JULY 2022

Dutch Association of Insurers

A case study interview

With Marko van Leeuwen
Senior policy advisor for non-life insurances

&

Tuğçe Serinkan
Junior policy advisor

IN COLLABORATION WITH ISUNA AND PII

ISUNA

PEACE INNOVATION INSTITUTE
THE HAGUE

VERBOND VAN VERZEKERAARS

Dutch Association of Insurers

The Dutch Association of Insurers (Verbond van Verzekeraars) is a branch organization representing almost all insurance companies in the Netherlands, both in life, and non-life insurance. The organization helps navigate the politics between insurance companies and the government to lobby policies that set realistic, attainable goals for multiple parties.

This includes the organizing of sector-specific platforms that join relevant (external) stakeholders in a similar setting to gather and share information and come to solutions together. Overall, the Dutch Association of Insurers is a very large integrated network of stakeholders. Within this, they try to ensure ethical actions and behavior from their members and advocate for appropriate rules and regulations.

Marko van Leeuwen &Tuğçe Serinkan

For this interview we were lucky to interview Mr. Marko van Leeuwen, the senior policy advisor for non-life insurances, and Ms. Tuğçe Serinkan, junior policy advisor, who together have played a significant role in the set-up of the cyber insurance platform. In this case study Marko and Tuğçe gave valuable insight to how from a policy side they tackle challenges within the cyber insurance sector.

The Organization's Branch into Cyber Insurance - the Market Challenges

Challenge 1: Complex Stakeholder Relationships

As cybercrime started to create global attention, a new market of insurance emerged that has demanded the attention of the Association. From a government side the implementation of policies such as the GDPR have created new challenges for companies and insurance companies alike to adhere to specific privacy rules that if broken, result in reputational and financial losses. Meanwhile, on the insurer side, the lack of a history of data breach or cyber incidents prevents accurate pricing mechanisms. This means we do not know what can happen, the frequency, the chance, and the magnitude of the damage. Additionally, attacks could occur at the same time, in many places.

From the insurer side, this is a catch 22; as clients aren't insured, there is no damage report to learn from, but without the damage report, there is no possibility for insurability either. Herein, it becomes difficult to write policy and price accurately. Marko explained that he believes that the current economic and political situation is more uncertain than in history, making it harder to navigate this new market.

Herein, a discussion arises within insurance companies and the government on where to draw the boundary in cyber insurance of what is considered insurable, and what is considered prevention (a client's investment responsibility). Insurance companies play a role as insurers in the case of damage, but not an investment towards preventative actions. However, setting and defining this boundary is not the simplest task.

For example, the Netherlands recently implemented a law mandating the use of smoke alarms in every home. The government, if mandating this would encounter challenges on checking whether every home has a smoke alarm, and thus ask the Association to develop policy that requires insurance companies to mandate people who have fire insurance, to have smoke alarms. This policy, however, is problematic given the competition law in the Netherlands, the Association cannot force a company to write a policy in a given manner.

This is where the cooperation between government and insurance companies is necessary to effectively write policy that is beneficial to all parties. Defining the prevention vs. insurability boundary is necessary as it helps define the premium of insurance, a price driven by the average damage cost per incident per sector.

The accumulation of risk within the cyber insurance market now, is what helps to define the insurability. However, there is no capacity for the insurance market to handle this accumulating risk and could lead to incredible (non)financial losses. In traditional insurance, risk is diversified between local, national, and global levels. While this is contextually measurable in the majority of sectors, in cyber crime or incidents diversification of risk cannot be separated geographically. Thus, working with international reinsurers helps as there is additional data from global networks. Although, even with this, it is still limited, and it remains unknown what the magnitude of cyber damage is in one area vs another.

Cyber insurance as of 2021 in the Netherlands is worth €36 million (up from €28 million in 2020), this is a surprising figure given the global statistics describing a worth of $20 billion by 2026, and the €14.9 billion value of non-life insurance in the Netherlands (2021).

Challenge 2: Low market penetration

This high-risk for insurers, that although investing to retain a position in a new market, is unappealing. “The market now is not competitive in this sense, the risk is too high. There is a “risk premium on a risk premium because you don’t know”. The financial and reputational outcomes can be catastrophic, for both small and large actors. When finding reinsurers to help unburden the full weight of an insurance provision, they too will only invest to the extent of their own solvency. Cyber insurance for insurers and reinsurers is only a margin of the business produced, and the risk does not outweigh the profit. Cyber insurance as of 2021 in the Netherlands is worth €36 million (up from €28 million in 2020), this is a surprising figure given the global statistics describing a worth of $20 billion by 2026, and the €14.9 billion value of non-life insurance in the Netherlands (2021).

