SEPTEMBER 2022

ISUNA

White Paper

Cyber Insurance: Multi-Stakeholder Challenges and Solutions

IN COLLABORATION WITH ISUNA AND PII

ISUNA

PEACE INNOVATION INSTITUTE
THE HAGUE

Introduction

In 2021, the average cost of a cybercrime breach was 4.24 million GBP (€ 4.83 million) [1]. This high and increasing number stems from the interconnected nature of stakeholders that operate within a companies' digital space. All stakeholders are affected during a cyber-attack; ranging from employees and entrepreneurs, to consumers, third parties, providers, etc [2].

The growing level of damage cybercrime can cause, and the continued dependence on technology for daily livelihood has led to the development of the cyber insurance market [3], [4]. Starting in the 1990s as a liability driven insurance, the cyber insurance market is currently one of the fastest growing industries. Currently the cyber insurance sector is estimated to hold around 2000 - 3000 unique cyber policies and the entire market is projected to be worth $20.4 billion (€ 20.35 billion) by 2025 [5],

Yet in the Netherlands, the 2021 estimated industry value was set at €36 million [7]. The disparity between the exponentially growing global figure and the Dutch market eludes to the impact of unique challenges the market faces. The largest identified include a lack of a shared taxonomy, availability of data, issues in clarity of insurability, and accurate pricing risks [4], [5], [8], [9]. Based on current research, two encompassing solutions exist that grip the foundations of these challenges.

These include improving transparency, and accessibility to data. Herein, there is a clear need to lay out the risks of the different stakeholders in the market and transition towards a space with accurate information that improves the entire cyber insurance sector.

The Current Picture on Transparency

Transparency is one of the key factors that helps enable accurate coverage mechanisms within cyber insurance [9]. Cyber risk carriers are one of the few stakeholders in the market that have the best information surrounding cyber risk practices [2], [5]. Information possessed by cyber risk carriers is asymmetric to entrant (re)insurance companies, and other stakeholders [5], [10]. Given the competitive nature of the market, individual stakeholders have different incentives to retain or share information.

This in turn reduces the overall quality of risk management and increases the total market costs in cyber insurance —both in operational costs in developing accurate pricing mechanisms, and in loss scenarios (re)insurers did not anticipate [9], [11]. Furthermore, the lack of (coherent) public information about how risk is (and should be) assessed within cyber insurance from policy and regulations leaves (re)insurance companies unclear on the best course of action for risk management and pricing premiums [5]. Intermediary organizations such as the Dutch Association of Insurers try to fill this gap. In this issue, the lack of public information blurs [1] the clarity of what is excluded and included within risk coverage packages [4], [9].

As privacy regulations increase, data sharing decreases, this creates an inaccessibility to data useful to improving the quality of risk management, market wide; such as the assessments of company risk profiles [5], [9].

The inaccessibility and unavailability of data for decision-makers, like (re)insurers, in combination with the general lack of awareness and education the companies face hinders overall adoption of cyber insurance and good cybersecurity measures [1], [5], [9].

Isuna and Transparency

The Isuna platform aims to remove the barriers of asymmetric information between market actors —client companies, insurance companies, policymakers, underwriters— by offering services that collect data on managing cyber security better and more personally.

Within the cyber insurance market our entrance commences through building subject matter expertise and knowledge within the sector. This will help us to build effective partnerships with key stakeholders from the insurance sector and the wider market. With the Peace Innovation Institute we want to help stakeholders to increase their cooperation and value generation.

This can be achieved by greatly increasing the knowledge from within the sector, clarity of products and the wider availability of cyber resilience capability and security awareness. Our approach has been validated by subject matter experts, our compliance partners NEN and is supported by the EU via Kansen voor West [12], [13].

In this paper we explore the cyber insurance market focusing on encompassing challenges the market faces, and how the Isuna approach can increase the value proposition of improving transparency and data accessibility to reduce market costs of our prospective partners, as explored in our first white paper for general insurance companies.

Section 1: General Overview of Cyber Insurance

Cyber insurance regards a niche insurance branch intended to protect companies and/or individuals from risks that are related to internet technologies. A multitude of stakeholders influence the cyber insurance industry and shape the developing form and structure. The largest identified stakeholder groups include: policy, internet service providers, government, (re)insurance companies, underwriters, SME associations, and businesses seeking cyber protection [9], [14]–[16].

