QUESTIONNAIRE ON CYBER RISK INSURANCE TO THE PRIVATE SECTOR

Background

1. Cyber risks pose a real threat to society and the economy, the recognition of which has been given increasingly wide media coverage in recent years. Cyber insurance can address the financial costs that arise from cyber-attacks and incidents, assisting in the recovery of those affected. In addition, cyber insurance can support risk reduction by promoting mitigation and prevention measures.

2. Given the increase in cyber risks, the OECD's Insurance and Private Pensions Committee (IPPC) is developing a project on cyber risk insurance with the aim of completing an in depth analysis of policy issues surrounding the development of a sound cyber insurance market with market conduct safeguards.

3. This project will look at various facets of the market and the issues that may arise as the market evolves and consists of three components (reports):

- Cyber risk insurance: the market and nature of insurance coverage available
- Risk awareness of cyber risks and the role of insurance in risk mitigation and prevention
- Regulatory and policy issues relevant to the development of cyber insurance markets

4. Under this project, three reports will be developed over the next 18 to 24 months period. It is hoped that the outcome of the project can be amalgamated towards the end, and discussed in an event on the topic in 2017.

5. For this purpose, we are circulating a survey questionnaire to the non-life (re)insurers to collect information on the cyber risk insurance market. The information collected will provide the basis of the three reports that will be developed. A separate survey questionnaire is being circulated to governments.

6. **Information collected from this Survey will remain confidential** – data gathered from individual insurers will not be shared with external parties but only with OECD Secretariat staff directly involved. Moreover, the data gathered in the Survey will be presented in the final report on a name-blind basis in order to protect the confidentiality of individual insurance companies and, as appropriate, in aggregated form. While we would be grateful if stakeholders can fill in the Survey in so far as possible and where applicable, we recognise that some information may not be available. Thus, we encourage stakeholders to provide responses where possible to ensure the OECD can collect as many contributions as possible.

7. We thank you for your cooperation and understanding in advance.

QUESTIONNAIRE ON CYBER RISK INSURANCE FOR THE PRIVATE SECTOR

PLEASE RESPOND BY ENTITY IF POSSIBLE (IF RESPONDING AT GROUP LEVEL, PLEASE INDICATE)	
Name of entity (please provide information on an individual entity basis)	GLOBAL FEDERATION OF INSURANCE ASSOCIATIONS (GFIA)
Country domiciled	GLOBAL
Name of contact	OSCAR VERLINDEN
Email	SECRETARIAT@GFIAINSURANCE.ORG
Responses should be sent to Lucie Amour (lucie.amour@oecd.org) **by 1 July 2016**.	

I. Extent and nature of cyber risk

(1) Please rate the factors which are leading to a significant change in the level cyber risk (including perception) in recent years:

- Dependence on public cloud computing: ☐ Important ☐ Moderate ☐ Low ☐ No impact
- Development of the Internet of Things (IoT)[1]: ☐ Important ☐ Moderate ☐ Low ☐ No impact
- Accumulation of big data[2]: ☐ Important ☐ Moderate ☐ Low ☐ No impact
- Proliferation of ransomware: ☐ Important ☐ Moderate ☐ Low ☐ No impact
- Sale and/or malevolent use of personal and security data acquired through cyber-attacks (including credit card and health information): ☐ Important ☐ Moderate ☐ Low ☐ No impact
- Sophistication of attacks/hacks: ☐ Important ☐ Moderate ☐ Low ☐ No impact
- Level of outsourcing that provides network access: ☐ Important ☐ Moderate ☐ Low ☐ No impact
- Aggregation of cyber risk[3]: ☐ Important ☐ Moderate ☐ Low ☐ No impact

[1] The Internet of Things (IoT) is the network of physical objects—devices, vehicles, buildings and other items—embedded with electronics, software, sensors, and network connectivity that enables these objects to collect and exchange data. For examples, having video devices on refrigerators and connected to a network has been a possible application being proposed.

