MILLIMAN WHITE PAPER

Market trends in cyber risk insurance within the Netherlands

Joris van der Moore
Joost Broens
Sjoerd Brethouwer

Introduction

Cyber risk is one of the fastest emerging risks of today. Companies are increasingly reliant on digital technologies, which has made cyber risk management a top priority for organisations. This is why cyber risk insurance plays a very important role in providing a possible solution against potential losses from cyber incidents. It is part of the complete cybersecurity management strategy. A possible solution to these threats is cyber insurance. This insurance can cover different types of risk, including the ransomware sum, regulatory fines on privacy, lost income due to attacks and the losses on more specific cyber incidents.

The cyber insurance market, while still relatively small compared to other insurance sectors, is one of the fastest-growing areas in the industry. Despite representing less than 1% of the nearly USD 800 billion total US industry direct premium written (DPW), cyber insurance saw an increase of 73% in 2021, reaching a total of USD 4.8 billion. A year later, it increased to USD 7 billion.[1] Reinsurer Munich Re has projected that the global cyber market could reach a size of USD 25 billion by 2025.[2] International insurance broker Howden predicts cyber insurance premiums could even exceed USD 50 billion by 2030.[3]

A good example of why premiums are increasing are cyber incidents like Wannacry, a ransomware attack from 2017 that infected 200,000 computers across 150 countries.[4] Affected systems included hospitals, factories and transportation systems. It is estimated that this cybercrime caused losses worth USD 4 billion worldwide.

That same trend is present in the Netherlands. Data from the Data Analytics Centre of the Verbond van Verzekeraars[5] shows that the cyber insurance market increased from EUR 10 million in 2015 to EUR 65 million in 2022. This is no surprise as the threats have also increased at an extreme rate. Last year, data breaches at NS, VodafoneZiggo and other companies leaked the data of over 2 million individuals.[6] Even more costly was a ransomware attack on the Dutch football association KNVB, which allegedly paid EUR 1 million to decrypt its data.

In this paper, the Dutch cyber insurance landscape will be discussed, followed by an analysis of the major cyber insurances. After that, the underwriting and risk management practices will be reviewed. Finally, the regulatory environment and future of the cyber insurance market will be analysed.

Dutch cyber threat landscape

In recent years, the amount and severity of cyber incidents has increased exponentially, including within the Netherlands. The type of incidents also varies widely and is constantly changing. In Figure 1 and Figure 2, the amount and type of incidents over the past eight years are shown, as reported by Datalekt, an online database for Dutch cyber incidents.[7] It is clear that data breaches occur most often, while transparency reports (data requests from government or private entities, detailing their data privacy and security measures) occur the least. Note that this only includes the reported incidents, and that the true amount will likely be much higher due to unreported events. The damage that comes from these incidents is often not directly visible, as it will often come in the form of lost business, reputation damage or loss of productivity. When there is a ransom involved, the amount is often not disclosed to prevent reputational damage. According to research by insurer Hiscox, the Netherlands even ranks second in terms of median costs incurred per firm.[8] More recently, the emergence of artificial intelligence (AI) has also introduced new cyber threats. Examples of recent threats that use AI include fake (video) phone calls[9] and phishing attempts, and AI can also be used for finding new digital vulnerabilities in software. The use of public chatbots using generative AI has also increased the risks of data breaches.

1 Guerriero, K.W., Bourdeau, T., & Raphael, S. (10 October 2023). Is Cyber Insurance Still Relevant for the Captive Market? Milliman White Paper. Retrieved 14 May 2024 from https://www.milliman.com/en/insight/is-cyber-insurance-still-relevant-for-captive-market?trk=feed_main-feed-card_reshare_feed-article-content#1.

2 Fitch Ratings (31 January 2023). Recent ILS Cyber Bond Issuance Encouraging for (Re)Insurers. Retrieved 14 May 2024 from https://www.fitchratings.com/research/insurance/recent-ils-cyber-bond-issuance-encouraging-for-re-insurers-31-01-2023.

3 Howden (5 July 2023). Howden predicts global cyber insurance premiums could exceed USD 50 billion by 2030. Retrieved 14 May 2024 from https://www.howdengroup.com/news-insights/howden-predicts-global-cyber-insurance-premiums-could-exceed-usd-50-billion-by-2030.

