressed.

Media coverage was also identified as a potential reinforcer of mistrust in cyber insurance. For example, some interviewees referred to the NotPetya ransomware attack on Mondelez International (the company that owns Cadbury). After initially offering a $10 million pay-out, insurance company Zurich later decided to reject the insurance claim after declaring the cyber-attack an 'act of war' [25]. At the time of the interviews, Mondelez International was taking legal action against Zurich – in the first legal dispute over a cyber insurance claim [4].

> "It gets a lot of media attention. For example, the chocolate company that are suing their cyber insurance company that won't pay out over NotPetya as they're classifying it as an act of war. When its reported in the type of stuff that the industry looks at... because we're all already quite cynical about cyber insurance... the reporting comes across biased, quite cynical. It's like 'we all knew it was true and look now it's happening [the insurance isn't paying out]"

> "The company, Cadburys or something like that, it is out there in public domain they are taking legal action against Zurich because they won't pay the claim."

This suggests that media coverage around cybersecurity could be a double-edged sword. On one hand it could potentially have the positive effect of increasing awareness of cyber risk. On the other hand, it may also reinforce negative perceptions of cyber insurance. Our findings suggest that there is significant work to be done on reassuring businesses that cyber insurance is worth investment.

3.5 Compliance Legislation as a driver for cyber insurance adoption

Our interviewees identified many barriers to insurance adoption; however, they also identified a key driving factor promoting uptake - compliance with legislation. This is in keeping with existing research suggesting that investment in information security is largely driven by external environmental and industry-related factors, including legal regulations and industry-specific demands and requirements [10,20,38].

> "The scale of potential liability under GDPR I think to some extent that might move the market more than cybersecurity because if you're trying to cost something you need a clear regulatory burden"

One of the insurance brokers we interviewed described an increase in insurance uptake following the introduction of the GDPR.

> "Last year there seemed to be a bit more purchase but GDPR seemed to be the trigger having said that is has quietened down a bit lately."

This echoes recent findings that suggest that the GDPR not only influenced decision-making at the basic level of whether to invest or not, but also what areas to invest in and the level of investment [20]. This could be due to the introduction of legislation helping to quantify risk, e.g., if there is a data leak you will be fined a considerable amount of money. However, the interviewee in our study also commented that the effect of the GDPR on cyber insurance purchasing was already showing signs of decreasing. This suggests that cyber insurance (and cybersecurity more generally) may be affected by recency effects, e.g., risk being perceived as higher for threats recently in the public eye (in this instance the introduction of the GDPR and potential to incur fines for non-compliance).

> "A lot of the decisions I would still say would be based on people's subjective views and you get influences such as recency and all of those other things if you had an incident a week ago and you ask someone what their risk, for a certain risk would be. They would probably raise it harder than before – So what is happening and what has still been going on is I would say the main thing."

Some of the interviewees expressed concern that even when insurance is adopted, this may be simply a perfunctory 'tick box' exercise to "*look as if you are covered"* [and therefore complying to legislation]. They expressed doubts that insurance would provide adequate coverage, i.e., that the pay-out would be enough to cover the damages caused in the event of a cyber-attack.

> "You get some things to look as if you have covered."

These findings illustrate that regulation and legislation as a driver for cyber insurance uptake may be effective, providing there are steps in place to ensure that insurance coverage is sufficient.

4 DISCUSSION

Our findings show that the internal decision-making process at company level involves a complex ecosystem (in keeping with previous research, e.g., [21]). These systems often vary significantly between companies, and can be influenced by business size, maturity, and sector. There is not a universal 'one size fits all' cybersecurity structure. Internally to the company there are many different processes also influencing these decisions – including a complex, non-universal, structure across many different boards, committees, teams, and departments. Each reflecting their own motivations,

priorities, and processes. Priorities and perceived threats may also differ between staff members, boards, committees, and departments. Even within the same company, different security-related decisions may be driven by different departments, teams and/or factors. For example, cyber insurance adoption often seems to be driven from outside of the technical teams (for example from finance). This complexity can make the internal decision-making process time-consuming. Recent work by the NCSC includes a cybersecurity toolkit for Boards to help businesses manage cybersecurity related discussions and decisions [44]. However, there is still work to be done in this area, and the complexity of internal processes may raise issues for parties marketing cyber insurance and aiming to identify which staff and departments to approach.

