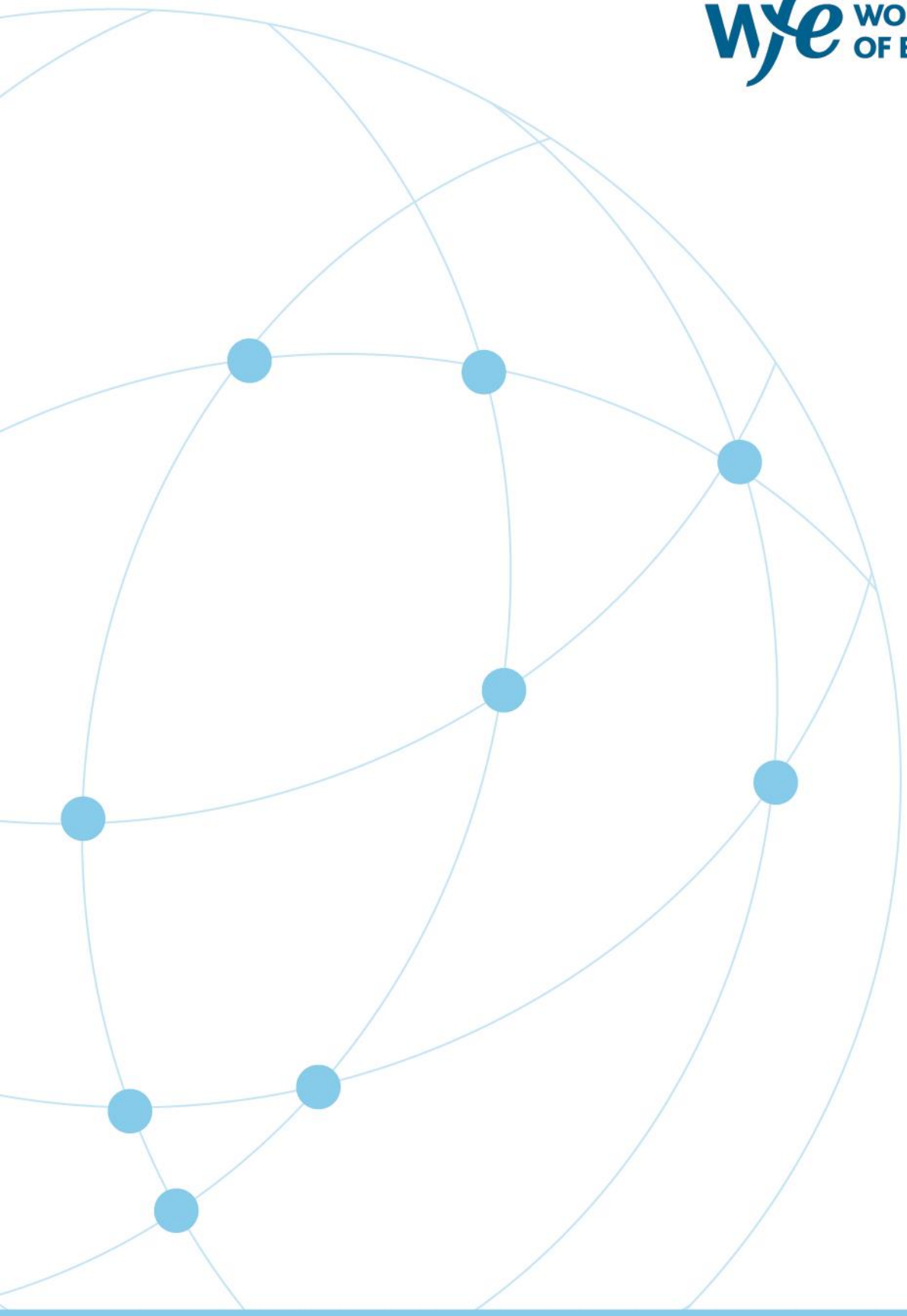
WORLD FEDERATION OF EXCHANGES



A WFE Snap Benchmarking report of Cyber Insurance

June 2024

Background

Established in 1961, the WFE is the global industry association for exchanges and clearing houses. Headquartered in London, it represents the providers of over 250 pieces of market infrastructure, including standalone CCPs that are not part of exchange groups. Of our members, 36% are in Asia Pacific, 43% in EMEA and 21% in the Americas. The WFE's 87 member CCPs and clearing services collectively ensure that risk takers post some $1.3 trillion (equivalent) of resources to back their positions, in the form of initial margin and default fund requirements. The exchanges covered by WFE data are home to over 55,000 listed companies, and the market capitalization of these entities is over $111tr; around $124tr in trading annually passes through WFE members (at end-2023).

The WFE is the definitive source for exchange-traded statistics and publishes over 350 market data indicators. Its free statistics database stretches back more than 40 years and provides information and insight into developments on global exchanges. The WFE works with standard-setters, policy makers, regulators and government organisations around the world to support and promote the development of fair, transparent, stable and efficient markets. The WFE shares regulatory authorities' goals of ensuring the safety and soundness of the global financial system.