Currently, the top 5 of the biggest companies operating within the cyber insurance sector include:

1. Hiscox
2. Chubb
3. The Hartford
4. AIG
5. CAN [4], [17].

Coverages

Cyber insurance has limited but general coverage featured across four lines of business:

- Property,
- Liability,
- Crime and fidelity,
- Kidnap and ransom [9], [18].

A majority of these coverages can be found within the areas, property and liability [9]. The areas of threat that carriers of risk cover are generally found in the following six categories:

- Data confidentiality breaches,
- Network security liability,
- Communication and media liability,
- Technology disruptions,
- Cyber extortion,
- Cyber fraud and theft [9].

Within these areas 86% of breaches were motivated under financial reason is and 10% under espionage [19]. While these areas of threat incorporate over 40 recognized insurance products; over the recent decades these products have been formalizing into a more cohesive product categorized into two areas:

- Stand-alone cyber insurance —one risk application,
- Packaged cyber insurance —broad risk applications [20].

What is excluded from coverage criteria remains to an extent vague, cyber terrorism, and politically motivated attacks falls under a different coverage criteria that require different coverage mechanisms [9], [21], [22]. Next, within property insurance policies, coverage of data loss can be excluded as data in some cases is viewed as an intangible asset [9].

Assessment

For a cyber insurance company to build the mechanisms that operate across lines of business and areas of threat, questionnaires (identified between 26 - 70 questions) are used to assess the company's status and develop a risk profile [5]. The questionnaire scores the necessary areas where coverage is appropriate and where coverage can be improved [5]. Within these risk assessments four general categories are defined:

- Organizational processes,
- Technical processes,
- Policies and procedures,
- Legal and compliance factors [5].

A general lack of awareness exists on the importance of cyber security. With the slow movement of governing bodies and respective institutions, their response has been somewhat inadequate to keep up with the rate at which cybercrime occurs, at a cost of nearly $1 trillion in 2020 (€ 997 billion) [23].

This creates an added layer of uncertainty and imbalance between the stakeholder groups of (re)insurance companies, and policy actors leaving businesses open to seeking protection to an extent, vulnerable [9].

Section 2: The Market Structure

Looking at an interactions-based model, Bohme and Schwartz (2010) provide a good theoretical model of the cyber insurance market. The key features of this model help explain why issues identified in cyber insurance exist. Five components outline the market structure, these follow as:

1. The Networked Environment: ICT operates within an interconnected network, this differs from conventional business as their physical value is dependent on the interconnections (social, logical, and physical) [10]. Businesses on the demand side for cyber insurance both are influenced and influential over these interconnections [10]. The interconnections uniquely shape the risk analysis process as risk assessment can not be conducted in isolation of its interdependencies [10].

2. The Demand Side: referred to as agents, those seeking insurance,

3. The Supply Side: those supplying insurance, (re)insurance companies,

4. Information Structure: the (incomplete and asymmetric) information that is distributed across different actors in the market,

5. Organizational environment: the stakeholders relevant in contexts of policy whose decisions have influence over agent cyber security decisions [10].

The existence of the cyber insurance market occurs when there is an increased likelihood of large losses, and the client is of high risk [11]. Within this understanding, there is a necessity for recognition of externalities that occur as a result of *security decisions* (interdependent security), *the correlated risk of common vulnerabilities shared between networks*, and the *asymmetric information within the structure of the network* [10]. These three obstacles affect the structural operation of the market.

This leads to (re)insurer inaccuracy in distinguishing client (agent) risk profiles to provide proper coverage mechanisms [5], [9]. Herein, (re)insurers must evaluate different drivers of business activity (i.e. examining supply chain transactions vs. sensitivity of managed data) [24]. The high level of interactions and integrations proposes a unique obstacle to the cyber insurance market.

Herein, the social and organizational knowledge that surrounds interaction is fueled by asymmetric information. This limits the quality across all dimensions of the market from the company, the (re)insurer, the cyber security product, the individual who made the cyber security product [25]. The extent of harm produced by the product and the limited knowledge of the individual who created the product is that a hacker, once cracking the system, can repeatedly conduct malicious behavior as the product is dominant across the industry [25]. Social and organizational asymmetric information prevents companies and (re)insurers from overcoming their common obstacle the hacker introduces [25].

