SEPTEMBER 2022

ISUNA

White Paper

Cyber Challenges for General Insurance & Financial Service Companies

ISUNA

PEACE INNOVATION INSTITUTE
THE HAGUE

Introduction

The cyber security industry faces an everlasting challenge surrounding awareness of the necessity and importance of cyber security within a company's operating framework [1]. As a risk, companies are unprepared to face the large losses that occur when a company is under attack. Only post-attack, do many companies start to take action to secure their system. It should be known, that the 6 trillion dollars lost due to cybercrime in 2021 globally could have been prevented or greatly reduced in many of the scenarios [2].

This overarching awareness and prevention issue has risen to a new market development, where the lack of preventative action towards cyber security, prioritizes market space for actors engaging in post-damage reconstruction and coping strategies for the aftermath of a cyber-attack.

Recently, more priority has been set towards resilience in cyber security which acts as a linking factor between aftermath-focused market actors and the need to be preventative and engaging. Other sectors have shown, that working preventatively has one of the highest positive outcomes, and lowest financial burdens, especially in the crime-reduction industry. To describe this better in an analogy, it is cheaper to wear sunblock every day than endure the financial, physical, and emotional costs of skin cancer. We choose to wear sunblock when it is sunny outside and when we know there is a high risk of getting a burn.

The short-term (burn) and long-term (probability of skin cancer) exist and work exactly like the risk of re-enforcing cyber security (and better yet, cyber insurance) measures.

The sun outside in this analogy represents the level of risk a company has in potentially suffering a breach. Here, companies are rated as more or less of a target for cybercrime based on:

- their industry,
- revenue,
- company size,
- products and services, and
- sensitivity of data.

One industry specifically vulnerable is the general insurance industry. A key target, insurance companies hold large sums of sensitive and private information that can be held as a ransom [3].

This white paper focuses on the larger issues and pain points insurance and financial service companies face. In line with empowering businesses to learn from one another, Isuna addresses this problem and expands on its product platform that dives further into how collaboration and transparency save overall costs in implementing effective cyber security measures.