With extensive experience of developing and enforcing high standards of conduct, the WFE and its members support an orderly, secure, fair and transparent environment for investors; for companies that raise capital; and for all who deal with financial risk. We seek outcomes that maximise the common good, consumer confidence and economic growth. And we engage with policy makers and regulators in an open, collaborative way, reflecting the central, public role that exchanges and CCPs play in a globally integrated financial system.

Website: www.world-exchanges.org
Twitter: @TheWFE

If you have any further questions, or wish to follow-up on our contribution, the WFE remains at your disposal. Please contact:

Chhavi Sinha, Regulatory Affairs Manager: csinha@world-exchanges.org

Richard Metcalfe, Head of Regulatory Affairs: rmetcalfe@world-exchanges.org

Nandini Sukumar, Chief Executive Officer: nsukumar@world-exchanges.org

1. Introduction

a) Overview of the Purpose of the survey

The WFE members of the Global Cyber Security Working Group (GLEX) had expressed challenges around securing cyber insurance, and stated that a benchmarking exercise on the topic could prove to be beneficial for the entire membership. It was therefore, decided to conduct a snap survey to determine the trends in the cyber security insurance and challenges faced by members around costing, coverage, barriers and other relevant factors.

b) Importance of Cyber Insurance in Risk Management

Cyber insurance has become a vital part of an organisation's risk mitigation strategy in the present era of cyber-related incidents. Cyber insurance can help ease financial losses associated with cyber incidents such as data breaches, ransomware attacks, business interruption, and legal liabilities. It allows organisations to transfer a portion of their cyber risk to insurance companies, thereby, providing a layer of risk mitigation and financial stability.

By having cyber insurance coverage, organisations can enhance their resilience against cyber threats. Knowing that they have financial support in case of a cyber incident, organisations can focus on implementing robust cyber security measures and incident response plans.

c) Objectives of the Report

The objective of the report is to exhibit the results of the survey and bring to attention areas of analysis and research, further development and inadequacies, faced by the exchange and CCP community.

2. Survey Methodology

In the year 2023-24, the WFE conducted a snap-survey on various aspects of Cyber Insurance amongst its members of GLEX, to gauge levels of interest in key questions. Seven GLEX members across multiple jurisdictions, including Asia-Pacific, Europe, the Middle East, and the Americas participated in the survey.

3. Executive summary

This Benchmarking report highlights the scope of cyber insurance across WFE membership. The report also unfolds the main barriers to getting a cyber insurance including lack of cyber insurance providers, costing and risk assessment challenges, coverage, and high deductibles. In terms of the scope of cyber insurance policies coverage, the survey underscores data breaches, business interruptions and other constituents like, network security liability, and reputational damage as being covered by members' cyber insurance policies[1]

The Benchmarking report emphasises that there is still scope for improvement or advancement in the field of securing a cyber insurance, and enhancing its coverage and size.

The WFE urges regulators and policymakers to take measures that can encourage insurer participation, expand market access, and support risk assessment and management to help enhance insurance availability and address gaps in coverage.

[1] Please refer to Page 6 and 7 for further explanation.

The report further captures the evolution of cyber insurance coverage over the past few years amongst the membership and emphasises the increased uptake of cyber insurance policies trend. However, it is noted that similar trends in terms of the cost of the coverage have been seen by the majority of the members.

The report concludes that the WFE will keep monitoring the area of cyber insurance, its evolution and barriers to securing it.

4. Analysis of Survey Results

This report is based on the responses of WFE members who operate across Europe, Asia-Pacific (APAC) and America to a set of 22 qualitative questions. Members of the GLEX Group were asked questions on their staffing, principal market coverage, existence of cyber insurance, its coverage, claims, premium, regulatory requirement, and the main barriers to getting cyber insurance.

Overall, the outcome of this survey provides useful insights on the existence of the cyber insurance policies, the evolution of its coverage and the main barriers to securing cyber insurance. Some of these topics are discussed in detail in the following section:

Members firms' principal Market

The survey results cover members operating in various jurisdictions, including Asia-Pacific, Europe, the Middle East, and the Americas. A majority of the member respondents indicated operations within European jurisdictions, followed by the Asia-Pacific region and North America.

