JULY 2022

Eye Security

A case study interview

With Job Kuijpers - CEO and co-founder of Eye Security

IN COLLABORATION WITH ISUNA AND PII

ISUNA eye. PEACE INNOVATION INSTITUTE THE HAGUE

Eye Security

Eye Security is a headliner cyber security and cyber insurance company providing an all-in-one package for the necessary security a small-medium enterprise (SME) needs.

Founded in 2020, the company has quickly expanded to over 60 workers. Their all-in-1 Eye Security package offers cyber monitoring and detection, 24/7 cyber response in the case of an incident, and as of recently, their own cyber insurance. Here a unique selling point for them has been the rapid pace supplying cyber insurance, and the low cost, outperforming the market at every level. Through a careful process of selection, Eye Security reduces the hassle and unnecessary products and services of cyber protection, adopting the most impactful and modern technologies to their package.

Job Kuijpers

CEO and co-founder of Eye Security

For this interview we were lucky to engage with Mr. Job Kuijpers, one of the 3 co-founders of Eye Security. His previous experiences working as Director National Communications Security Agency at the General Intelligence and Security Service (AIVD). He gave us a unique insight to understanding how a company like Eye security provides a necessary advantage for SME's. In this case study, Mr. Kuijpers explained to us the current landscape of cyber insurance and how Eye Security overcomes SME specific market obstacles.

www.eye.security info@eye.security +31886444888

Overview of the market - the playground

In outlining the market of Dutch cyber insurance, Eye Security identified three key influencers, based on their positioning and relationship to the emerging risks in the market. It should be noted many other smaller actors are present within the market, however, at the grand scale, these are the big three to be aware of for Eye Security.

1. SME's

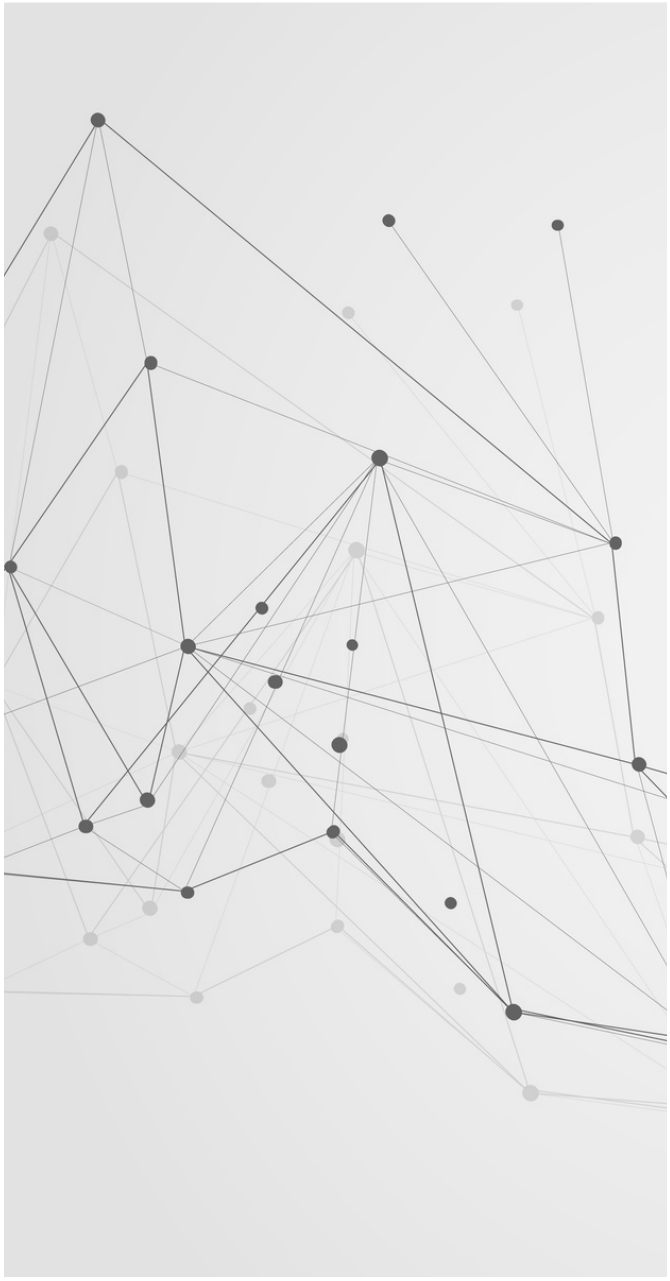
The first player are the actual SME's. The daily operations of SME's already run at a high-risk level, an integral component of start-up or operational nature. With this behavior, the current adoption of high-level cyber security is lagging, and the risk isn't seen as more than usual to the current risks the business faces on an everyday basis.