Recently we have seen increased governmental emphasis upon cybersecurity and cyber insurance. For example, in the US, President Joe Biden has pledged to "make cybersecurity a top priority at every level of government" and "elevate cybersecurity as an imperative across the government, further strengthen partnerships with the private sector, and expand […] investment in the infrastructure and people we need to defend against malicious cyber-attacks" [24]. The Biden administration could require all governmental vendors to have cyber insurance in place. Furthermore, the U.S Cyberspace Solarium Commission [43] has called for the development of cyber insurance certifications - to encourage uptake of cyber insurance and improved cybersecurity posture, across both public and private sectors. Similar developments have been seen in the UK, for example the Government Cyber Security Strategy [46] has recently been introduced; this strategy runs until 2030 and aims to significantly improve the government's resilience to cyber-attacks. These initiatives recognize that widespread uptake of cybersecurity measures can increase cybersecurity resilience at the wider level - not only across the organization or sector, but on a wider societal level. For example, in the recent UK integrated review of security, defence, development and foreign policy [47], the government describes its aim of establishing a 'whole-of-society' approach to resilience. However, such initiatives will only be successful if barriers to cyber insurance adoption are understood and addressed.

Financial restrictions clearly pose a key barrier to insurance uptake, especially for SMEs who describe a difficult trade-off between security and keeping their business running. For many businesses, there are financial restraints on the budget available for cybersecurity – and this will often be split between cybersecurity protection measures and insurance. If premiums are regarded as too costly, businesses may opt to, or feel forced to, take the risk of being uninsured and rely solely on self-protection measures. Recently, there has been a push for those in the insurance industry to use the COVID-19 pandemic as an opportunity to engage with the SME market. For example, by emphasizing business reliance upon technology and the potential debilitating impact of a cyber-attack [17]. However, increased awareness may not be sufficient if policy premiums remain cost prohibitive.

The process of applying for cyber insurance was highlighted as another barrier to uptake due to being perceived as complicated and effortful (supporting findings by [38]). Businesses find it difficult to answer the questions posed by insurers in order to obtain a policy. Even when a policy, or quote, was obtained, businesses felt unable to assess whether the coverage would be sufficient to cover the losses if a cyber-attack was experienced. Other barriers to uptake included a distrust of insurers paying out in the instance of a cyber-attack; a concern compounded by unclear wording of insurance policies, perceived 'grey areas' in coverage and media coverage of unpaid claims. To facilitate uptake, policy wording needs to be easier for businesses to understand, and data or processes need to be available to help businesses adequately and effectively assess their own cyber risk and the impacts an attack could have upon their business (including financial and reputational impacts). Improved transparency regarding policy coverage – and insurers ongoing expectations of the insured party - could help to boost confidence in cyber insurance products. Standardization of policy wording could potentially help to address confusion over coverage and help to clarify the 'grey area' between traditional insurance and cyber insurance.

Our findings support recent work suggesting that cyber insurance is still lacking solid methodologies, standards and tools to quantify risk [13]. The sharing of data in a collaborative fashion between insurers has been recommended as a way to address these concerns, i.e., the creation of a shared dataset between all industry parties to help guide cyber insurance decisions. However some research suggests this may not be favorable with all parties – particularly if some feel this will disadvantage their competitive edge as one of the market leaders and/or lower barriers to competitors entering the market [28]. Future work needs to investigate how this issue can be addressed.

Legislation was identified as a potential facilitator of insurance uptake. In keeping with recent research [38], our findings suggest that there may be a disconnect between past literature regarding security decision making as intrinsically motivated, and the emerging literature that shows that companies may be more motivated to invest in security because they are required to comply with legislation. Legislation as a driver for cyber insurance fits with a theoretical model proposed by Burke and Litwin [9], which suggests that the most dominant factor on organizational performance and change is the external environment. In much the same way, we show that in relation to cybersecurity decision-making in companies, external factors appear to have a strong influence.