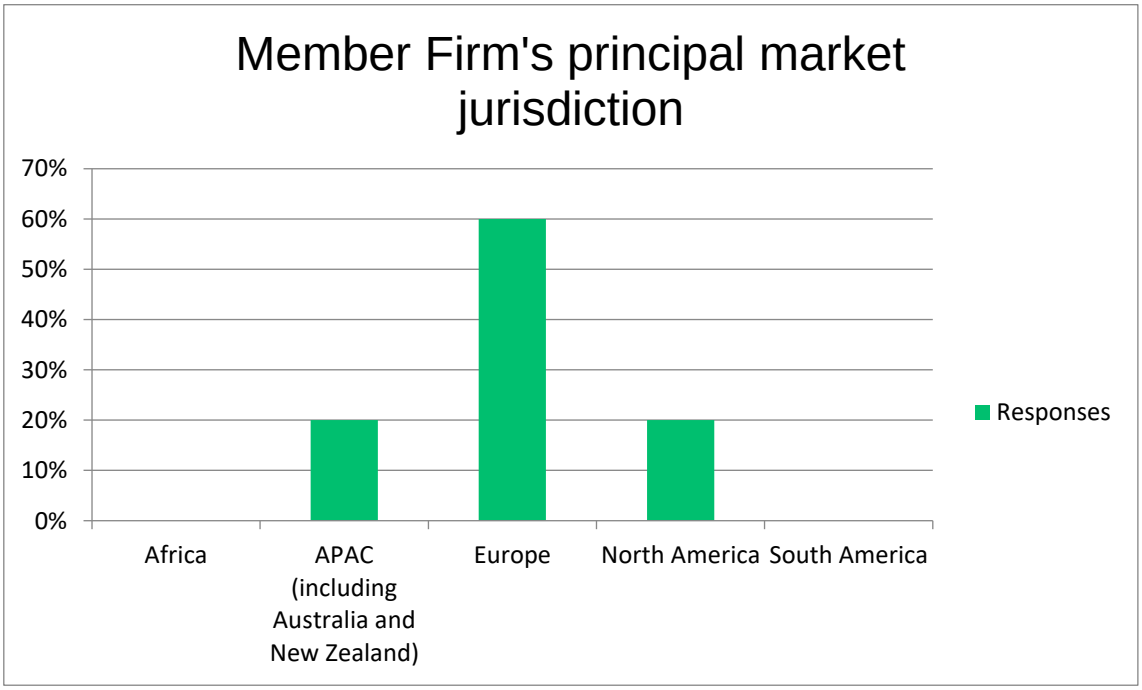


Figure 1

On the question of staffing, members indicated to have employee numbers ranging from 650 to 4500.

<u>Existence of Cyber Insurance within Membership organisation</u>

The decision of whether to obtain cyber insurance depends on a combination of factors, including risk tolerance, financial considerations, and organisational priorities. While cyber insurance can provide valuable financial protection against cyber risks, firms carefully evaluate their unique circumstances and consult with insurance professionals to make informed decisions about cyber risk management and insurance coverage.

When we asked our members whether their organisation has cyber insurance in place, about 60% of the respondent members indicated that currently they have a cyber insurance (Figure 2). Members revealed that their cyber insurance has existed for anywhere between 11 years and 4 years.

The above survey results illustrates that there is still scope for improvement or advancement in this field. Cyber insurance practice has perhaps not matured amongst many of the member organisations.

70% of respondents reported that their organisation doesn't use a self-insurance complementary to the cyber insurance.[2] They do not, in other words, "self-insure".

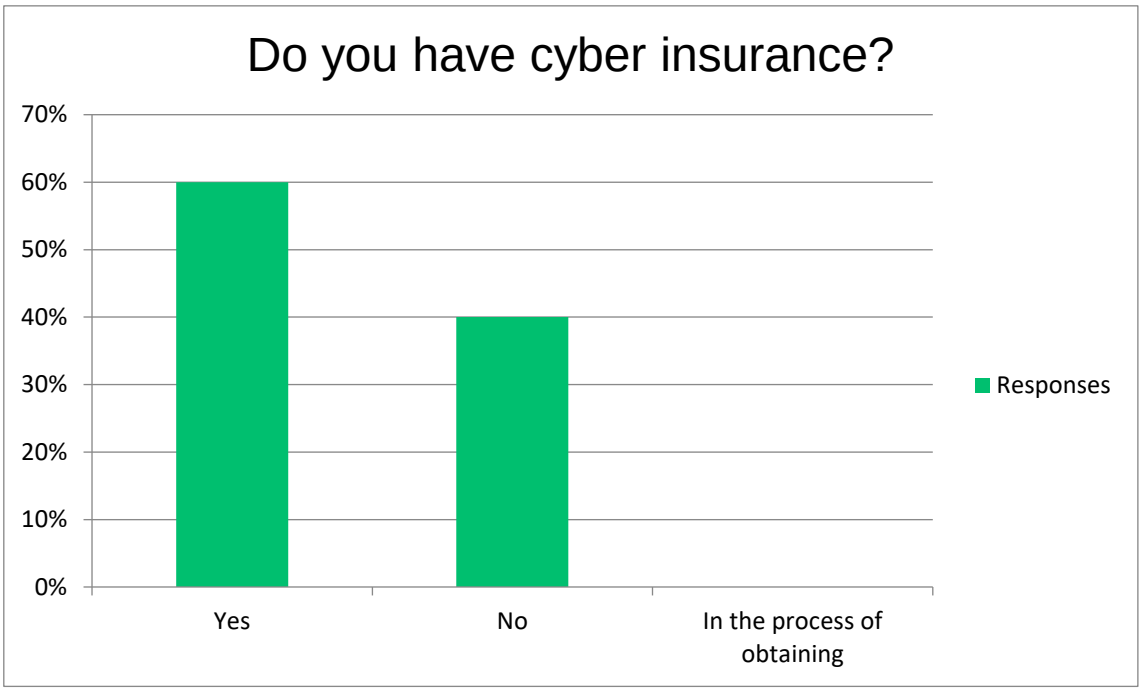


Figure 2

Cyber insurance required by Regulation

Cyber insurance requirements imposed by regulations vary by jurisdiction and industry. While some regions or sectors have implemented regulations that mandate cyber insurance coverage or certain aspects of cyber risk management, others have not yet established explicit requirements.