4 Kaspersky. What is WannaCry ransomware? Retrieved 14 May 2024 from https://www.kaspersky.com/resource-center/threats/ransomware-wannacry.

5 Published statistics by Verbond van Verzekeraars. Retrieved 14 May 2024 from https://www.verzekeraars.nl/publicaties/actueel/markt-cyber-verdubbeld and https://www.verzekeraars.nl/verzekeringsthemas/schade/cyber.

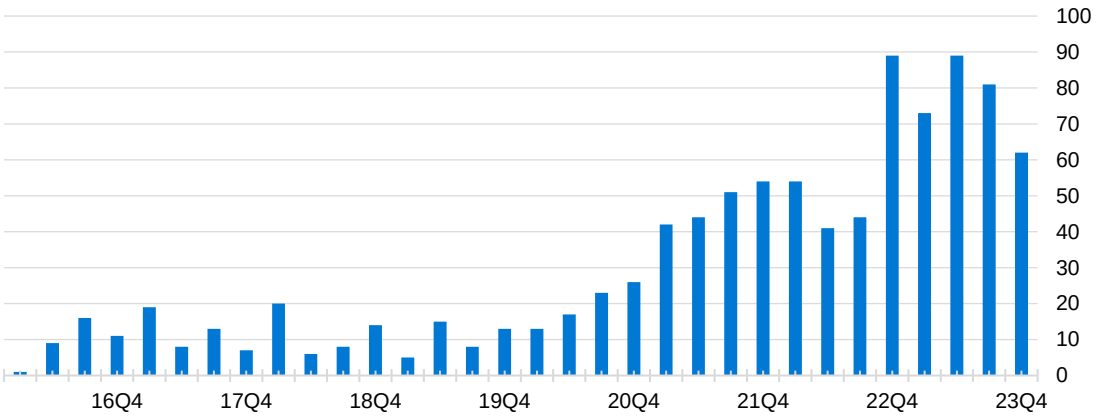
6 Kasteleijn, N. & Moorman, J. (30 March 2023). Data Breach of Dutch Companies Is Increasing: At Least 2 Million Customers Affected. NOS News. Retrieved 14 May 2024 from https://nos.nl/artikel/2469510-datalek-nederlandse-bedrijven-steeds-groter-zeker-2-miljoen-klanten-getroffen.

7 DataLekt. Overview: All Cyber Incidents. Retrieved 14 May 2024 from https://www.datalekt.nl/home/overzicht-alle-cyber-incidenten/.

8 Hiscox. Hiscox Cyber Readiness Report 2023. Retrieved 14 May 2024 from https://www.hiscoxgroup.com/sites/group/files/documents/2023-10/Hiscox-Cyber-Readiness-Report-2023.pdf.

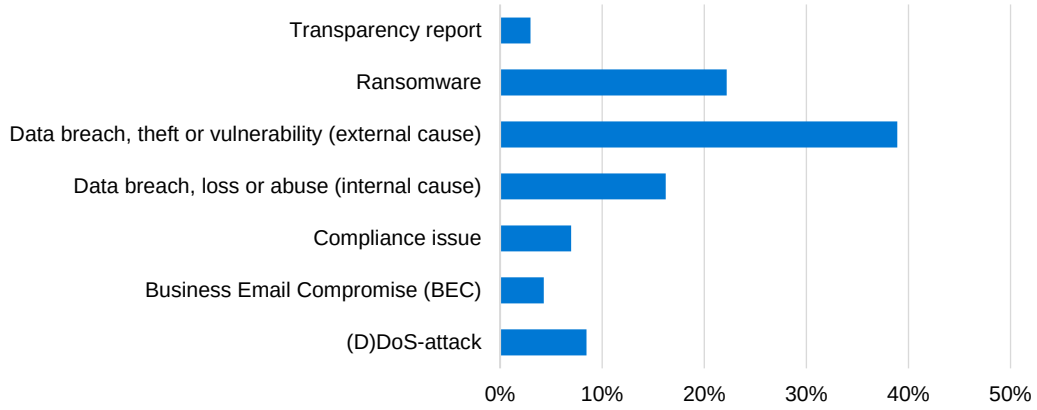
9 NRC. Fraud attempt with AI clone of CEO of online bank Bunq. Retrieved 14 May 2024 from https://www.nrc.nl/nieuws/2023/10/04/fraudepoging-met-ai-kloon-van-topman-onlinebank-bunq-a4176143 (subscription required).