[2] Big data is the accumulation of large and complex data, generated by everything around us at all times, every digital process and social media exchange, and may be analysed computationally to reveal patterns, trends, and associations, especially relating to human behaviour and interactions. For example, Big Data in healthcare is being used to predict epidemics, cure disease, improve quality of life and avoid preventable deaths.

[3] Using a vulnerability of widely used software/systems that may lead to numerous incidents/attacks leading to aggregated losses. Because of the non-physical nature of cyber risk, (re)insurers may also suffer losses from a vast number of insureds spread across different geographies as a result of a single event. In addition, an

- Awareness of cyber risk by (potential) policyholders: ☐ Important ☐ Moderate ☐ Low ☐ No impact
- Level of cyber security measures being employed and implemented: ☐ Important ☐ Moderate ☐ Low ☐ No impact
- Emergence of cyber risk linked to terrorism: ☐ Important ☐ Moderate ☐ Low ☐ No impact
- Implications/impact of cyber risk in existing policy coverages (e.g., coverage that may be implicitly covered in general liability, business interruption or other policies): ☐ Important ☐ Moderate ☐ Low ☐ No impact
- Others ( ): ☐ Important ☐ Moderate ☐ Low ☐ No impact

Comments:

(2) Has the frequency of cyber-attack/incident and/or severity been of greater concern in recent years?

☐ Frequency

☐ Severity

☒ Both

(3) Would you consider your country and its businesses to be at risk from cyber-attacks/incidents? If yes, please rate the perceived level of risk.

☐ High (constant or imminent attack/incident, and/or high impact)

☐ Moderate (occasional attack/incident, and/or moderate impact)

☐ Low (few attack/incident, and/or low impact)

☐ No risk

(4) In what sectors of the economy/society has the increase in risk exposure and losses from cyber risk been most apparent in recent years, and/or contagion of cyber risk to other sectors been of concern?

All sectors of the economy that have any electronic component to its business are exposed to cyber risk. The risk is also not limited to large enterprises, but also presents a challenge for small and medium-sized enterprises (SME's). Traditionally, financial institutions have been considered the prime target for a cyber-attack, but in recent years we have to expand that thinking more broadly to include sectors such as the health sector, energy sector, technology sector, automotive sector, transportation sector, retail, media and publishing firms, law firms, governmental bodies, etc. This list is not intended to be an exhaustive list or a reflection of the next big target, but rather we are flagging examples to show the broad array of potential targets. This wide spectrum is not only due to the evolving motivation for cyber-attacks, but also an increasing sophisticated and persistence by cyber attackers to find the weakest point of entry. While business of all sizes and industry segments should incorporate cyber risk into their overall risk assesments, studies have shown that the financial sector remains a prime target for attackers followed by the health sector, retail, and technology sectors.

(5) What aggregation and accumulation of risk is apparent for cyber risk insurance, and how is this being monitored?

Aggregation and accumulation of risk for cyber insurance represents a major challenge for (re)insurers. As the cyber market evolves, a key challenge for insurers will be to ensure that risk aggregation within a cyber insurance policy as well as across all classes of business, is properly

---

"extreme loss scenario" from cyber risk may also stem from a number of unrelated loss events affecting numerous insureds during any given annual period or a combination of scenarios. There is potentially a high level of systemic risk from overlapping multiple insurance lines of business.

monitored and their exposures prudently managed. Some of the aggregation and accumulation scenarios that insurers are carefully monitoring as they responsibly grow the market include: (a) Supply chain risks - businesses rarely conduct business in a vacuum, instead they have many business relationships; therefore, a cyber event at one business could have a broad reaching impact on a number of different insureds; (b) a cyber-attack could occur at an industry level as opposed to and individual company; and (c) cyber incidents present complex risk scenarios that are capable of triggering coverage under multiple policies. For example, one incident may involve business interruption, director & officer liability, extortion, property damage, and data breach response and recovery. It is also important to note that in the increasingly connected world, these scenarios are not limited to individual nation states, but could have a simultaneous global impact.