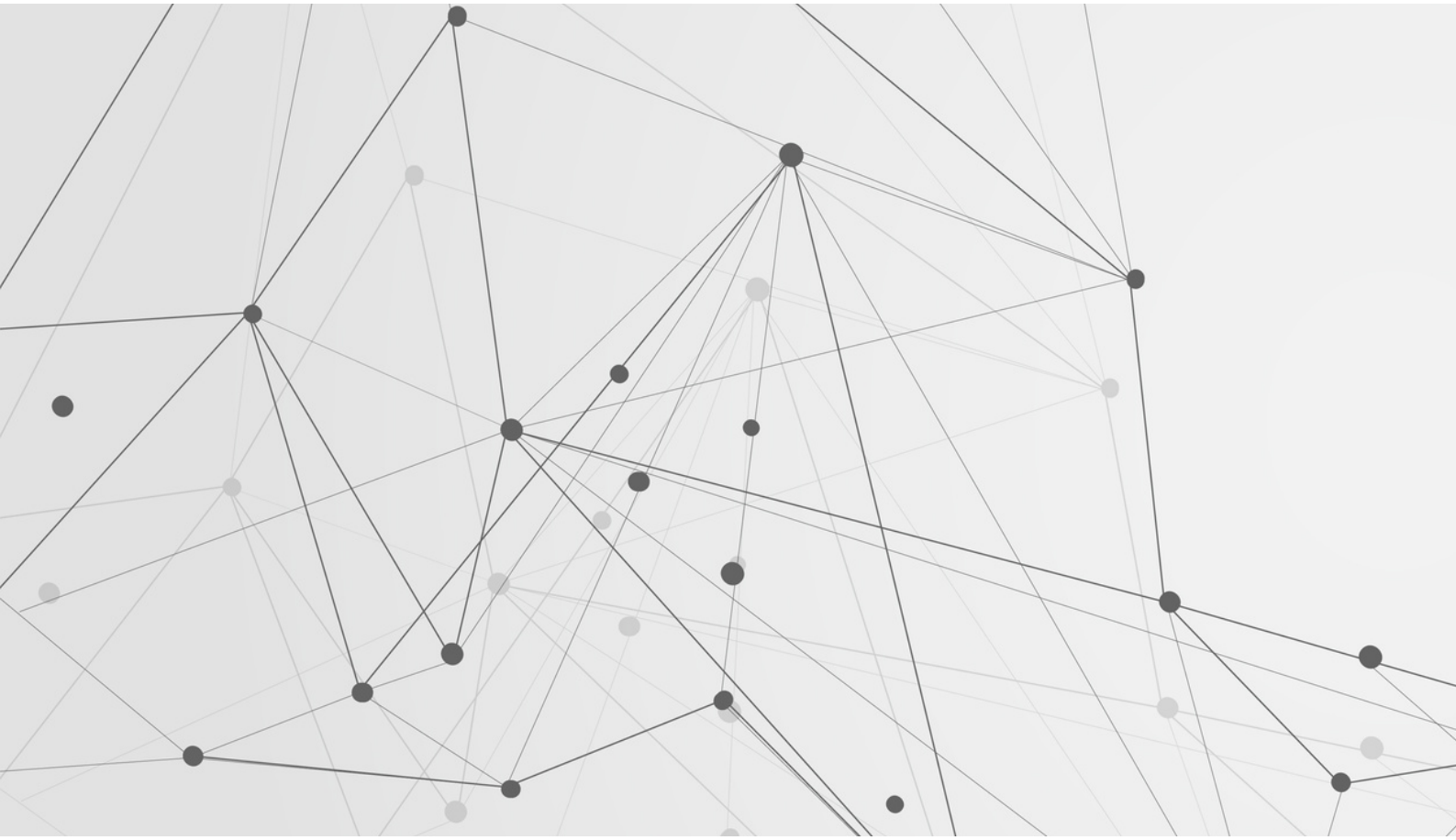
A) Problem statement

Insurance companies are placed in a special position, as they are required to include cyber security both internally and keep an eye on external developments in the field as it impacts their value chain [4].

Embracing this dynamic level of innovation has two effects on insurance companies. Firstly, on the consumer/ demand side, the expectation is heightened by asking for 24/7 service and accessibility to services via apps on smartphones. On the competitor/ market side, new financial technology companies are working to move risks previously needed in insurance (such as starting up a business), into other areas such as crowdfunding (GoFundMe, and Kickstarter as examples). The means for insurance companies to modernize and innovate are stretched thin and the opportunity to grow lies in the strength of the infrastructure of the business. Simply, an important component of the strength lies in cyber security.

Currently, many of the new services used by companies have cyber security embedded in the design of the service which updating old practices and services become more difficult. Rather, insurance companies are earlier suggested to retain the newer IT service. Effectively insurance companies are left to an extent vulnerable about processes occurring in new service design, and uninformed about how to upgrade processes in old service design [5].

In keeping up with these pressures, a common theme within cyber security is the fear-induced staging of cyber security and law specialists that enter a company with intentions to help strengthen the cyber security practices and ask them to sign non-disclosure agreements. This prohibits companies from communicating with one another to readily learn how to build best practices. It prevents companies who are enduring the same experiences from sharing them, improving transparency over the field, and building resiliency.



B) Pain points of Financial Service Companies

Each industry faces a set of unique pain points that require tailored solutions. For financial service companies, research has shown the following pain points to be most prominent across the industry:

1: Asymmetric Stakeholder Relationships

Asymmetric Stakeholder Relationships: Underwriters, clients, the government, and third-party actors, are all involved in the delivery of well-organized insurance packages. Within cyber security, the lack of (shared) knowledge adds additional pressure on the stakeholder engagement in which asymmetric information from one stakeholder (such as poor knowledge of GDPR) results in imbalanced partnerships between the company and the government.