FIGURE 1: REPORTED CYBER INCIDENTS PER QUARTER IN THE NETHERLANDS



Source: DataLekt.NL.

FIGURE 2: TYPE OF REPORTED CYBER INCIDENT FROM 2016 TO 2023



Source: DataLekt.NL.

Dutch cyber insurance market and key players

In the Netherlands, the market consists of different carriers, brokers and partnerships. Carriers in the Netherlands offer a range of cyber insurance products, mainly tailored to the corporate market, but in recent years also to the retail market. This is line with trends observed in the general European market for cyber insurance, as surveyed recently by the European Insurance and Occupational Pensions Authority (EIOPA).[10]

While companies often require specific insurance (with high insured sums), retail customers (individuals or small businesses) typically have lower risk profiles and require a smaller coverage. Key carriers for corporate clients in the Netherlands include AIG, Allianz, Achmea (Centraal Beheer), Chubb, De Goudse and Hiscox.

Brokers such as Aon, Howden, Marsh and WTW play a crucial role in connecting businesses with suitable cyber insurance policies. They help clients with the possible cyber insurance terms and provide advice on the appropriate type and amount of coverage based on specific risk exposures.

Furthermore, partnerships between insurance companies and cybersecurity and/or law firms are becoming increasingly common. These partnerships enable insurance providers to offer their clients additional services such as risk assessments, incident response services, compliance and cybersecurity training.

10 EIOPA (30 April 2024). Report on the Digitalisation of the European Insurance Sector. Retrieved 14 May 2024 from https://www.eiopa.europa.eu/document/download/6ca9e171-42b9-44d7-a2e6-beaf0134ecb8_en?filename=Report%20on%20the%20digitalisation%20of%20the%20European%20insurance%20sector.pdf.

The market has also seen the emergence of captives and reinsurers, as well as the use of cyber insurance-linked securities (ILS) and catastrophe (CAT) bonds. These instruments can be a useful tool to transfer some of the risk from the insurer to second or third parties. However, due to the concentrated nature of current cyber insurance coverage, cyber events could have severe impacts on insured portfolios. This high concentration risk and corresponding volatility has restrained appetite among reinsurers and capital markets for these risk transfer mechanisms. According to internal research conducted by analytics and data provider PCS,[11] there are around 250 companies globally with at least USD 200 million in cyber insurance. Only five insured losses in this pool would wipe out the roughly USD 1.1 billion in yearly premium they generate—a bit more than 20% of global cyber insurance premium.

On the demand side, the picture is somewhat mixed. The recent growth in gross premiums and claims in the Belgium, Netherlands and Luxembourg (Benelux) region has been driven by a combination of factors, including changes in the threat landscape (and awareness thereof), market competition and the regulatory environment. However, recent economic strain from COVID-19 and rising inflation rates has led some companies to view cyber insurance as a luxury. As a result, the premium volumes are not fully keeping pace with the rise in frequency and severity of cyber incidents such as data breaches and ransomware attacks.

Coverages offered

The cyber risk insurance market offers a wide range of coverages to protect businesses (both corporate clients and smaller businesses) and individuals (retail clients) from several types of cyber threats. These coverages help to mitigate different risks, which can be helpful for companies with a certain risk appetite. These coverages can include:

- **Cyber extortion**: This coverage is designed to protect against ransomware attacks and other forms of cyber extortion. It typically covers the cost of specialist services to respond to the incident and, in some cases, the ransom payment itself.
- **Cyber fraud and theft:** This coverage provides protection against financial losses resulting from cyber fraud or theft, and can include phishing attacks or unauthorised fund transfers.
- **Business/IT/network disruption:** This coverage compensates for the loss of income and increased costs of operation due to a disruption in the insured party's IT systems or network caused by a cyber incident.
- **Data confidentiality breaches:** This coverage addresses the financial consequences of data breaches, including the costs of notifying affected individuals, credit monitoring services and potential regulatory fines and penalties, including those under the General Data Protection Regulation (GDPR).
- **Legal expenses:** This coverage pays for the legal costs associated with responding to a cyber incident, such as hiring a lawyer or defending against lawsuits.