5 CONCLUSIONS

In summary, despite significant cyber risk and increasing awareness, uptake of cyber insurance remains low. Businesses are discouraged by high policy premiums, complicated and effortful risk assessments and exclusions – leading to a lack of confidence in policy suitability, and mistrust of insurers regarding pay-outs in the event of an incident. Legislation may help to increase uptake, but data and improved risk assessment procedures are still required to enable tailored policy pricing and ensure that policies offer appropriate coverage. Clearer policy terms and conditions could help to improve confidence in coverage and likelihood of receiving a pay-out following a cyber-attack. Tackling the data void remains the key to addressing tensions between insurers and businesses. Doing so, could increase cyber insurance adoption with positive implications for security at the organisational and societal level.

ACKNOWLEDGEMENTS

This research was funded by the European Union's Horizon 2020 research and innovation programme under the CYBECO grant agreement No 740920.

REFERENCES

[1] ABI. 2019. *Cyber insurance payout rates at 99%, but uptake still far too low*. Retrieved February 4, 2021 from https://www.abi.org.uk/news/news-articles/2019/08/cyber-insurance-payout-rates-at-99-but-uptake-still-far-too-low/

[2] AON. 2017. *Global Cyber Risk Transfer Comparison Report*. Retrieved January 21, 2021 from https://www.aon.com/risk-services/thought-leadership/2017-global-cyber-risk-transfer-comparison-report.jsp

[3] AON. 2017. *Global Cyber Market Overview*. AON.

[4] Robert Armstrong and Oliver Ralph. 2019. Mondelez sues Zurich in test for cyber hack insurance. *Financial Times*. Retrieved February 5, 2021 from https://www.ft.com/content/8db7251c-1411-11e9-a581-4ff78404524e

[5] B. Aziz, Suhardi, and Kurnia. 2020. A systematic literature review of cyber insurance challenges. In *2020 International Conference on Information Technology Systems and Innovation (ICITSI)*, 357–363. DOI:https://doi.org/10.1109/ICITSI50517.2020.9264966

[6] Jean Bolot and Marc Lelarge. 2009. Cyber Insurance as an Incentive for Internet Security. In *Managing Information Risk and the Economics of Security*, M. Eric Johnson (ed.). Springer US, Boston, MA, 269–290. DOI:https://doi.org/10.1007/978-0-387-09762-6_13

[7] Dawn Branley-Bell, Yolanda Gómez, Lynne Coventry, José Vila, and Pam Briggs. 2021. Developing and Validating a Behavioural Model of Cyberinsurance Adoption. *Sustainability* 13, 17 (January 2021), 9528. DOI:https://doi.org/10.3390/su13179528

[8] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3, 2 (January 2006), 77–101. DOI:https://doi.org/10.1191/1478088706qp063oa

[9] Warner. W Burke and George. H Litwin. 1992. A Causal Model of Organizational Performance and Change. *Journal of Management* 18, 523 (1992). DOI:https://doi.org/10.1177/014920639201800306

[10] E Chew, M Swanson, K M Stine, N Bartol, A Brown, and W Robinson. 2008. *Performance measurement guide for information security*. Gaithersburg, MD. DOI:https://doi.org/10.6028/NIST.SP.800-55r1

[11] Alma Cohen. 2005. Asymmetric Information and Learning: Evidence from the Automobile Insurance Market. *The Review of Economics and Statistics* 87, 2 (May 2005), 197–207. DOI:https://doi.org/10.1162/0034653053970294

[12] Alma Cohen and Peter Siegelman. 2010. Testing for Adverse Selection in Insurance Markets. *Journal of Risk and Insurance* 77, 1 (2010), 39–84. DOI:https://doi.org/10.1111/j.1539-6975.2009.01337.x

[13] S. Dambra, L. Bilge, and D. Balzarotti. 2020. SoK: Cyber Insurance – Technical Challenges and a System Security Roadmap. In *2020 IEEE Symposium on Security and Privacy (SP)*, 1367–1383. DOI:https://doi.org/10.1109/SP40000.2020.00019

[14] John II S. Davis, Martin C. Libicki, Stuart E. Johnson, Jason Kumar, Michael Watson, and Andrew Karode. 2016. *A Framework for Programming and Budgeting for Cybersecurity*. RAND Corporation Santa Monica United States. Retrieved January 21, 2021 from https://apps.dtic.mil/sti/citations/AD1002054