(6) What type of cyber-attack/incident (e.g., firm level/ industry level, credit card/health data etc.) would be most damaging in terms of the cyber risk policies of (re)insurers, including in terms of impact or frequency?

We cannot assess which type of cyber-attack/incident would be most damaging in terms of impact or frequency on a cyber risk policy. Each type of attack/incident presents its own individual challenges that as the market evolves, the (re)insurance industry continues to enhance the understanding of to appropriately underwrite and price the risk. .

II. Cyber risk insurance policies

(1) What is the definition or elements of a cyber risk incident which would trigger the coverage of losses from cyber risk? To what extent is there retroactivity of an incident for occurrence based policies? Does an attack need to be attributed before a claim is paid?

The definition or elements of a cyber risk incident that trigger coverage will differ by company and to an extent different policies. It is important to note that variation in defintions and elements is a common characteristic of any new and emerging market and that any regualtory initiatives should be sufficiently flexible to allow for the market to grow and evolve naturally.

Cyber risk should be considered as a peril that based on the type and characteristics of the event and loss could trigger various exposures. It is the characteristics of the event and not the "cyber" label that is relevant to policy coverage. We do not have any information to share on the retroactivity question, but would suggest that generally attribution is not the focus of many stand-alone cyber policies. This of course can differ by company and policy and does present a challenge when distinguishing whether the bad actor is criminally motivated or is a nation state.

(2) Has your entity taken action to comprehend the level of aggregate exposure to cyber risk across policies, in particular for policies where coverage may be implicitly being covered?

☐ Yes ☐ No ☐ Not known ☐ Other (please explain in the comments section)

If yes, has your entity taken action to ensure capital availability for when these are realised and how?

(3) In terms of developing cyber insurance contracts, please indicate if any of the following issues have posed a problem in providing coverage, and comment on possible actions that could assist in improving coverage:

	If this has been an issue in developing cyber risk policies	Comments
Loss exposure cannot be quantified	☐	Unable to Answer
Correlation and aggregation of risks	☐	Our comments on correlation and aggregation of risks are highlighted above
Average loss per event is high	☐	Unable to Answer
Maximum possible losses are high	☐	Unable to Answer
The level of cyber risk exposure of existing policies is uncertain or possibly high	☐	Our comments on correlation and aggregation of risk above touch on this issue of exposure under multiple existing policies. While this is a challenge, insurers are taking the necessary steps to understand the potential exposure triggers under traditional policies. The trades and our member companies also encourage consumers to understand how their existing policies cover the "cyber" peril and what additional coverage options they should consider to fill any gaps.
The ability to provide affordable coverage that provides sufficient security for policyholders and a reasonable return on capital	☐	Unable to Answer
Supporting legal framework is uncertain	☐	Unable to Answer
Risk cannot be sufficiently reinsured	☐	Our member organizations are not aware of any reinsurance capacity issues.
Notification or other regulatory requirements related to cyber-attacks would be difficult to economically cover	☐	In the United States it has been suggested that thte notification requirements help grow the cyber market. Some have suggested the recent EU regulation may have the same impact.
Difficulty of attributing a cyber-attack/incident	☐	As mentioned above, it will depend on the type of policy and company, but generally attribution is not a focus of whether or not the policy is triggered.