This means, according to the network of the prototype —including the embedded networked knowledge of the actor— information asymmetries exist [25]. Thus, different threats dependent on their class have differing extents of impact and approaches the cyber insurance market can take. To give context, spam mail thrives often in what is known as a “homogeneous network class” [25].

Spam mail spreads across operating systems of installed platforms that are often identical as a result of market dominance, the consequences of spam mail affect differently

than in the event of a company-wide hardware failure. The different nature of these events requires different cyber insurance strategies [25]. This sheds light on the breadth of range a cyber insurance company needs to explore to value the common vulnerabilities within distributed systems [25].

Stakeholders Within The Market

At a structural level, differing key stakeholder groups attain differing levels of agency —their ability to establish and implement change [26]. Agent power is relative to the institutional makeup of the country and region, and thus, cyber insurance responses are indicative of the means by which a national context conducts business [26].

This organizes a series of constraints (re)insurers adhere to in each context [25]. Here, (re)insurers are inclined to navigate policies that create mutually beneficial relationships and create pathways that promote or undermine cyber insurance transparency and accuracy. The current largest stakeholders and their pain points are identified:

1. Policy/ Government/ Regulatory Actors
   a. Lack of public information shared
   b. Vague language use

2. Underwriters
   a. Unclear on insurability - exclusion/ inclusion
   b. Unclear pricing strategies

3. (Re)insurers
   a. Unclear on insurability, what is insured, what isn't
   b. Unclear pricing strategies

4. Companies seeking protection
   a. How to be cyber secure
   b. Entering NDA agreements that incur fear
   c. Lack of knowledge and understanding
   d. Lack of awareness

5. Managed Service Providers
   a. No link to insurers
   b. Lack of communication with other stakeholders [5], [9], [16], [27].

Section 3: Challenges

A Shared Taxonomy & Clarity on Insurability

Many insurance companies are uncertain about the extent to which exclusions can be applied across the different classes of threats [9]. Current implementation of public policy measures are vague in language and use differing language across different policies [5]. The output of policy creates questionable outcomes for (re)insurer coverage actions [9]. Underwriters are challenged with deciphering the risks within the vagueness of public policy and leads to questioning the accuracy of quantified risk [9], [27].

This reveals the opportunity for governments to develop more explicit expectations from the cybersecurity and cyber insurance industry to assist in making the scope for underwriters more concrete [9]. For example, a shared taxonomy would prove beneficial between active stakeholders in the market surrounding the insurability of fines set by the General Data Protection Regulation (GDPR) [9]. Currently, (re)insurance companies will reimburse GDPR issued fines based on the reputational risk incurred towards themselves [9].

In order to create more grounded decisions the OECD outlines three components that prevent the creation of a shared taxonomy, these include:

1. Policy language generally lacks conformity in definitions and exclusionary criteria regarding cyber risk,

2. Governments lack clear statements within their jurisdiction on the insurability of:
   a. Fines
   b. Penalties
   c. Ransoms
   This impacts risk for (re)insurers in their ability to cover for uninsurable losses,

3. Governments lack clarification of responsibilities of (re)insurance companies in their extent of compliance to adopted sanctions and public policy measures [9].

Availability of Data

In response to clarity in taxonomy and enhancing the clarity on insurability, a large risk underwriters face is making informed decisions about accurate coverage and predictions for loss events to not incur a negative value [11]. The lack of available data that can be shared between (re)insurance companies leads to market wide insufficient knowledge about past claims, resulting in less accurate pricing of premiums, slowing efficiency [27].

Furthermore, within cyber insurance, the leading, largest companies benefit from their access to large pools of past incident and claims data. They maintain a competitive advantage by selectively choosing with which circle to share this information [27]. Governments encourage insurers to engage in “horizontal cooperation agreements” that share large incident and claims data, to overcome issues in market dominance [27]. However, a series of external restrictions prohibit this [27].

Firstly, the field is new, there is a general lack of knowledge and expertise in such a vastly growing industry [27].

Secondly, (re)insurance companies may be constricted by non-disclosure agreements with policyholders and thus unable to share data [27].