The maximum coverage provided by a policy typically depends on the premium. However, recent developments in the market have seen rates going up and coverage limits going down. These changes are driven by the increasing risk and uncertainty associated with cyber threats. This is only expected to increase in the future, because the maximum potential damage will likely increase.

In terms of pricing strategies, insurers typically consider many dimensions and they are based on a risk assessment. This includes standard factors like the insured party's industry, turnover and size. However, also more nuanced factors are looked at like cybersecurity measures (e.g., employee training) and the level of awareness in the insured party's industry (e.g., IT vs. hospitality). Prices for smaller companies or individuals are usually fixed, based on the factors described earlier. Their needs focus more on understanding the risks and outsourcing of the IT infrastructure. Larger companies might get a custom offer, depending on the specific needs and vulnerabilities of the company, which might include reputation, the type and amount of data handled and setting up a robust IT infrastructure.[12]

Most cyber insurance policies also directly include preventive measures against cybercrime, such as risk assessments, cybersecurity training and incident response planning. After an incident, insurers often provide expert help to manage the crisis and mitigate the damage. This additional help usually benefits both the insurer and the company or individual by limiting the probability and severity of such an incident. Many insurers offer these risk management services, either directly or through partners. For example, NN offers its retail clients a service called Cyberwacht,[13] which provides 24/7 assistance to customers in the event of a cyber incident. Other insurers offer risk management services through external providers, like the partnerships mentioned in the previous section.

11 Johansmeyer, T. (11 January 2021). Cybersecurity Insurance Has a Big Problem. Harvard Business Review. Retrieved 14 May 2024 from https://hbr.org/2021/01/cybersecurity-insurance-has-a-big-problem.

12 EIOPA (2018). Understanding Cyber Insurance – A Structured Dialogue With Insurance Companies. Retrieved 14 May 2024 from https://www.eiopa.europa.eu/document/download/7cec5eef-4b6d-4cd7-ad0f-b4add0a3fe17_en?filename=Understanding%20Cyber%20Insurance%20-%20Report.

13 See https://verzekerd.decyberwacht.nl/.

Figure 3 shows the variation in coverages offered to corporate clients by the largest cyber insurers in the Netherlands. For different incidents, assessments have been made as to whether the losses incurred are covered or not by the policies offered. Most insurance policies are in line with each other. All policies cover loss of business, network interruptions and expert help. The major differences between the policies primarily lie in their coverage around third-party involvement, system errors and human error. The coverage is similar to those of other European insurers (as surveyed recently by EIOPA[14]) and is in some cases even more complete than the average cyber insurance offered elsewhere in Europe.

FIGURE 3: POLICY COVERAGE OF MAJOR CYBER INSURANCES FOR CORPORATE CLIENTS IN THE NETHERLANDS

COVERAGE PER INSURER	AIG[15]	ALLIANZ[16]	CENTRAAL BEHEER[17]	CHUBB[18]	DE GOUDSE[19,20]	HISCOX[21]
NETWORK INTERRUPTION						
Loss of business income due to cyber incident	y	y	y	y	y	y
Business interruption	y	y	y	y	y	y
Damage to intangible assets	n	n	n	n	n	n
Damage to tangible assets (products liability)	n	n	n	n	n	n
Loss due to outside provider security or system failure	y	n	n	n	n	y
Loss due to system failure or human error	y	n	y	y	n	n
CYBER EXTORTION						
Cost of ransom payment	y	y	y	y	n	y
Cyber specialist	y	y	y	y	y	y
ELECTRONIC DATA INCIDENT						
Loss due to accidental damage of computer system	y	y	n	n	n	n
CYBER THEFT						
Financial loss from fraudulent electronic transfer of funds	y	y	y	y	n	y
Data restoration	y	y	y	y	y	y
Extra expense	y	y	y	y	y	y
System cleanup cost	y	y	y	y	y	y
Administrative investigation and penalties	y	y	y	y	y	y

Underwriting and risk management practices

The underwriting process for cybersecurity insurance involves a comprehensive risk assessment. This includes evaluating a company's cybersecurity practices, IT infrastructure, data protection measures and incident response plans. Factors such as the size of the company, its industry (and corresponding cybersecurity awareness), the type and amount of data handled and its dependence on third-party providers are also considered. The use of technology and data analytics is crucial in this process, with databases from established third parties providing valuable insights into cyber incidents. Continued investments into modelling solutions are needed to help carriers manage and price (systemic) exposures.