[15] Wanchun Dou, Wenda Tang, Xiaotong Wu, Lianyong Qi, Xiaolong Xu, Xuyun Zhang, and Chunhua Hu. 2020. An insurance theory based optimal cyber-insurance contract against moral hazard. *Information Sciences* 527, (July 2020), 576–589. DOI:https://doi.org/10.1016/j.ins.2018.12.051

[16] Eleanor Vaida Gerhards. 2018. Cybersecurity insurance: popular but poorly understood. *Property Casualty 360*. Retrieved January 21, 2021 from https://www.propertycasualty360.com/2018/07/10/cybersecurity-insurance-popular-but-poorly-understood/

[17] GlobalData. 2020. *2020 UK SME Insurance Survey*. Retrieved February 4, 2021 from https://www.actuarialpost.co.uk/article/cyber-insurance-uptake-remains-low-from-smes-18763.htm

[18] Andrew Granato and Andy Polacek. 2019. The Growth and Challenges of Cyber Insurance. (2019). DOI:https://doi.org/10.21033/cfl-2019-426

[19] Benjamin R Handel. 2013. Adverse Selection and Inertia in Health Insurance Markets: When Nudging Hurts. *American Economic Review* 103, 7 (December 2013), 2643–2682. DOI:https://doi.org/10.1257/aer.103.7.2643

[20] Margareta Heidt, T U Darmstadt, Jin P Gerlach, and Peter Buxmann. 2019. A Holistic View on Organizational IT Security: The Influence of Contextual Aspects during IT Security Decisions. In *52nd Hawaii International Conference on System Sciences*. Retrieved from https://hdl.handle.net/10125/60049

[21] David Rios Insua, Caroline Baylon, and Jose Vila. 2020. *Security Risk Models for Cyber Insurance*. CRC Press.

[22] Nir Kshetri. 2020. The evolution of cyber-insurance industry and market: An institutional analysis. *Telecommunications Policy* 44, 8 (September 2020), 102007. DOI:https://doi.org/10.1016/j.telpol.2020.102007

[23] M. Lelarge and J. Bolot. 2009. Economic Incentives to Increase Security in the Internet: The Case for Insurance. In *IEEE INFOCOM 2009*, 1494–1502. DOI:https://doi.org/10.1109/INFCOM.2009.5062066

[24] Asaf Lifshitz. 2021. Five ways the Biden administration could impact cyber insurance. *PropertyCasualty360*. Retrieved May 30, 2022 from https://www.propertycasualty360.com/2021/01/20/five-ways-the-biden-administration-could-impact-cyber-insurance/

[25] Nicole Lindsey. 2019. Cyber Insurance Not Valid in Case of Cyber War, Says Major Insurance Company. *CPO Magazine*. Retrieved February 1, 2021 from https://www.cpomagazine.com/cyber-security/cyber-insurance-not-valid-in-case-of-cyber-war-says-major-insurance-company/

[26] David de Meza and David C. Webb. 2001. Advantageous Selection in Insurance Markets. *The RAND Journal of Economics* 32, 2 (2001), 249–262. DOI:https://doi.org/10.2307/2696408

[27] NCSC. 2020. We've got you covered: experts produce first-ever technical advice on cyber insurance. Retrieved February 5, 2021 from https://www.ncsc.gov.uk/news/experts-first-advice-on-cyber-insurance

[28] J. R. C. Nurse, L. Axon, A. Erola, I. Agrafiotis, M. Goldsmith, and S. Creese. 2020. The Data that Drives Cyber Insurance: A Study into the Underwriting and Claims Processes. In *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, 1–8. DOI:https://doi.org/10.1109/CyberSA49311.2020.9139703