Transparency/disclosure of IT security is insufficient	☐	Given litigation sensitivities, there is a concern that companies are not sharing forensic reports with their insurer following a breach. The reason for not sharing these reports is out of an abundance of caution to avoid breaking any legal privilege that may be attached to the document or infomration.
Others ( )	☐	

(4) Please indicate whether your entity provides the below **standalone cyber risk policies** that specifically cover cyber incidents, and the types of incidents covered, the losses covered, and applicable deductibles (or share):

Coverage	Type of cyber incident covered	Insured losses covered	Deductibles (or share)	Maximum coverage available
First Party				
☐ Crisis management	☐ Hostile attacks on information and technology assets) ☐ Other ( )	☐ Costs of specialised service provider to reinstate reputation ☐ Cost for notification to stakeholders and monitoring (e.g., credit card usage) ☐ Other ( )		
☐ Business interruption	☐ Hacking ☐ Denial-of-service attack ☐ Malware ☐ Other ( )	☐ Cost to reinstate systems ☐ Loss of profits ☐ Coverage for data restoration costs (many cyber policies do not cover the costs to replace, upgrade or maintain a computer system that was breached) ☐ Other ( )		
☐ Data asset protection	☐ Information/data assets are altered, corrupted or destroyed by a computer attack ☐ Damage or destruction of other intangible assets (e.g., software applications) ☐ Other ( )	☐ Cost resulting from reinstatement and replacement of data ☐ Cost resulting from reinstatement and replacement of intellectual property (e.g., software) ☐ Other ( )		
☐ Cyber extortion	☐ Extortion to release or transfer information or technology assets ☐ Extortion to change, damage, or destroy information or technology assets ☐ Extortion to disturb or disrupt services ☐ Other ( )	☐ Cost of extortion payment ☐ Cost related to avoid extortion (investigative costs) ☐ Cost of ransom (included in some policies) ☐ Other ( )		
☐ Cyber fraud	☐ Theft of moneys	☐ Loss of moneys		

	☐ Theft of data assets ☐ Other ( )	☐ Cost resulting from reinstatement and replacement of data ☐ Other ( )		
☐ Intellectual property	☐ Theft of intellectual property (software, trademark) ☐ Other ( )	☐ Cost resulting from reinstatement and replacement of intellectual property (e.g., software) ☐ Other ( )		
Third Party				
☐ Privacy liability	☐ Disclosure of confidential information (personally identifiable information, protected health information or confidential corporate information) collected or handled by the firm or under its care, custody, or control due to negligence, intentional acts, loss, theft by employees, via a computer network or offline access. ☐ Other ( )	☐ Legal liability (defence and claims expenses, (fines) and regulatory defence costs) ☐ Vicarious liability (when control of information is outsourced) ☐ Crisis control (*e.g.*, cost of notifying stakeholders, investigations, forensic and public relations expenses) ☐ Credit monitoring: cost of credit monitoring, fraud monitoring or other related services to customers and employees affected by a cyber event ☐ Identity theft protection for customers ☐ Other ( )		
☐ Network security liability	☐ Unintentional insertion of a computer virus causing damage to a third party ☐ Unauthorized access of the insured causing damage to a third party system ☐ Disturbance of authorised access by clients ☐ Misappropriation of intellectual property ☐ Other ( )	☐ Cost resulting from reinstatement of data (restore or recreate data and software for third parties) ☐ Cost resulting from legal proceedings ☐ Other ( )		
☐ Communication and media liability	☐ Breach of software, trademark and media exposures (libel, etc.) ☐ Other ( )	☐ Legal liability (defence and claims expenses (fines), regulatory defence costs) ☐ Other ( )		
☐ Other ( )				
Comments:				

(5) In cases where some cyber coverage is included in other types of policies, please indicate whether any of the following **cyber risk-related exclusions** apply:

Policy	Cyber risk-related exclusions
☐ Property and business interruption policies including contingent business interruption (loss or damage to physical property and resulting loss of revenue resulting from an insured physical peril (fire, flood, etc.)	☐ Business interruption without material damage ☐ Loss must be caused by a physical peril (not virus or hackers)