Currently 10 – 12 companies are offering a cyber product in the Netherlands, often providing a full package (insurance + services). For a company to be insured, the process starts with a risk assessment then the company is suggested to take prevention steps. After these have been taken, the company is insured and has access to third party expertise and specialists who help solve additional challenges along the way. This is an effective set up as many companies, in the event of a cyber breach, are unaware of the steps they must take to receive proper help. However, while this package is helpful, the premium is more expensive as it includes the costs of additional services, making it less attractive to Small Medium Enterprises (SMEs).

The overall high accumulation of risk, and the costliness of premiums, outline the low level of market penetration. Insurance companies cannot afford to hold back money for damage coverage for larger client bases, and the market of SMEs are not in the best position to afford cyber insurance as the package includes more than just the insurance price.

The solutions

The Cyber Insurance Platform

As part of a public-private partnership with Chubb 2,5 years ago, the Association with financial support from the government was able to develop a platform focused on solving issues and developing discussions within the cyber insurance space.

Now representing 7 insurance companies, and relevant stakeholders (such as the police, as cyberattacks are still dealt with by the legal forces), subtopics and objectives have been identified to push the agenda. These are increasing awareness, prevention, and data sharing for people and SMEs.

Solution 1: Awareness and Prevention

To stimulate awareness and preventive action, the government financially supported the Association in the development of a Digital Security Risk Classification model that includes 11 questions to assess the safety of your positionality within a cyber security space, and tips to improve your cyber resiliency. This is necessary given the chain cooperation many SMEs and multinationals share in regard to exchanges of information they may have.

This unique model in the Netherlands helps to create a shared language to discuss clearly what the risks are and helps to send a similar message towards clients of what is going on. In combination with the Business Association of the Netherlands, and consistent touch base with insurance advisors, this clarity is maintained, and everyone shares and holds the same information. The next step in this risk model is to develop certification schemes.

Solution 2: Data sharing

The next topic is on improving data sharing. This starts with a prior discussion on how to even start collecting data. This includes discussion which classifications the sector wants, and to what level data can be managed, and from there asking insurers to report that every year. Currently the association asks for information about yearly turnover, however, this does not provide information on risk and profitability. Currently global insurance players have the upper hand, they are better informed than local insurance players, and policies from one place could be translated to another. Within the Netherlands, local players find it difficult to offer an insurance product within this competition.

To make a cyber insurance product work, they need to: start a discussion about what and how to collect data, then agree together, that everyone will report in a shared database. At first the database will be empty as there are few incidents, but that slowly over time will increase. The drawback here is that given the private nature of data as set by the GDPR, the first few data sources released can never truly be “private”. Thus, reporting now can only be done at a very aggregated level. That is not optimal, but it is a start. From here, it makes sense to expand this data collection to neighboring countries to learn more.

The vision for the Association of Dutch Insurers is clear, the cyber insurance platform intends to:

- Help risk awareness: financial instruments, certification schemes, publications;
- Try to send the same message from all parties, to create a common direction and goal;
- To improve and stimulate each other towards sharing data.

Conclusion

According to the GDPR, all companies are obliged to report data breaches. This is when we could argue for the sharing of aggregated data. The umbrella organization, Insurance Europe, has made efforts to try to convince the European Commission to share information. Yet, so far, these policy initiatives fail. The maintenance of data sharing within the multinational level outweighs local players and risks chances of a monopoly occurring if large governmental players are not collaborative with stakeholders.

ISUNA believes getting the right players round the table and discussing challenges will open the dialogue to sharing solutions, as the Association has shared with us. It's important to recognize with the volatility of the market, a local insurance provider such as Nationale Nederlanden and Achmea, could not cater to 60 – 70% of the market, but can still find potential to make a profit in cyber insurance. Sharing different company perspectives and solutions can help lower insurance risks as well. By starting now, we can help the Netherlands become a leader in this market, where other countries and companies can follow.

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[1] and recently validated by an EU Kansen voor West program.[2]

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 are developing case studies, such as this one, to highlight approaches and to help the insurance sector build their services and collaborations based upon building market share through the provision of improved services. We will continue this work and look forward to sharing our analysis and research. If you work within the cyber insurance sector and can provide some insight or want to be the subject of the next case study please contact us directly.

We'd like to thank Mr. Marko van Leeuwen and Ms. Tuğçe Serinkan for their time and energy in providing us with insights about cyber insurance and his expertise as senior and junior policy advisors at the Dutch Association of Insurers.

1. www.nen.nl/isuna
2. 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