Thirdly, privacy of data and sensitivity of data may further prohibit sharing [27]. Given the evolving nature of the field, keeping up with antitrust legislation, and encouraging unwilling (re)insurance companies already established in the market to share data may prevent the development of the larger market [27]. This limits the ability for new entrants to pave a successful route creating wider issues of accessibility to cyber insurance [27].

Pricing Risks

Pricing accurate premiums has been one of the largest challenges throughout the expansion of the cyber insurance market. Insurance companies are motivated to uncover a certain level of transparency that allows for the premium pricing to have a profitable margin that does not incur negative value in the scenario of a loss event [11].

Multiple reasons affect pricing accuracy, one of the first is stakeholder incentives; underwriters for cyber insurance use their knowledge of pricing as intellectual property (IP) as a means to maintain leverage in the seniority of their position [27]. This gives underwriters a competitive edge that helps them perform better in the market than other competitors. Their ability to retain that information and share only within small circles allows for a competitive edge. This retainment may increase uneducated and uninformed behavior by potential and current clients resulting in further loss events [11], [28].

Where companies seeking cyber protection face issues of education, the entire market suffers. Thus, a systematic literature review by Romanovsky et al., (2019) identified the current strategies cyber (re)insurers use to price risks:

- Looking at external sources
- Guessing and estimation
- Looking at competitors
- Relying on their own underwriting experience
- Adapting the prices from other insurance lines [5].

Within these strategies (re)insurance carriers assess company clients through multiple lenses prioritizing different business aspects such as industry type, turnover, sensitivity of data dealt with, etc. This in turn is linked to attached rates, either a flat rate or base rate, then attach security questionnaires or link the flat rate to hazard groups [5]. The significant variation in strategy, and lack of basis on concrete information helps to explain the instability of quality risk management across the market. The energy spent creating different pricing mechanisms incurs higher costs than working towards shared data and transparency.

Conclusion: Transparency as an encompassing solution & Isuna

This white paper aims to show that despite the cyber risks and threats there are many opportunities for stakeholders to increase the value they provide to businesses. This value can be in the shape of effective, understandable, and complete cyber insurance. Our research shows room for wider linked solutions that connect the stakeholders with clients and products to the cyber security supply chain.

For example, an insurance provider is a key stakeholder that benefits from the increased resilience of their clients and as such the clients should be able to align their complete cyber requirements against a trusted supplier list.

Our current focus is upon cyber security and data privacy. With our partner NEN, we have developed a secure digital Platform that helps businesses assess their cyber proposition and plan improvements that will help them comply with ISO27001, ISO27701 and data privacy regulations such as GDPR and AVG in the Netherlands. Our joint research corroborates many of the challenges that are faced by the insurance sector and their clients, these include:

- Lack of comparable data to ensure the solutions (including insurance) are appropriate for the business,
- Complex technical language that is difficult to understand and then apply to the business,
- Closed service options that effectively disrupts valuable information and intelligence sharing,
- Disparate tools and solutions that are not scalable or applicable to the business or sector,
- Duplication of tools or effort that results in decreased efficiency and higher costs.

We worked closely with our partners and subject matter experts to develop the understanding of the issues and to develop an effective solution. However, we know that we are part of the wider solution and as such must build communication channels and partnerships to ensure that we can resolve the challenges and build cyber safe environments for businesses.

Our platform helps clients build their resilience, awareness, and can also provide valuable insights to their partners and stakeholders such as insurance companies. These insights can be structured to provide an overview of the company against the relevant sector.

Further, the insights are available at different levels, for example administrator or user, to provide the relevant data for the stakeholders and parties involved. All whilst ensuring that security and data privacy is paramount. We provide a set of tools via our Compliance Platforms, ensuring that we can work closely with insurance providers and their clients on a number of added value propositions as seen in the table below:

The role of Isuna, together with our partners, is to help realise the potential value that can be identified, innovated, and delivered by multiple stakeholders or providers. With knowledge from the Association of Dutch Insurers, the market value of €36 million shows potential for expansion in the region. This is feasible through collaborations that can support clients and reduce the challenges that they face.

The requirements are evidenced, and the available market has space for multiple viable solutions, and new sector bridging partnerships. Working together the collaborations can provide services at a greater scale and build trust within the cyber marketplace. We have found that by identifying the challenges and value propositions we can match the solutions to the needs of the potential customers.