Since 1 January 2016 organisations have been obliged to organise their data exchange in such a way that they can demonstrate that they have this under control, or that they have immediate measures in place to prevent data leaks (Art. 34a of the Personal Data Protection Act). While a cyber security expert may help arrange this, the business remains somewhat uninformed of the procedures in place and is not protected against making mistakes. This leads to the next pain point;

2: Control and grip on data

Control and grip on data: Nowadays one of the most important 'possessions' of organisations, is a necessity in today's digital society. Yet, the range to which data can travel is beyond traditional methodologies remaining inside the business office. This creates a risk of reprimands or fines from the relevant Data Protection Authority in the event of observed or suspected shortcomings.

The grip is further undermined by the structure of insurance companies. It is encouraged for clients to access online portals via their own digital devices. On mobile devices or browser viewings firewall protections and cybersecurity setups embedded into app design help to an extent in the protection of data, however many users will still access their portals through non-secure devices further increasing the risk of cyber attack and the overall vulnerability of the insurance company [2].

3: The combination of policy and technology

The combination of policy and technology: government regulations are not informed with coherent taxonomies regarding the laws and fine print on how to best implement cyber practices [3, 4]. This results in a series of economic challenges as the responsibilities and liabilities of different parties in a policy setting are not well defined leaving it to non-policy actors to decide the best course of action which can be more costly than necessary. Additionally, it leverages a bias of creating or prohibiting services based on potential reputational damages that can occur resulting from a breach.

Gaps exist within the regulatory policies for financial service companies where fear of cybercrime and fear of breaking regulations paralyzes insurance companies in drawing a realistic boundary between taking measures to face the relative risk of cyber-crime, that does not go overboard in meeting government regulations. The dual-fear mechanism in practice is discussed behind non-disclosure agreements with experts. The lack of transparency between experts, the insurance company, and the government increases the cost of implementing and identifying the best practices in cyber security. [6]

The tension herein helps understand why at the moment, there is no certification process for Data Breach and GDPR Tooling approved by the Dutch Accreditation Council (RvA). Revealing the further volatility and range of the margin of error in interpreting cyber security regulation.

C) The cost of a fine

Addressing these pain points can help ease the concerns about compliance and data leakage. The overall costs of these paint points can be reduced through better transparent communication between key stakeholders. GDPR as a primary example has effectively been in place since July of 2018 [7]. Within the EU, the Finance, Insurance, and Consulting Industry rank as the 5th highest sector in the total sum of fines totalling €31,727,508 and the 4th highest sector referencing the number of fines issued at 110, 4 of which have been from companies based in the Netherlands [8].

These fines have increased over time, especially in the past year (noting the pandemic and online shift have increased the ability for cybercrime to occur). The fines are being issued at higher amounts, now easily issued in the millions of euros. The majority of these fines were issued on a basis of internal compliance measures, of which there was no sufficient legal basis for the processing of consumer data as controllers did not succeed in acquiring the consent of customers to process their data [9]. This amounted to a total of €6,383,970 [10]. The following table shows the total sum of fines issued by the GDPR, the number of fines, the average cost over total fines since its first fine, the median cost per fine, and the average cost of fine per month from 2019 to the present for the Insurance, Consulting, and Finance Industry.

Within this table, there is an estimated growth of €6.416.532,50 per year if the current circumstances do not change. The lack of changes in national laws amidst the increase in fines reveals the fines are not a temporary measure [11]. This is further supported by the increasing value of the median cost per fine with an estimated growth of €127.200,00 per year.

Without change, the estimated total sum of fines will cost €79.247.575,00 in 10 years. With a median increase of cost at €16.354.250,00 in 10 years. These striking figures only account for GDPR fines, not the additional losses from cyber attacks. Although frightening, it is important to remember these fines can be avoided when companies and experts can communicate with each other and collaboratively understand their compliance mechanisms.