2. (Re)Insurers

Secondly, are the (re)insurers; the insurance market dove into cyber insurance without complete information as to the costs of cyber-crime and the risks associated. This has resulted in volatile pricing mechanisms, and unfeasible security requirements for customers, making lots of companies uninsurable and therefore completely exposed to the cyber risk.

3. The government

Thirdly, is the government; in an attempt to take cyber-crime more seriously and protect the privacy of consumer data, their lack of a shared taxonomy and disconnect to stakeholders prevents successful delivery of regulation. The government operates in two forms: firstly, is through subsidies and tax cuts (carrot approach), or through forcing measures such as fines given from the GDPR (stick approach).



The challenges

Challenge 1: Lack of awareness

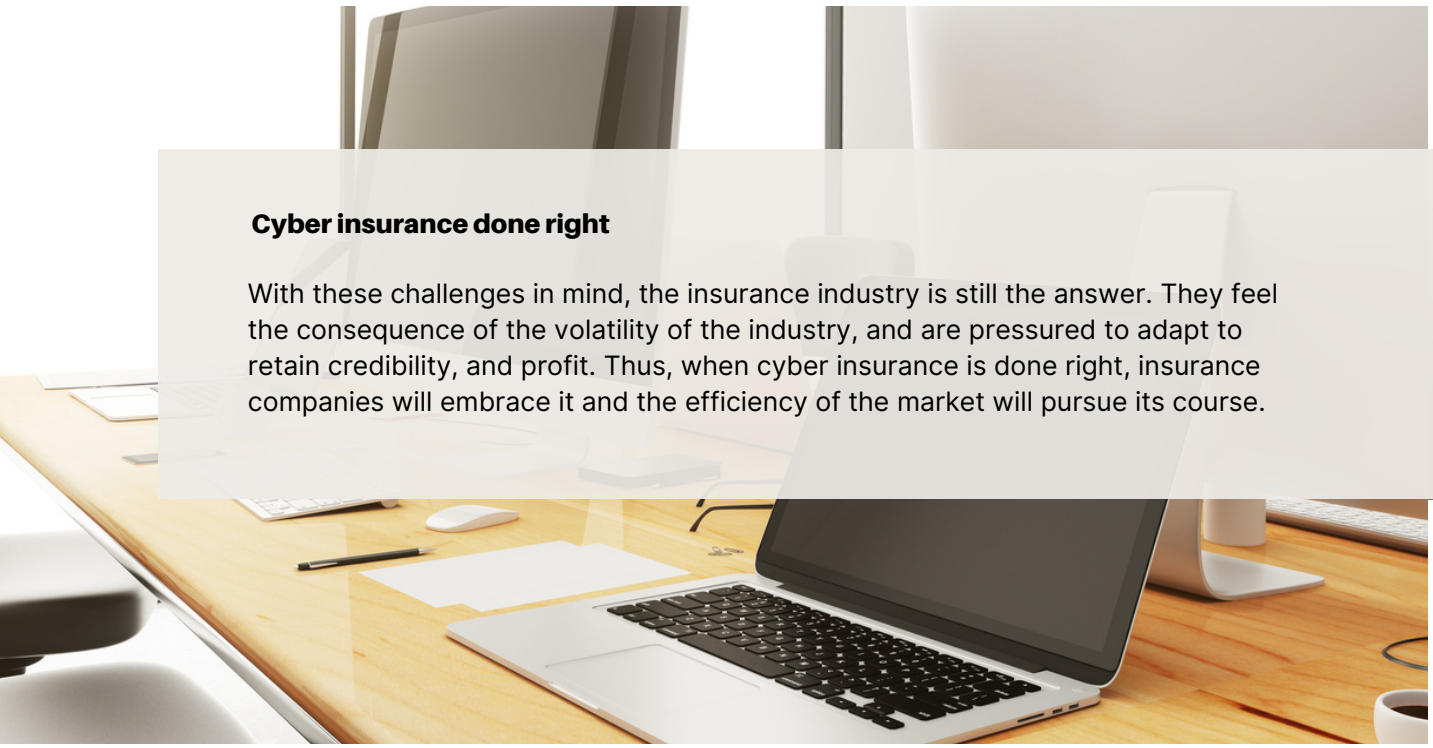
Within this emerging market, new players are aiming to capitalize on the rapid growth and potential payoffs for cyber insurance. In what Mr. Kuijpers calls “a market of cowboys”, new entrepreneurs are trying to get in and lasso a share of the profit. This is profitable as the client base of companies looking for cyber security and insurance aren’t informed of their needs properly — this is part of a larger systemic issue on the lack of awareness companies face regarding cyber protection. Information asymmetry here leads to a new market of lemons: uncertain quality within the products is sold from cowboys to the uninformed client-base. To overcome this, Eye Security is particularly cautious about which modern technologies they adopt into their package offering only the most necessary, impactful services and valuable trusted partners.