Insurance Providers	Insurance Clients
Complete cyber proposition of clients	Compliance to effective cyber standards
Datasets for clients and sectors	A complete toolset to manage and improve
Overviews for administration and assessment	Engagement mechanics to encourage improvement
Application of proven standards and regulations	Comprehensive support from subject matter experts
Validated and approved platform (EU and Royal NEN)	Always improved cyber controls and updates

References

[1] IBM, “Cost of a Data Breach Report 2021,” Aug. 09, 2021. https://www.ibm.com/nl-en/security/data-breach (accessed Mar. 22, 2022).

[2] MordorIntelligence, “Cybersecurity Insurance Market | 2022 - 27 | Industry Share, Size, Growth - Mordor Intelligence.” https://www.mordorintelligence.com/industry-reports/cyber-security-insurance-market (accessed Mar. 22, 2022).

[3] ProWriters, “Cyber Insurance History,” ProWriters, Jan. 23, 2020. https://prowritersins.com/cyber-insurance-blog/cyber-insurance/ (accessed Mar. 22, 2022).

[4] MarketWatch, “Global Cyber Security Insurance Market 2021 Segmentation, Future Business Strategy, Manufacturers Analysis and Forecast by 2027 - MarketWatch.” https://www.marketwatch.com/press-release/global-cyber-security-insurance-market-2021-segmentation-future-business-strategy-manufacturers-analysis-and-forecast-by-2027-2022-03-14 (accessed Mar. 22, 2022).

[5] S. Romanosky, L. Ablon, A. Kuehn, and T. Jones, “Content analysis of cyber insurance policies: how do carriers price cyber risk?,” J. Cybersecurity, vol. 5, no. 1, p. tyz002, Jan.

2019, doi: 10.1093/cybsec/tyz002. [6] Vantage Market Research, “Cybersecurity Insurance Market Size USD 26.24 Billion by 2028.” https://www.vantagemarketresearch.com (accessed Sep. 07, 2022).

[7] Verbond van Verzekeraars, “Cijfers & statistieken.” https://www.verzekeraars.nl/branche/data-analytics-en-onderzoek/cijfers-statistieken (accessed Sep. 07, 2022).

[8] USGAOgov, “Cyber Insurance: Insurers and Policyholders Face Challenges in an Evolving Market | U.S. GAO.” https://www.gao.gov/products/gao-21-477 (accessed Mar. 22, 2022).

[9] OECD, “Encouraging Clarity in Cyber Insurance Coverage,” p. 42, 2020.

[10] R. Böhme and G. Schwartz, “Modeling Cyber-Insurance: Towards A Unifying Framework,” p. 36.

[11] J. Bolot and M. Lelarge, “Cyber Insurance as an Incentivefor Internet Security,” Dec. 2008, doi: 10.1007/978-0-387-09762-6_13.

[12] NEN, “Isuna.” https://www.nen.nl/isuna (accessed Mar. 22, 2022). [13] Kansen Voor West, “Isuna Compliance and Resilience Platform.” https://www.kansenvoorwest2.nl/nl/nieuws/isuna-compliance-and-resilience-platform/ (accessed Mar. 22, 2022).

[14] N. Khaniejo and A. Sinha, “Economics of Cybersecurity II: Stakeholders,” p. 5.

[15] Cyberlinksecurity, “Who are my Cyber Stakeholders?,” Cyberlink Security, Jul. 01, 2020. https://cyberlinksecurity.ie/who-are-my-cyber-stakeholders/ (accessed Mar. 22, 2022).

[16] J. M. Bauer and M. J. G. van Eeten, “Cybersecurity: Stakeholder incentives, externalities, and policy options,” Telecommun. Policy, vol. 33, no. 10, pp. 706–719, Nov. 2009, doi: 10.1016/j.telpol.2009.09.001.

[17] P. Chen, “The Best Cyber Insurance Companies for 2022,” AdvisorSmith, 2022. https://advisorsmith.com/cyber-liability-insurance/best-cyber-insurance-companies/ (accessed Mar. 22, 2022).

[18] Howden, “Cyber Insurance - From Cyber Experts | Howden Netherlands.” https://www.howdengroup.com/nl-en/cover/cyber-insurance (accessed Mar. 22, 2022).