We asked members whether cyber insurance was required by any regulation applicable to their company. The majority of the members indicated that cyber insurance was not required by regulation for their company, however, a small percentage of members did indicate the requirement by regulation (Figure 3).

[2] Self-insurance involves setting aside your own money to pay for a possible loss instead of purchasing insurance and expecting an insurance company to reimburse you. With self-insurance, you pay for a cost such as a medical procedure, water damage, theft, or a fender bender out of your own pocket rather than filing a claim under your policy with an insurance company. Obtained from https://www.investopedia.com/terms/s/selfinsurance.asp

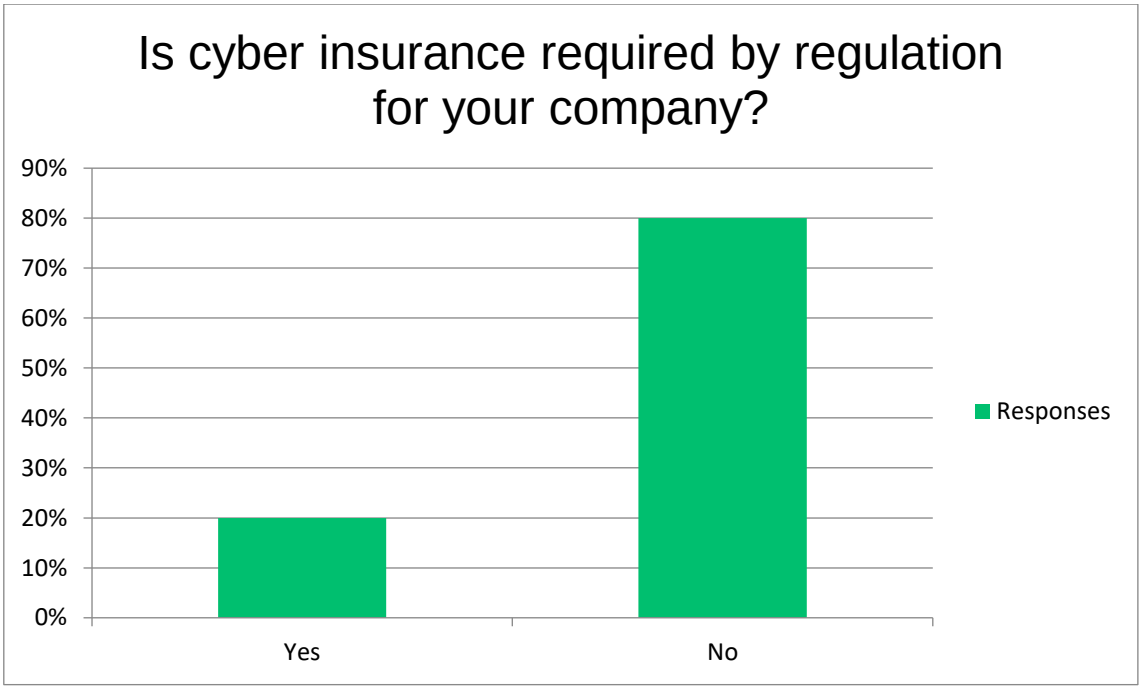


Figure 3

About 80% of the members indicated that their organisation would like to continue to have cyber insurance in the future.

5. The main barriers to getting cyber insurance

The main barriers to obtaining cyber insurance can vary depending on the organisation and industry, but common barriers include:

1. **Cost:** One of the primary barriers to obtaining cyber insurance is the perceived cost of premiums. Some organisations may view cyber insurance as an expensive investment, especially if they have budget constraints or believe that the likelihood of a cyber incident is low.

2. **Coverage:** In some regions or industries, there may be limited availability of cyber insurance coverage options. This limited market availability can restrict organisations' ability to obtain suitable cyber insurance.

3. **Risk Assessment:** Insurers often require organisations to demonstrate their cyber security measures and risk management practices before offering coverage. Any organisation with insufficient cyber security measures or a high-risk profile may face challenges in obtaining favourable terms or adequate coverage.

4. **High deductible or excess:** In insurance it is the initial amount that the insured party must pay before the insurance coverage takes effect. It is an important consideration when selecting insurance policies and balancing premium costs with financial risk exposure.