Table 1: GDPR fines from 2019 - April 2022

Year	Total fines	Median fine	Average fine	Fines issued	Average cost of fine per month
2019	€2.249.185,00	€80.000,00	€97.790,65	23	€187.432,08
2020	€9.559.640,00	€478.500,00	€341.415,71	28	€796.636,67
2021	€15.082.250,00	€446.100,00	€335.161,11	45	€1.256.854,17
2022 (until April)	€2.959.600,00	€514.800,00	€269.054,55	11	€739.900,00

Numbers taken from the GDPR enforcement tacker, 2022

Table 2: Estimated Growth of GDPR Assuming Current Conditions

Date	Per year		In 10 years	
	Estimated growth	Median increase in costs	Estimated Total Sum of Fines	Median Increase of Cost
2019 - 2022 (April)	€6.416.532,50	€127.200,00	€79.247.575,00	€16.354.250,00

Numbers taken from the GDPR enforcement tacker, 2022

D) The cost of a cyber attack

Since the pandemic, the global financial sector has been hit the hardest by cybercrime, this has increasingly occurred with the digitalization of the financial sector [12]. In 2020 February, the number of attacks was set at 5,000 per week and increased to 200,000 per week in late April [13]. This reportedly disrupted 20% of network operation activities at financial service companies [14].
Cyber-crime costs vary per form of crime, in a report by KPMG, three tiers of attacks were classified [15].

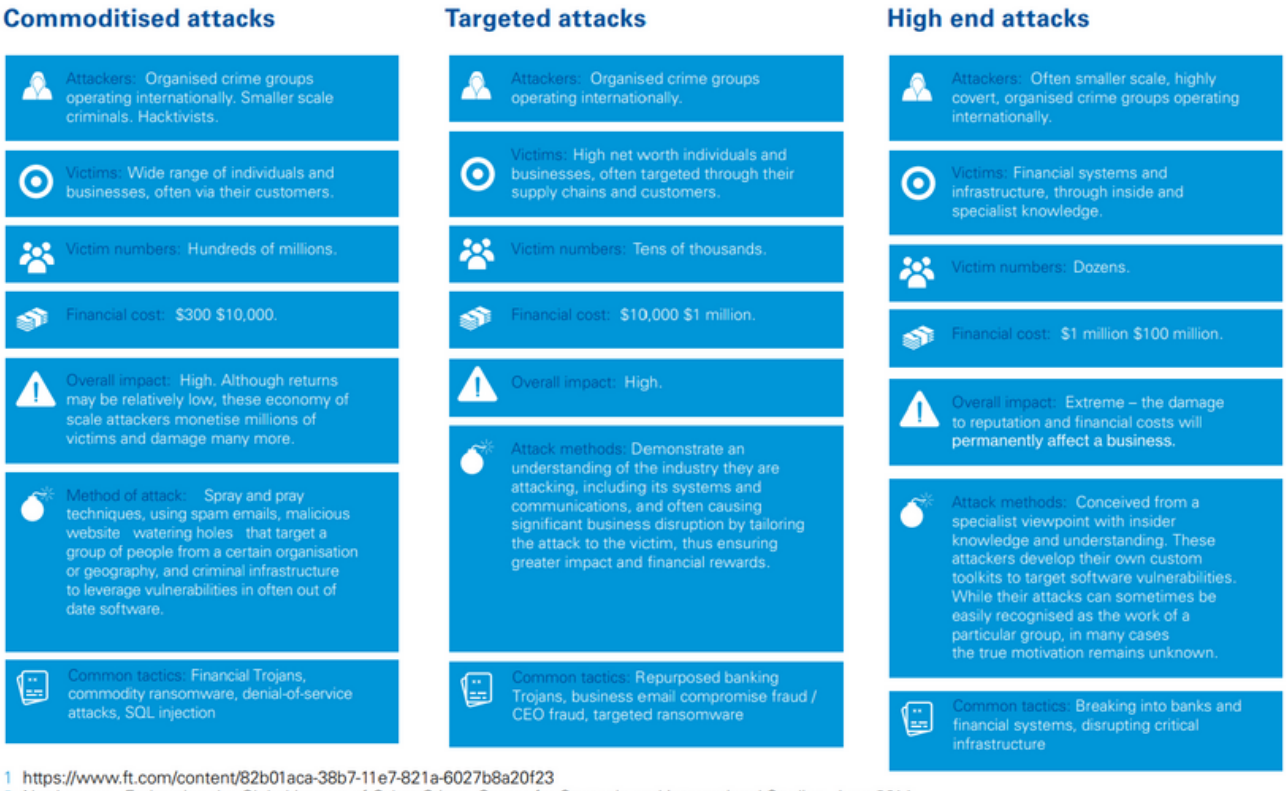
Neither GDPR costs nor cyber crime costs account for reputational losses, in which the financial sector has been the most scrutinized industry as they have had to comply the fastest, adapt to consumer digital needs, and are the heaviest cyber-targeted industries [16].