[19] Verizon, “2022 Data Breach Investigations Report | Verizon.” https://www.verizon.com/business/resources/reports/dbir/ (accessed Sep. 07, 2022).

[20] Code & Pepper, “Cybersecurity Insurance Providers - TOP4 Companies,” Code & Pepper, Mar. 23, 2021. https://codeandpepper.com/cybersecurity-insurance-providers/ (accessed Mar. 22, 2022).

[21] OECD, “Insurance Coverage for Cyber Terrorism in Australia - OECD,” 2020. https://www.oecd.org/finance/insurance/insurance-coverage-for-cyber-terrorism-in-australia.htm (accessed Mar. 22, 2022).

[22] G. J. May, “Nelson Mullins - The TRIA Cyber Risk Coverage Debate Should Be Resolved as Part of Its Renewal,” Nelson Mullins Riley & Scarborough LLP. https://www.nelsonmullins.com/idea_exchange/insights/the_tria_cyber_risk_coverage_debate_should_be_resolved_as_part_of_its_renewal (accessed Sep. 07, 2022).

[23] “The Hidden Costs of Cybercrime on Government | McAfee Blog.” https://www.mcafee.com/blogs/other-blogs/executive-perspectives/the-hidden-costs-of-cybercrime-on-government/ (accessed Sep. 07, 2022).

[24] “Hiscox – A case study interview | Isuna,” Mar. 28, 2022. https://isuna.net/2022/03/28/hiscox-a-casestudy-interview/ (accessed Sep. 07, 2022).

[25] R. Böhme, “Towards Insurable Network Architectures,” It - Inf. Technol., vol. 52, no. 5, pp. 290–293, Sep. 2010, doi: 10.1524/itit.2010.0605.

[26] M. Marenco and T. Seidl, “The discursive construction of digitalization: a comparative analysis of national discourses on the digital future of work,” Eur. Polit. Sci. Rev., vol. 13, no. 3, pp. 391–409, Aug. 2021, doi: 10.1017/S175577392100014X.

[27] OECD, “Enhancing the Availability of Data for Cyber Insurance Underwriting,” 2020. https://www.oecd.org/daf/fin/insurance/building-a-sustainable-cyber-insurance-market.htm (accessed Sep. 07, 2022).

[28] Oliver Wyman, “Cyber Risk in Asia-Pacific - the Case for Greater Transparency.” https://www.marsh.com/ph/migrated-articles/cyber-risk-in-asia-pacific-the-case-for-greater-transparency.html (accessed Mar. 22, 2022).

About Isuna

Isuna BV, based at the HSD Campus in The Hague is a company that focuses upon helping companies build their resilience to cyber threats and increase their awareness of the options that are available to them. To do this we provide Compliance Platforms that enable companies to effectively and efficiently implement regulations such as ISO27001 and GDPR (or AVG here in the Netherlands). We are trusted partners of Royal NEN* and recently validated by an EU programme**.

We have initiated a project to better understand the Cyber Insurance market and to connect stakeholders so that we can increase the accessibility, understanding and value to businesses. We have developed five case studies featuring key stakeholders in the Dutch cyber insurance market. These include:

- Hiscox
- Milliman (London office)
- Verbond van Verzekeraars (Dutch Association of Insurers)
- Eye Security
- Zicht Adviseurs (Advisors)

The contributions from our supporting partners listed above have been critical to developing knowledge about the sector and evidence considerable innovation in the industry. This is the second of two white papers centered on market challenges in (cyber) insurance. We will continue this work and look forward to sharing our analysis and research.

You can see all our white papers and case studies directly on our website. Furthermore, if you work within the cyber insurance sector and can provide some insight or want to be a part of our efforts as we scope the state of the industry, please contact us directly at info@isuna.net.

HISCOX Milliman VERBOND VAN VERZEKERAARS

eye Zicht risico- en verzekeringsadviseurs

* www.nen.nl/isuna

** https://www.kansenvoorwest2.nl/nl/nieuws/isuna-compliance-and-resilience-platform/

EUROPESE UNIE
Europees Fonds voor Regionale Ontwikkeling.
Mede gefinancierd in het kader van de respons van de Unie op de COVID-19-pandemie.

G4P4 Kansen voor West II