5. **Lack of providers:** Refers to a situation where there are limited options or insufficient availability of insurance companies or providers offering specific types of insurance coverage or services within a particular market or industry, such as cyber insurance.

6. **Claims Handling:** Organisations with a history of cyber incidents or claims may encounter higher premiums or difficulty obtaining coverage due to perceived risk.

WFE members have expressed challenges and barriers regarding securing a cyber insurance. We therefore asked them to indicate whether cost, coverage, risk assessment or a lack of providers were the main barriers. 80% cited a lack of cyber insurance providers as a barrier, 60% mentioned it was costing and risk assessment challenges, whereas 40% indicated that it was coverage, high deductibles and other factors such as underwriting effort (i.e. additional internal approval steps within the insurance companies), the risk of being a prime target for hackers and, consequently, the potential for significant losses. 20% said that it was due to claim handlings.

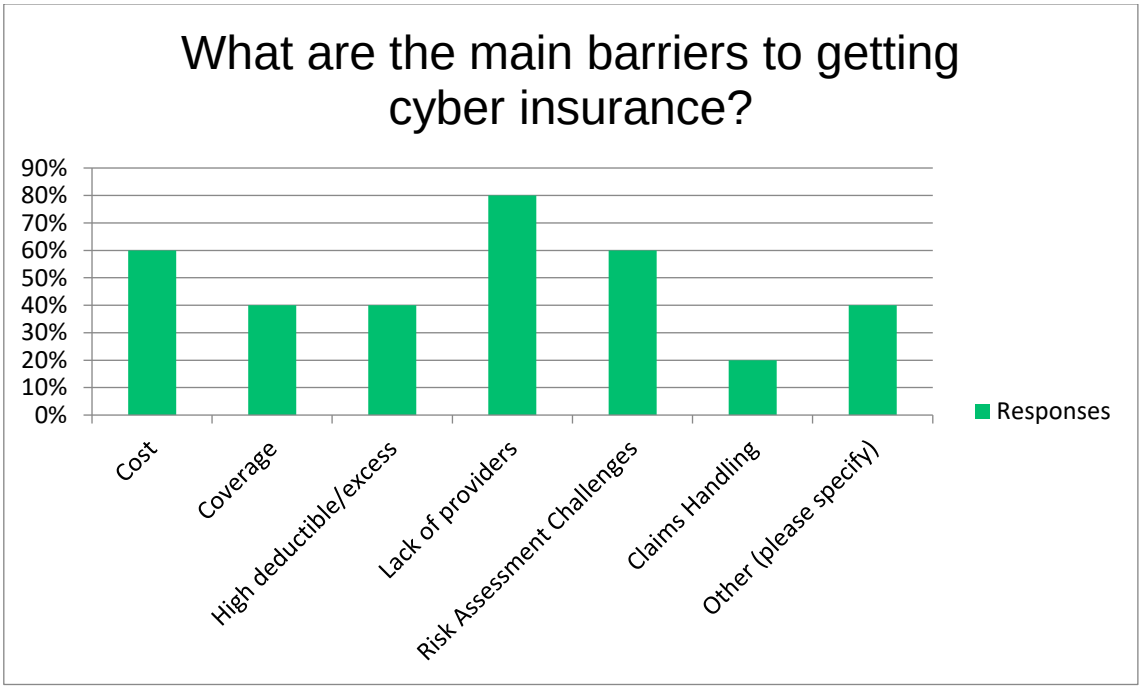


Figure 4

As reported by the European Insurance and Occupational Pensions Authority (EIOPA) in 2018, and also noted by the WFE members, cyber insurance has existed for a number of years in jurisdictions like the Americas; however the current survey suggests that in jurisdictions like Europe, the main barrier remains the shortage of providers, followed by concerns related to cost and risk assessment criteria.[3] The escalating significance of cyber insurance due to rising cyberattacks underscores the need for continued efforts in this area.

Addressing the lack of providers requires collaboration between insurance industry stakeholders, policymakers, and regulators to promote market growth, innovation, and competition. The WFE urges regulators and policymakers to take measures that can encourage insurer participation, expand market access, and support risk assessment and management to help enhance insurance availability and address gaps in coverage. Additionally, for its part, the exchange industry will look to continue fostering a constructive dialogue with insurers to navigate insurance markets effectively and identify suitable coverage options, despite market challenges.

[3] It is estimated that approximately 90% of the stand-alone cyber insurance market is located in the United States (PwC, 2016; Marsh 2016) and only approximately 5% to 9% is based in Europe, which amounts to between USD150 million and 400 million. **EIOPA, 2 August 2018, Understanding Cyber Insurance - A Structured Dialogue with Insurance Companies. Page 3**. https://www.eiopa.europa.eu/publications/understanding-cyber-insurance-structured-dialogue-insurance-companies_en

Cyber insurance coverage

Knowing the size of cyber insurance coverage helps indicate what resources organisations have in place to mitigate potential financial losses resulting from cyber incidents such as data breaches, ransomware attacks, or business interruptions.