	☐ Data is usually not considered as “property” ☐ Computers and their data are susceptible to some specialist causes of damage, which will not be covered if you are insured by general policy. ☐ Other ( )
☐ Theft insurance policies (theft of tangible assets following forcible or violent entry to/exit from the premises)	☐ Theft of data, which is an intangible asset and one which is often stolen remotely ☐ Reputation and identity theft are not covered. ☐ Other ( )
☐ Directors and officers (D&O) liability policies	☐ Securities claim (shareholder class action, derivative claims, regulatory action) ☐ Other ( )
☐ Terrorism insurance policies (physical damage)	☐ Cyber-attack: designed to compromise the information technology infrastructure ☐ Other ( )
☐ Fidelity guarantee/crime policies	☐ Covers employees, but not third party property, such as customer/client data ☐ Business income loss or other liability ☐ Theft of data or information is often specifically excluded ☐ Financial losses following fraud or misappropriation ☐ Other ( )
☐ General liability policies	☐ Criminal or deliberate acts of the insured or its employees, malicious unauthorised use of insured’s own network intended to damage, misuse or destroy its clients’ data or to cause denial of service attack ☐ Liability for electronic data and privacy breaches may be specifically excluded ☐ Computer virus transmission ☐ Fines and investigation by regulator ☐ First party costs: crisis management expenses (including expenses associated with a privacy breach such as notification costs and regulatory defence), PR, credit monitoring expenses, loss of business income and cyber extortion and ransom ☐ Other ( )
☐ Technology errors and omissions (E&O) policies	☐ Property damage ☐ Personal and advertising damage ☐ Other ( )
☐ Other ( )	

(6) What issues (if any) have emerged regarding claim disputes over the definition of cyber risk policies?

(7) What proportion of your existing policies with cyber risk elements do you consider to be at immediate risk from being triggered by a cyber-attack and/or cyber incident?

- ☐ 100%
- ☐ 70%
- ☐ 50%
- ☐ 30%
- ☐ 10%
- ☐ Not at risk

(8) For the purpose of the project, we would be grateful if you could attach a sample policy relevant to cyber risk for each or one of the policies provided above. This will be used to analyse the contract terms being provided, and will form a core element of the project.

(9) If available and possible, please indicate the type of policyholders that your entity provides cover for cyber risk:

- ☐ Listed companies
  Please indicate the proportion of this type of policyholders' policies to gross written premiums of cyber policies %
- ☐ Large non-public companies
  Please indicate the proportion of this type of policyholders' policies to gross written premiums of cyber policies %
- ☐ SMEs
  Please indicate the proportion of this type of policyholders' policies to gross written premiums of cyber policies %
- ☐ Individuals
  Please indicate the proportion of this type of policyholders' policies to gross written premiums of cyber policies %

(10) What sectors of the economy purchase and are most relevant for cyber risk insurance policies of your entity?

III. Relevant cyber risk insurance data

(1) What are the **gross written premium levels** of cyber insurance of your entity?

Gross written premiums	2011	2012	2013	2014	2015
Gross written premiums of your entity (currency and unit:)					
Of which, standalone cyber protection policies (% to total)					
Of which, cybersecurity coverage that is part of a traditional policy (e.g. property, business interruption, liability policies etc.)					

(share of premium covering cyber as % to total)					
Comments:					

(2) What have been the **insured losses** linked to cyber risk of your entity?

Insured losses	2011	2012	2013	2014	2015
Insured losses of your entity (currency and unit:)					
Of which, standalone cyber protection policies (% of total losses)					
First party losses					
Third party losses					
Of which, cyber protection coverage that is part of a traditional policy (e.g. property, business interruption, liability policies etc.) (% of total losses)					
First party losses					
Third party losses					
Comments:					

IV. Underwriting and risk mitigation

(1) What type of risk assessment, and security audit/ and other mitigation measures (if any) are carried out in advance of offering a cyber protection policy, and how is this reflected in premiums (e.g., ISO 27000 standards required, appointment of security officer)?

(2) Are certain conditions or requirements imposed as regards to the cyber security of the policyholder, and if so, what are these requirements?