For a company to track this themselves, they could follow a simple equation:

Average daily revenue + Average daily operational costs = Potential daily loss.

Average daily operational costs here refer to wages, hire of offices, and all other costs. To see the number of days an organization can survive before going bankrupt, companies can look at:

The daily loss / own and available cash and reserves = number of days before bankruptcy.



1 https://www.ft.com/content/82b01aca-38b7-11e7-821a-6027b8a20f23
2 Net Losses - Estimating the Global Impact of Cyber Crime, Center for Strategic and International Studies, June 2014

Image credit from KPMG - Cyber Security and the Insurance Sector Report, 2017.

The Isuna solution

The solution proposed takes into consideration the predicted cost of €6.4 million per year, Isuna BV developed a Compliance and Maturity Measurement tooling solution (based upon GDPR and ISO standards) for insurance advisors.

In addition, special Security software offers a very user- and implementation-friendly platform for the secure sharing of data, regardless of the device (desktop, laptop, tablet or smartphone), so that there is 24/7 control and overview. With simple instructions, any user can apply it and it has little or no impact on the existing IT environment. In this way, the business can clearly understand its resilience levels and the insurance company can easily fulfil an advisory and executive role for its insurance advisors.

Rather than simply having a green check mark to meet a certification standard and later discovering the flaws in the system, a business has more clarity and control in creating real progress that meets compliance regulations. The whole thing has been translated into a complete solution consisting of:

- Alignment to complementary standards
- Unique tools that assist businesses and insurance companies
- Assessment and Maturity Reporting provide resilience measurements
- The Improvement space provides complete project management tools
- Community and Help Desk space provides solutions and advice to users
- Validated by Royal NEN
- Helps businesses complete the relevant certification

Through this unique solution, businesses are in a position to better plan and prioritize their vulnerabilities and improve their spending through best-placed investments on their most specific pain points. Insurance advisors hold a large amount of privacy-sensitive information of both their clients and potential clients. As they must comply with rules imposed by the GDPR on financial service providers to ensure that the interests of their clients are met with care and security.

With the help of the Isuna Platform, insurance companies are better positioned to better protect the companies they insure, this control over resilience helps to lower the risks and costs associated with the insurance companies operations. Overall, this can help expand their businesses while maintaining cybersecurity costs at a stable level.

After 25 May 2018, the Dutch Data Protection Authority conducts random checks on whether and to what extent the GDPR Act is being complied with [17]. It seems logical that in addition to healthcare, government, large companies and financial service providers will be tested. In the case an insurance agency was to have a Data Breach, but could prove the process of implementing GDPR & ISO-compliant measures, and demonstrate their interpretation of those measures; assurance and verifiability would contribute positively to the trust that its customers have in it concerning privacy.

The use of tried and tested GDPR tooling for this, with organisational and legal support where necessary, would be interpreted as a strong signal that insurance advisers are serious about privacy, thus creating a marketing advantage over other insurance advisors. By complying with the Data Breach and the GDPR legislation, the chance of data leaks and complaints about breaches of privacy is reduced. This also reduces the likelihood of warnings, reprimands or fines from the Dutch Data Protection Authority in the event of observed or suspected shortcomings.