In order to understand the extent of financial protection against cyber-related risks that the members have secured through cyber insurance, we surveyed our members about the size of their organisation's cyber insurance coverage. 70% of responders indicated that they have cyber insurance coverage of less than $25 million, while approximately 30% reported insurance coverage ranging from $25 million to $100 million.

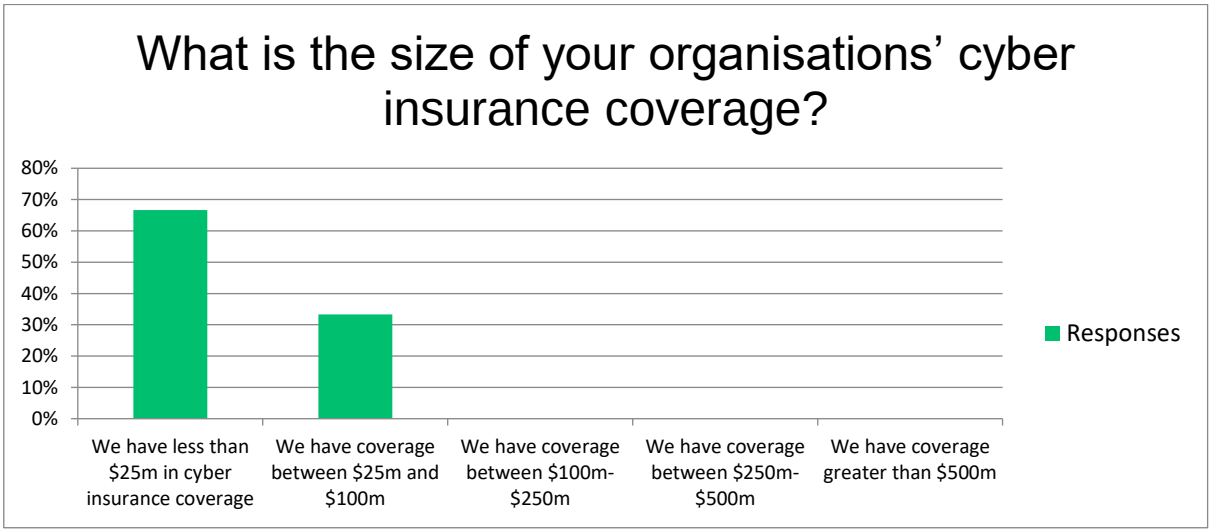


Figure 5

Scope of Cyber Insurance Policy Coverage

Cyber insurance policies typically provide coverage for a range of cyber-related risks and expenses. The specific coverage can vary depending on the insurance provider and the policy terms, but common components covered by cyber insurance policies include:

a) **Data Breach Coverage**: This includes expenses related to investigating a data breach, notifying affected individuals, providing credit monitoring services, and managing public relations.
b) **Cyber Extortion:** Coverage for costs associated with ransomware attacks or other forms of cyber extortion, including ransom payments (if necessary and permitted), and expenses related to negotiating with cyber criminals.
c) **Business Interruption Losses:** Compensation for income losses and extra expenses incurred due to a cyber incident that disrupts normal business operations.
d) **A social engineering loss:** Refers to a type of financial loss that occurs as a result of manipulation or deception of individuals within an organisation to carry out unauthorised financial transactions or divulge sensitive information.
e) **Reputational damage:** Refers to the negative impact on an organisation's reputation and public perception resulting from incidents, events, or actions that harm its integrity, trustworthiness, or credibility. In the

context of cyber incidents, reputational damage often occurs due to data breaches, cyberattacks, or other security incidents that compromise sensitive information or disrupt business operations.

f) **Digital asset:** Digital asset insurance coverage refers to insurance policies designed to protect against financial losses resulting from the theft, loss, or unauthorized access to digital assets. Digital assets encompass various types of electronic data, cryptocurrencies, virtual currencies, and other digital records stored on electronic devices or online platforms.

g) **Others:** Others can include**, System Damage and Restoration, Regulatory Fines and Legal Expenses, Third-Party Liability, etc**

The majority of the members indicated that data breaches, business interruptions and other constituents like network security liability and reputation costs were covered by their cyber insurance policy.