14 EIOPA (30 April 2024). Report on the Digitalisation, op cit.

15 AIG. ProfessionalEdge Cyber. Retrieved 14 May 2024 from https://www.aiginsurance.nl/content/dam/aig/emea/netherlands/documents/documenten-toolkit/nl-fincy-10040523.pdf.

16 Allianz. Cyberverzekering. Retrieved 14 May 2024 from https://www.allianz.nl/content/dam/onemarketing/benelu/allianz-nl/local/1/1000125-178-07.pdf.

17 Central Beheer. Cyberverzekering. Retrieved 14 May 2024 from https://www.centraalbeheer.nl/-/media/files/zakelijk/polisvoorwaarden/2024/cyb24-cyberverzekering.pdf.

18 Chubb. Cyber Enterprise Risk Management (ERM). Retrieved 14 May 2024 from https://www.chubb.com/content/dam/chubb-sites/chubb-com/benelux-nl/for-businesses-brokers/cyber-enterprise-risk-management/documents/pdf/chubb-cyber-erm-brochure_nl-use03-19_web.pdf.

19 De Goudse. Spellregels Cyberrisk. Retrieved 14 May 2024 from https://www.goudse.nl/-/media/files/goudse/spelregels-cyberrisk-992616.pdf.

20 De Goudse. Cyber Insurance. Retrieved 14 May 2024 from https://verzekeringskaarten.nl/goudse/cyberrisk.

21 Hiscox. CyberClear by Hiscox Polisvoorwaarden. Retrieved 14 May 2024 from https://adviseur.hiscox.nl/sites/adviseurnl/files/2022-09/Polisvoorwaarden%20CyberClear%20by%20Hiscox%20HCC-202201.pdf?_ga=2.128426380.142643525.1712232997-539596750.1712232997&_gl=1*182zlhg*_ga*NTM5NTk2NzUwLjE3MTIyMzI5OTc.*_ga_C7P4FCC3E2*MTcxMjIzMjk5OS4xLjAuMTcxMjIzMjk5OS42MC4wLjA.

These modelling situations should not rely solely on past data and should also consider the adversarial nature of cyber risk. Cyber threats evolve and adapt over time and it must be assumed that new possibilities for future attacks will emerge.

In turn, better articulation of results to alternative capital providers is a key requirement to unlocking more (re)insurance capacity. Reinsurance capacity is of significant importance to cybersecurity insurance, with approximately 45% of cyber insurance premiums currently ceded to reinsurers according to a recent report by Howden.[22] Notwithstanding the emergence of other options like CAT bonds and ILS to transfer cyber risk to the capital markets, there is still a need for more capital in the cyber insurance market. However, as noted above, the limited appetite of reinsurers and capital markets for cyber exposures can be attributed to the high concentration risk towards cyber threats and corresponding volatility. As such, large insurers are seen to utilise reinsurance contracts where they retain more risk (e.g., as excess-of-loss and tail-risk occurrence covers) compared to standard quota share contracts. These structures are also more in line with the preferences of ILS investors and unlock more capacity to transfer cyber risks towards capital markets. In conjunction, some carriers have implemented a number of exclusions and higher deductibles to become more comfortable managing the attritional losses.

In response to the substantial business threats cyber risks pose and the low capacity for cyber (re)insurance, the use of captives has seen an increasing trend in the cyber market.[23] Companies that understand their cyber exposures better than their insurers are considering setting up captive insurers and securing as much reinsurance behind the captive as possible to increase consumer confidence, market stability and risk diversification.

Although various options for underwriting exist, the limited options to reduce and/or transfer risk, together with the increasing loss ratios, force insurers to increase their premiums.[24]

Regulatory environment

Since 2018 the General Data Protection Regulation (GDPR) has become effective in the European Union. The GDPR has influenced the cyber risk insurance landscape in various ways.