Challenge 2: The disconnect between the government and SME’s

The second challenge regards the disconnect between the government and SME’s. The current observation showed the government is better in navigating support towards larger companies who are already well established and have a prior existing support system. SMEs on the other hand are not receiving this same level of support, and once facing an attack are left to deal with the repercussions alone. The slow rate of help from government services in events such as a cyber-attack force SME’s to face the hardest, sometimes irreparable losses very much alone.

Challenge 3: Protection is not adapting quick enough to the change of cyber threats

The third challenge is the difference between innovation and magnitude of cyber-crime compared to the review time of the insurance industry. At the end of the year, an insurance company will review its policies, costs, and revenues - of which in those results will tighten or loosen policies and change premiums. However, within cybercrime adaptations are made on wider and faster scales, the iterations for premium review are not up to par with the rate at which cybercrime affects businesses financially.



Cyber insurance done right

With these challenges in mind, the insurance industry is still the answer. They feel the consequence of the volatility of the industry, and are pressured to adapt to retain credibility, and profit. Thus, when cyber insurance is done right, insurance companies will embrace it and the efficiency of the market will pursue its course.

The solutions

In being able to utilize the insurance market, Eye Security has an approach of "we are all in one ecosystem, let's help each other". Their unique business model allows for them to operate a cyber insurance model within a portfolio of complete information.

Cyber insurance companies face high loss ratios, higher than 100%. Eye Security has a loss ratio of 0%. Offering their own cyber insurance underwritten by Hiscox (see our previous case study here), they have made efforts to support impact reduction. For example, if you own a building, you can take measures to reduce the probability of a fire occurring, such as implementing no smoking policies. But while this policy may exist, the chance exists someone will leave a candle on during the night, resulting in a fire. Impact reduction happens when you have a fire extinguisher in your direct vicinity, after the fire has started, you can work to reduce the impact. Eye security takes this impact approach seriously in being prepared for addressing the systemic risks that occur throughout cyber-crime.

A success story for them was this Christmas when many companies were affected by the Log4J exploit. While many companies were hurt and cyber insurance providers felt severe financial impacts, Eye security was able to predict the impact and immediately prepare their clients against any vulnerabilities they may have. None of their clients were hurt during this period.

By working with their extensive company clientele network, Eye security retains internal information on what technologies and actions work best to understand which impacts and how to reduce specific impacts most efficiently. This helps them to organize the prevention methods a company requires in order to clarify the insurability of their business. "The only way to tackle (systemic) risk is with inside data, and to have full response capability. It's a capability you have when you are ABN Amro or Shell, but for a medium size company that doesn't exist, and that is what we are bringing." Their inside data and team of experts allows them to outperform the slowness of the cyber insurance market as their iterations occur at the speed at which cybercrime and systemic risks occur. They are aware of any of the changes made. With this they are able to accurately assess the costs an attack would create and accurately price the premium.

> **"The only way to tackle (systemic) risk is with inside data, and to have full response capability. It's a capability you have when you are ABN Amro or Shell, but for a medium size company that doesn't exist, and that's what we are bringing."**

Eye Security currently protects SMEs with an average of 50 – 500 workplaces, their biggest client holds 5000 workplaces. The depth and specificities of inside data gives Eye security

the ability to put active measures in place through good technical solutions that align well to reducing ransomware attacks across Europe for example.

ISUNA

In positioning Isuna within this wider discussion of overcoming challenges of different stakeholders, testing resiliency becomes a point to highlight. Herein, Eye Security is impact driven and resiliency is built within the frame of cyberattack.

Isuna operates in a complimentary fashion in resiliency towards compliance. The earlier mentioned disconnect at the government level does set the stage for companies to be financially and reputationally burdened by (un)intentionally failing to comply with standards such as the GDPR and the ISO 27001. Impact can be reduced one step at a time when resiliency is tested and action is taken once a vulnerability is identified.

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. Job Kuijpers for his time and energy in providing us with his insights about cyber insurance and his expertise as co-founder of Eye security.

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