[29] D. L. Pain, J. Anchen, M. Bundt, E. Durand, M. Schmitt, and C. Bieck. 2016. *Cyber: In search of resilience in an interconnected world*. Zurich. Retrieved February 16, 2021 from https://www.swissre.com/dam/jcr:30b64544-9514-4389-aaf1-13fb74f51eab/ZRH-16-09789-P1_Cyber+Publication_web.pdf
[30] Sasha Romanosky, Lillian Ablon, Andreas Kuehn, and Therese Jones. 2019. Content analysis of cyber insurance policies: how do carriers price cyber risk? *Journal of Cybersecurity* 5, tyz002 (January 2019). DOI:https://doi.org/10.1093/cybsec/tyz002
[31] Michael Rothschild and Joseph Stiglitz. 1978. Equilibrium in Competitive Insurance Markets: An essay on the economics of imperfect information. In *Uncertainty in Economics*, Peter Diamond and Michael Rothschild (eds.). Academic Press, 257–280. DOI:https://doi.org/10.1016/B978-0-12-214850-7.50024-3
[32] Peter Siegelman. 2003. Adverse Selection in Insurance Markets: An Exaggerated Threat Essay. *Yale L.J.* 113, 6 (2004 2003), 1223–1282.
[33] Joseph E. Stiglitz. 1977. Monopoly, Non-Linear Pricing and Imperfect Information: The Insurance Market. *The Review of Economic Studies* 44, 3 (1977), 407–430. DOI:https://doi.org/10.2307/2296899
[34] Guy Thomas. 2017. *Loss Coverage: Why Insurance Works Better with Some Adverse Selection*. Cambridge University Press.
[35] Murray Turoff and Linda Plotnick. 2012. The ISCRAM Future Threat Delphi: Nostradamus Revisited. In *ICSRAM*. Retrieved from http://iscram.org
[36] Ganbayar Uuganbayar, Artsiom Yautsiukhin, Fabio Martinelli, and Fabio Massacci. 2021. Optimisation of cyber insurance coverage with selection of cost effective security controls. *Computers & Security* 101, (February 2021), 102121. DOI:https://doi.org/10.1016/j.cose.2020.102121
[37] Shaun S. Wang. 2019. Integrated framework for information security investment and cyber insurance. *Pacific-Basin Finance Journal* 57, (October 2019), 101173. DOI:https://doi.org/10.1016/j.pacfin.2019.101173
[38] Eva Weishäupl, Emrah Yasasin, and Guido Schryen. 2018. Information security investments: An exploratory multiple case study on decision-making, evaluation and learning. *Computers & Security* 77, (August 2018), 807–823. DOI:https://doi.org/10.1016/J.COSE.2018.02.001
[39] Daniel Woods and Andrew Simpson. 2017. Journal of Cyber Policy measures and cyber insurance: a framework Policy measures and cyber insurance: a framework. (2017). DOI:https://doi.org/10.1080/23738871.2017.1360927
[40] Dirk Wrede, Tino Stegen, and Johann-Matthias Graf von der Schulenburg. 2020. Affirmative and silent cyber coverage in traditional insurance policies: Qualitative content analysis of selected insurance products from the German insurance market. *Geneva Pap Risk Insur Issues Pract* 45, 4 (October 2020), 657–689. DOI:https://doi.org/10.1057/s41288-020-00183-6
[41] 2016. *Consultation Paper: Cyber insurance underwriting risk*. Bank of England Prudential Regulation Authority. Retrieved March 23, 2021 from https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/consultation-paper/2016/cp3916
[42] 2019. *Cyber Security Breaches Survey*.
[43] 2020. *Cyberspace Solarium Commission Executive Summary*. U.S. Cyberspace Solarium Commission. Retrieved May 30, 2022 from https://drive.google.com/file/d/1c1UQI74Js6vkfjUowI598NjwaHD1YtlY/view?usp=embed_facebook
[44] 2021. *Cyber Security Toolkit for Boards*. National Cyber Security Centre. Retrieved May 30, 2022 from https://www.ncsc.gov.uk/section/board-toolkit/home
[45] Cyber Security Breaches Survey 2022. *GOV.UK*. Retrieved May 20, 2022 from https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022
[46] *Government Cyber Security Strategy: 2022 to 2030*. GOV.uk. Retrieved May 30, 2022 from https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030/government-cyber-security-strategy-2022-to-2030-html
[47] *Global Britain in a competitive age. The integrated review of security, defence, development and foreign policy.*