(3) Has sufficient data been available to support the underwriting and pricing of cyber risk policy, and if not, what has been the basis of underwriting and pricing of policies?

A lack of actuarial data is one of the challenges to continued expansion of the market. The ever-evolving nature of the risk necessitates an understanding of historial and recent data ponits. That said, there are products that have been around long enough to benefit from a more robust source of actuarial data. For example, in the U.S. current products providing for privacy and data security events evolved from a technology focused E&O policy that was developed approximately 15 years ago. A regulatory landscape then evolved establishing data breach response obligations. As such there is a more mature market around 1st party response coverages (i.e. notification, investigation, and compliance expenses) and 3rd party coverages for lawsuits and regulatory actions alleging system failures, theft, and/or inadequate disclosures. Some have suggested the new EU regulation may help expand the cyber insurance market throughout Europe.

To help expand the market offerings conversations have evolved regarding what data insurers would need and how they could obtain such data.

(4) What type of modelling of cyber risk is your entity using (e.g., deterministic and/or probabilistic options, single risk and/or portfolio-level) and what improvements are being considered?

Overall, there is a lack of predictive cyber risk modelling. Compared to natural catastrophes cyber risk is relatively new, so there is a lack of historical data to help with modelling efforts. Further, the continual evolution of the threat complicates the issue. Nevertheless, insurers are engaging in their own modelling efforts and over the past two years broader efforts, such as the AIR Worldwide project and RMS/AIR/Lloyd's joint project have commenced to help fill this modelling gap.

(5) Have any efforts been made to improve the quantification of cyber risk by your entity or national trade association or insurance institute?

The U.S. Department of Homeland Security has convened conversations with Chief Information Security Officers and insurers to explore whether or not a voluntary private data repository is possible and if so, what that repository must look like and how it should operate. Also, in the UK, the British insurance industry is exploring the possibility of a government led database where companies are mandated to record details of cyber-attacks.

(6) Has your entity or trade association carried out any analysis/measures for greater prevention/mitigation of cyber risk?

V. Issues relevant to the future of cyber risk insurance

(1) What are the risks from an expanding cyber risk insurance market? Has the vulnerability of the insurance sector to cyber-attacks increased, or will it increase?

We are not aware that there are any risks from an expanding cyber risk insurance market. The insurance industry continues to look for ways to meet market demand in a responsible way and as such the market will continue to evolve as insurers continue to expand their knowledge of the risk. It is important

Whether or not the insurance sector's vulnerability to cyber risks will increase remains to be seen, but insurers are taking steps, as they always have, to make sure they are protecting consumer information.

(2) Do you have plans to extend cyber protection policies to SMEs and individuals (consumers)? If so, what types of coverage do you envision?

(3) Has there been policy or initiatives taken to raise awareness of cyber risks by your entity or national trade association?

☐ Yes ☐ No ☐ Not known ☐ Other (please explain in the comments section)

If so, what is the policy/initiative?

(4) Are any initiatives being taken either by your entity, the trade association or in cooperation with your country's government to improve the provision of cyber risk insurance more widely?

Globally governments have placed a significant amount of importance on enhancing the cyber resiliency of their country. To the extent government has been interested in the role cyber insurance can play in increasing

resiliency, our organizations have been involved in education efforts to explain what the cyber insurance product is and its value as a risk transfer mechanism.

It is important for governments to support the development of the cyber insurance market by allowing the market to grow through a natural evolution. Insurers are in the business of managing risk responsibily and are taking the same approach with cyber insurance. Cybersecurity presents a unique and ever-evolving risk landscape, but fundamently challenges such as the lack of data and standardization exist with any new and emerging market and with time the market responds appropriately to these challenges. As such, governments should exercise caution when considering regualtory activity, if any, in this area and avoid imposing ureasonable requirments that could stifle innovation and the continued development of the cyber insurance market.