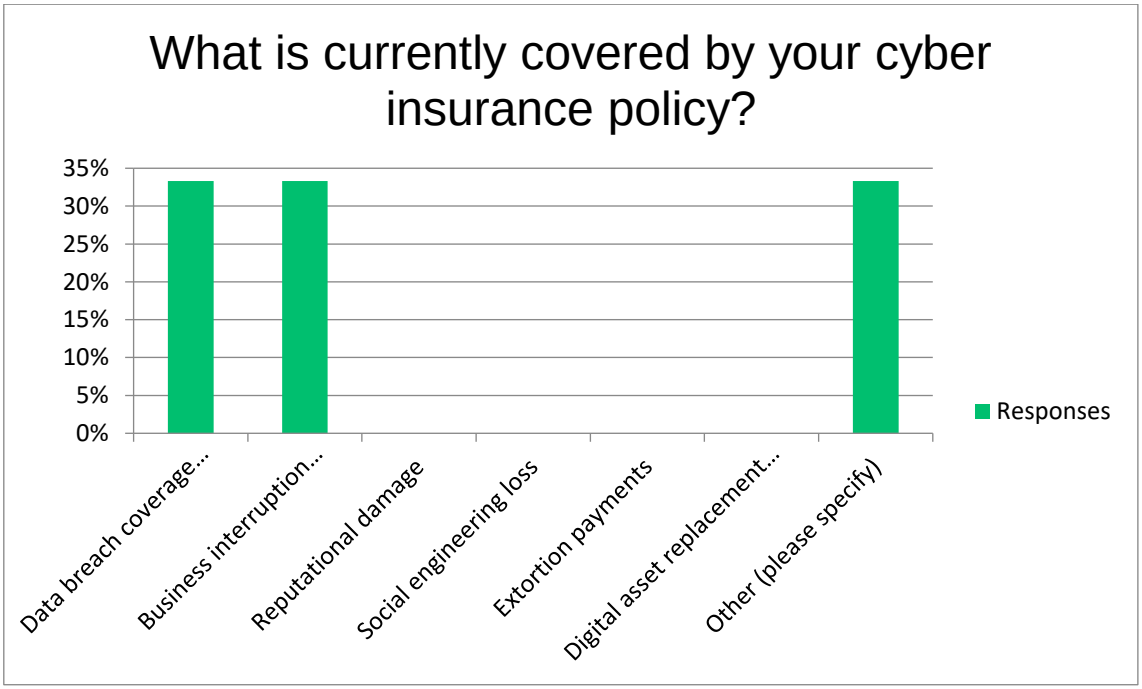


Figure 6

<u>Evolution of cyber security insurance coverage</u>

With the advancements in technology, the changing cyber threat landscape, regulatory developments and increased awareness of cyber risks among organisations; the cyber security insurance coverage has evolved across organisations.

This trend is reflected across WFE membership as well.

Previous (confidential) WFE work in 2021 suggested that the majority (~80%) of organisations had either no cyber insurance policy in place or had a policy covering less than $25m of cyber impact, suggesting that cyber insurance was being used to transfer only some of the risk associated with cyber incidents, not all of it.

The risks most commonly covered by cyber insurance policies were data breaches and business interruptions, which aligned with the respondents' view that these risk areas were of most concern for their organisations. However, respondents also said that they felt the Insurance industry isn't ready for the business as there is a lack of clarity on how insurance firms quantify cyber risk and organise pay-outs.
In the current survey, as seen in Figure 2, more members have moved to having cyber insurance. However, the majority of the members continue to have cyber insurance coverage of less than $25 million.

When asked whether their cyber insurance policy coverage would change in the future, the majority noted that no changes are expected, though some members indicated that they do plan to increase the size of their cover.

Members have suggested to repeat the survey next year and review how the scope and size of cover has evolved.