If despite this, something does go wrong, it can be shown that, by using tooling software and the accompanying organisational measures, an attempt has been made to comply with the GDPR and ISO legislation. It is then expected that a warning and possibly binding advice will suffice. This tracking and tooling of Isuna help to lower the cyber compliance and resilience costs that in turn lower the entry barrier for companies to improve their cyber resilience. This leads to more business activity and growth potential in the areas of cybersecurity and (cyber) insurance.

References

[1] Romanosky, Sasha, et al. "Content analysis of cyber insurance policies: How do carriers price cyber risk?." Journal of Cybersecurity 5.1 (2019): tyz002.

[2] Ventures, C. (2019). 2019 Official Annual Cybercrime Report.

[3] Eiopa (2021). https://www.eiopa.europa.eu/

[4] Kabir, U. Y., Ezekekwu, E., Bhuyan, S. S., Mahmood, A., & Dobalian, A. (2020). Trends and best practices in health care cybersecurity insurance policy. Journal of healthcare risk management, 40(2), 10-14.

[5] OECD (2020), The Role of Public Policy and Regulation in Encouraging Clarity in Cyber Insurance Coverage. www.oecd.org/finance/insurance/The-Role-of-Public-Policy-and-Regulation-in-EncouragingClarity-in-Cyber-Insurance-Coverage.pdf

[6] OECD (2020), The Role of Public Policy and Regulation in Encouraging Clarity in Cyber Insurance Coverage. www.oecd.org/finance/insurance/The-Role-of-Public-Policy-and-Regulation-in-EncouragingClarity-in-Cyber-Insurance-Coverage.pdf

[7] Kao, M. B. (2019). Regulating the Cybersecurity of Insurance Companies in the United States. Transactions: Tenn. J. Bus. L., 21, 11.

[8] CMS (2022). Enforcement Tracker. Database. https://www.enforcementtracker.com/?insights

[9] CMS (2021). GDPR Enforcement Tracker Report. https://cms.law/en/media/local/cms-hs/files/publications/publications/gdpr-enforcement-tracker-report-2021-executive-summary?v=1

[10] CMS (2021). GDPR Enforcement Tracker Report. https://cms.law/en/media/local/cms-hs/files/publications/publications/gdpr-enforcement-tracker-report-2021-executive-summary?v=1

[11] CMS (2021). GDPR Enforcement Tracker Report. https://cms.law/en/media/local/cms-hs/files/publications/publications/gdpr-enforcement-tracker-report-2021-executive-summary?v=1

[12] CMS (2021). GDPR Enforcement Tracker Report. “Finance, Insurance, and Consulting” https://cms.law/en/deu/publication/gdpr-enforcement-tracker-report/finance-insurance-and-consulting

[13] CMS (2021). GDPR Enforcement Tracker Report. https://cms.law/en/media/local/cms-hs/files/publications/publications/gdpr-enforcement-tracker-report-2021-executive-summary?v=1

[14] Aldasoro, I., Frost, J., Gambacorta, L., & Whyte, D. (2021). Covid-19 and cyber risk in the financial sector (No. 37). Bank for International Settlements.

[15] KPMG (2017). “Cyber Security and the Insurance Sector” https://assets.kpmg/content/dam/kpmg/uk/pdf/2017/08/cyber_security_and_insurance_sector.pdf

[16] KPMG (2017). “Cyber Security and the Insurance Sector” https://assets.kpmg/content/dam/kpmg/uk/pdf/2017/08/cyber_security_and_insurance_sector.pdf

[17] Campbell, E. (2019). Dutch Data Protection Authority issues first GDPR-fine. Compliance Junction. https://www.compliancejunction.com/dutch-data-protection-authority-issues-first-gdpr-fine/

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 first 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