The regulation demands strong cybersecurity measures, thereby impacting cyber risks. It has also intensified data privacy concerns, leading to an increase in data breach risks. The GDPR fines and penalties for data breaches and noncompliance have been a significant factor in shaping the treatment of data breaches in policy wording. Additionally, GDPR compliance has become a critical component of underwriting and risk assessments. Since 2018, the total of all GDPR fines in the European Union sum up to almost EUR 4.5 billion.[25]

Besides the GDPR, several other regulations have come into effect more recently. On the policyholder side, another European measure has been in effect since 2023, in the form of the Network and Information Security (NIS2) directive.[26] NIS2 aims to enhance the security of network and information systems within the EU by requiring operators of critical infrastructure and essential services to implement appropriate security measures and report any incidents to the relevant authorities. The insurance industry has indicated that access to cyber incident data reported under the NIS2 directive would benefit cyber insurance offerings, and stresses the importance of harmonised incident reporting through further technical guidance by the European Union Agency for Cybersecurity (ENISA).[27] Access to harmonised cyber incident data is expected to enhance a uniform and common understanding of cyber threats and incidents across the EU and to improve cyber underwriting practices as such. In addition, EIOPA proposed a new template on cyber underwriting, S.14.03, as a part of the 2020 review of Solvency II (SII).[28] This template will provide a standardised framework for assessing cyber risk, which facilitates more accurate and consistent underwriting practices.

Regarding insurers' own cybersecurity, the Digital Operational Resilience Act (DORA) is an EU regulation that will apply as of 17 January 2025.[29] DORA is set to introduce broad requirements for insurance (and other financial) companies in IT risk management, incident reporting, stress testing, and third-party arrangements. DORA's aim is to make sure that the financial sector in Europe can stay resilient in the event of a severe operational disruption. Moreover, in recently agreed provisional amendments to the Solvency II directive a new Pillar 2 requirement has been included that the operational risk management system is to include cybersecurity.[30]

22 Howden predicts global cyber insurance premiums, op cit.

23 Guerriero, K.W., Bourdeau, T., & Raphael, S. (10 October 2023), op cit.

24 Johansmeyer, T. (11 January 2021), op cit.

25 According to data compiled until March 2024 by enforcementtracker.com provided by CMS Law.Tax.

26 The NIS2 directive is available at: https://eur-lex.europa.eu/eli/dir/2022/2555.

27 Insurqnce Europe (18 March 2021). Position on the Review of EU Rules on the Security of Network and Information Systems (NIS2). Position Paper. Retrieved 14 May 2024 from https://www.insuranceeurope.eu/publications/1635/position-on-the-review-of-eu-rules-on-the-security-of-network-and-information-systems/download/Position+on%20the%20review%20of%20EU%20rules%20on%20the%20security%20of%20network%20and%20information%20systems.pdf.

28 More details on EIOPA's proposal for the new Quantitative Reporting Template (QRT) are available at https://www.eiopa.europa.eu/document/download/e248a973-3a23-4719-9673-d36a6f219d30_en?filename=Report%20on%20quantitative%20reporting%20templates.pdf.

29 EIOPA. Digital Operational Resilience Act (DORA). Retrieved 14 May 2024 from https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en.

30 See page 132 of the provisional amendments to the SII directive (agreed between the European Parliament, European

Council and European Commission), available at https://data.consilium.europa.eu/doc/document/ST-5481-2024-INIT/en/pdf.

With these evolvements in regulation, insurers need to adapt both their underwriting and risk management practices. This adaptation is not only needed to ensure compliance regarding their own cybersecurity, but also to provide robust coverage for their clients.

Non-affirmative (silent) risks

Non-affirmative or silent cyber risks refer to potential exposures in traditional insurance policies that do not explicitly include or exclude cyber risks. This means a policy may inadvertently cover cyber risks, leading to unexpected claims and significant losses for insurers. An example can be a cyberattack that leads to a malfunction in a company's heating/cooling system, resulting in physical damage to the building.

A stress test conducted by the National Bank of Belgium (NBB) in 2022[31] has identified silent cyber as a potential material issue for the Belgian insurance sector. For the cyber scenarios analysed, silent cyber risk drives 40% to 80% of the claims in stress. Given the similarity in general insurance products between the Netherlands and Belgium, silent cyber is also expected to be material for the Dutch insurance sector.