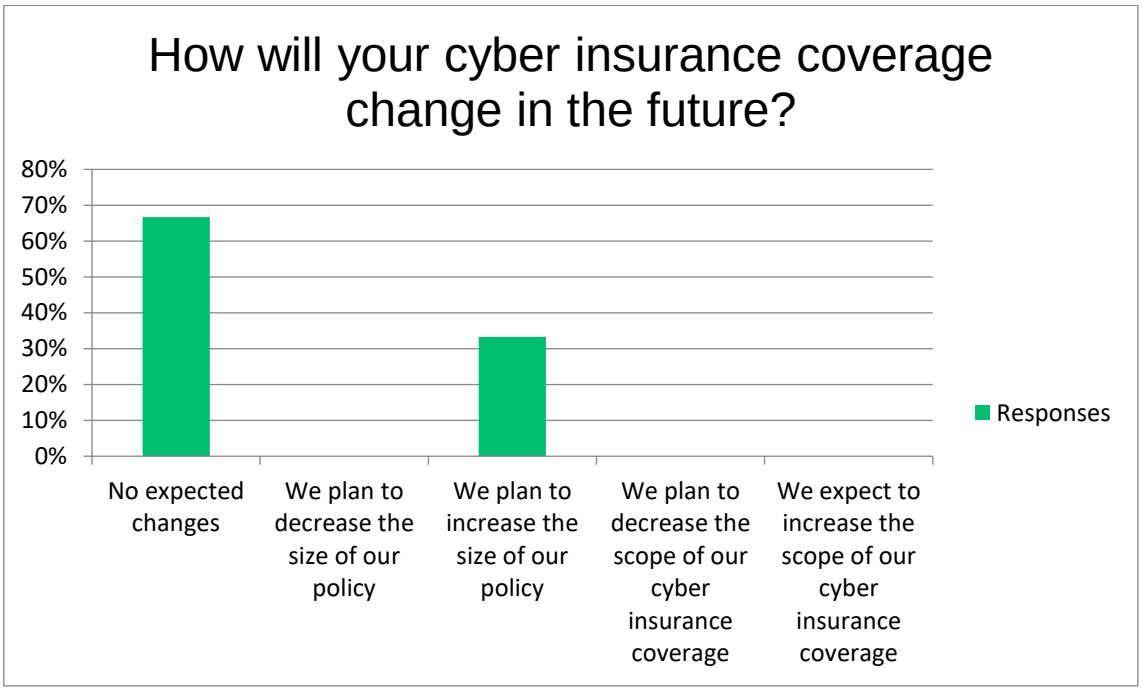


Figure 7

Members were asked if the cost of their material cyberattacks were ever more than the deductible /excess amount to recover. None of the responders said it was (Figure 8). This result is not reflective of the concerns raised by the WFE members that there wasn't enough coverage provided by cyber insurance policies to cover cyberattacks. The WFE is encouraged to look into this question again next year when the survey is repeated for its members.

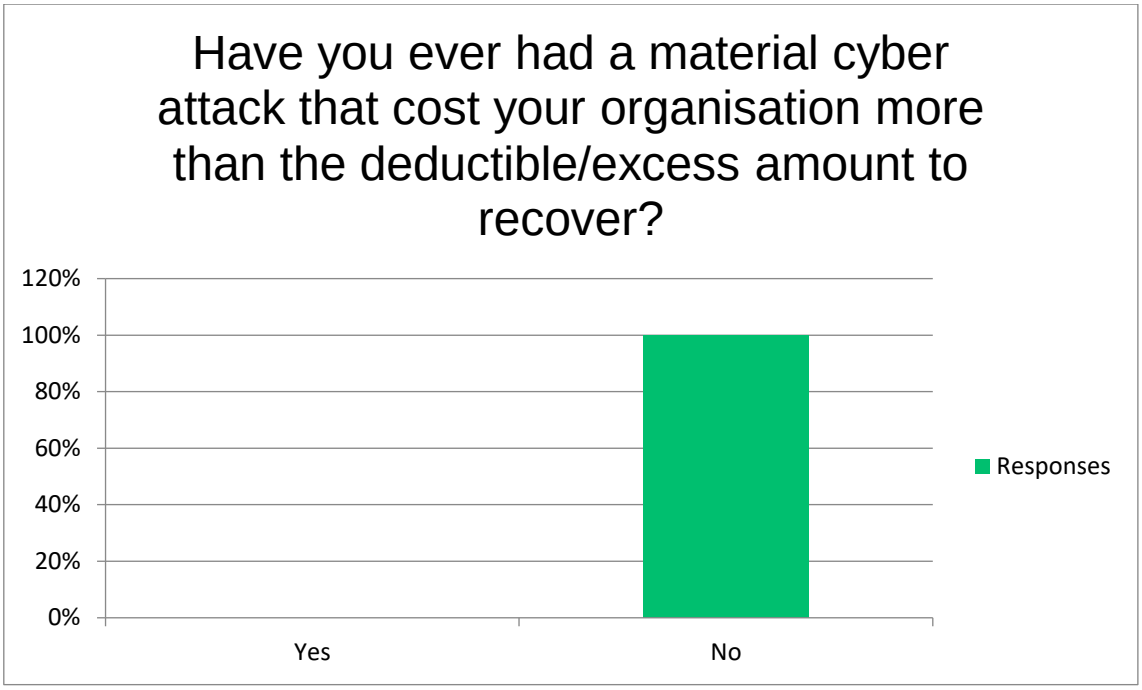


Figure 8

6. Conclusion

Although based on a limited sample size, the outcome of this survey provides useful insights on the existence of the cyber insurance policies, the evolution of its coverage and the main barriers to securing cyber insurance.

Regarding the existence of cyber insurance within membership organisations, the survey results illustrate that there is still scope for improvement or advancement in this field. The cyber insurance practise has perhaps not matured amongst many of the member organisations.

The current survey underscores that in jurisdictions like Europe, the main barrier remains the shortage of providers, followed by concerns related to cost and risk assessment criteria. The escalating significance of cyber insurance due to rising cyberattacks underscores the need for continued efforts in this area. Addressing the lack of providers requires collaboration between insurance industry stakeholders, policymakers, and regulators to promote market growth, innovation, and competition. The WFE urges regulators and policymakers to take measures that can encourage insurer participation, expand market access, and support risk assessment and management to help enhance insurance availability and address gaps in coverage. Additionally, for its part, the industry will look to continue fostering a constructive dialogue with insurers to navigate insurance markets effectively and identify suitable coverage options despite market challenges.

The extent of organisations' cyber insurance coverage and its breadth are influenced by factors, including their ever-increasing reliance on technology, the evolving cyber threat landscape, regulatory changes, and a heightened awareness of cyber risks within organizations. WFE members have therefore decided to keep monitoring the area of cyber insurance, its evolution and barriers to securing it.