Currently, underwriting practices are changing, with insurers increasingly seeking to clarify the extent of cyber coverage in their policies. This often involves either explicitly excluding cyber risks or affirmatively including them and pricing them accordingly. A recent example is CyberGerust from Univé,[32] which is an additional cyber insurance and service for retail clients, by default included in their home contents and liability insurance. It includes a help desk and coverage for damage to the client's (or others') electronic devices after a hack.

These changes are very important for maintaining the sustainability of the cyber insurance market. By clearly defining the scope of coverage, insurers can make sure that they are adequately pricing their policies and not exposing themselves to unanticipated cyber-related claims.

However, the process of identifying and quantifying silent cyber risks can be challenging due to the complexity of cyber threats. Insurers will need to continually refine their underwriting practices (e.g., exclusions) and risk management strategies to stay ahead of these risks. As stated earlier, investments into modelling solutions and databases are needed to adequately assess and price these risks.

Outlook and conclusion

When looking at the future of the cyber insurance industry, there is a lot of uncertainty. But what can be said with certainty is that the market will grow, with global projections reaching USD 25 billion by 2025 and even more than USD 50 billion by 2030. This increase in volume will be driven by increasing digital reliance, escalating threat landscape and growing awareness of cyber risks. It will also come with an increase in volatility, as the size and frequency of cyber threats will only increase.

The biggest challenges that insurers face are the complexity and adversarial nature of cyber threats, low availability of historical data and its limited use to predict new threats, standardisation in policies, pricing and underwriting practices and silent cyber risks.[33] While all of these challenges can be solved by spending money and time in the needed research, insurers have to be sure not to underestimate these risks.

The regulatory landscape is also quickly changing. The GDPR, DORA and NIS2 regulations all try to force companies to increase their cybersecurity.[34] The recent increase in cyberattacks has shown that this is necessary for secure and reliable financial services, where insurance companies are no exception.

Lastly, the recent emergence of artificial intelligence (AI) is also expected to significantly affect the cyber industry. Not only can it be used to improve cybersecurity measures (e.g., detective and predictive algorithms[35]), but also malicious parties can make use of it.

Even with all of the above-mentioned challenges, the outlook for the cyber insurance industry is positive. This is mainly due to the increasing demand. Improvements in data analytics and actuarial modelling can make sure the pricing of premiums is done accurately. It also looks like the much-needed capital is coming to the cyber (re)insurance market.

31 The results and recommendations from the 2022 NBB stress-test can be found at https://www.nbb.be/doc/cp/eng/2022/2022_insurance_stress_test.pdf.

32 Univé. CyberGerust with Univé. Retrieved 14 May 2024 from https://www.unive.nl/cybergerust.

33 A more extensive white paper on challenges faced by insurers providing cyber risk coverage can be found at https://www.milliman.com/en/insight/cyber-risks-what-are-the-challenges-for-insurers. For modelling solutions that reflect the adversarial nature of cyber risk, please see https://www.milliman.com/en/Products/Complexriskanalysis.

34 In another briefing note, more information can be found on what next steps (re)insurers can take for the new DORA requirements: https://ie.milliman.com/en-gb/insight/digital-operational-resilience-act-dora-next-steps-for-insurers.

35 For potential uses of data science techniques in detection and prevention by (re)insurance companies, please see https://nl.milliman.com/nl-nl/insight/data-science-potential-uses-in-risk-management.

What Milliman can do for you

Milliman consultants have considerable experience in advising insurers on their risk management and underwriting practices. Regarding cyber risks, Milliman consultants can rely on a vast global pool of expertise, research and products for their services. Moreover, Milliman consultants also have the expertise and experience to help with the latest data science and AI techniques and to provide support in building detective and predictive algorithms. For an overview of where Milliman consultants can help in the area of cyber risk, data science and AI, please visit:

- https://nl.milliman.com/nl-nl/data-science-artificial-intelligence
- https://www.milliman.com/en/risk/cyber-risk

Milliman

Milliman is among the world's largest providers of actuarial, risk management, and technology solutions. Our consulting and advanced analytics capabilities encompass healthcare, property & casualty insurance, life insurance and financial services, and employee benefits. Founded in 1947, Milliman is an independent firm with offices in major cities around the globe.

milliman.com

CONTACT

Joris van der Moore
joris.vandermoore@milliman.com

Joost Broens
joost.broens@milliman.com

Sjoerd Brethouwer
sjoerd.brethouwer@milliman.com