Position Paper

Insurance Europe response to FSB consultation on effective practises for cyber incident response and recovery

Our reference:	EXCO-CS-20-036	Date:	17 July 2020
Referring to:	FSB consultation on effective practises for cyber incident response and recovery		
Contact person:	Áine Clarke, Policy Advisor, General Insurance	E-mail:	Clarke@insuranceeurope.eu
Pages:	7	Transparency Register ID no.:	33213703459-54

Summary

Insurance Europe is the European insurance and reinsurance federation, which, through its 37 member bodies – the national associations – represents all types of insurance and reinsurance undertakings, including pan-European companies, monoliners, mutuals and SMEs. The security of Information and Communication Technology (ICT) systems is of key importance to the industry, as is its ability to respond to and recover from cyber incidents both efficiently and effectively. As Insurance Europe is a representative body, and the toolkit addresses the practices of individual financial institutions, Insurance Europe is unable to provide detailed responses to all questions outlined in the consultation paper. However, Insurance Europe welcomes the opportunity to provide input, where possible, to the questions on a toolkit of effective practises for cyber incident response and recovery.

General

1.1. Have you learnt any lessons from the COVID-19 pandemic and related cyber activity that will contribute to your cyber incident response and recovery practices?

In general, European (re)insurance companies have responded to national lockdown orders and/or recommendations to maintain social distance by transitioning their combined workforce of over 900,000 employees to teleworking and setting up effective protocols to facilitate this transition. They have implemented contingency plans to protect their customers and employees while minimising service interruptions. This process has been deployed with the maximum level of efficiency possible, although networks and ICT systems have been stretched, like in other sectors. However, given that there have been no major disruptions reported, the ICT security and contingency programmes put in place by European (re)insurers have proven to be robust when confronted with the new COVID-19 working environment.

Insurance Europe aisbl
Rue Montoyer 51, B-1000 Brussels
Tel: +32 2 894 30 00 • Fax: +32 2 894 30 01
E-mail : info@insuranceeurope.eu
www.insuranceeurope.eu

As regards malicious cyber activity during the COVID-19 pandemic, Insurance Europe's members have not reported any major changes to the threat landscape or increases in threat levels and incidents during the pandemic. However, COVID-19 is now being commonly used as a lure and a threat in standard cyberattacks e.g. phishing emails.

As risk prevention is core to the business of insurance, (re)insurers have also played a key role in raising awareness of cyberattacks during the COVID-19 pandemic and several national associations have run campaigns during this period. In particular, Insurance Europe's members have been active in raising awareness of the risks associated with the move to home working, including the increased vulnerability of businesses due to the use of private home networks and computers. In this regard, the pandemic has confirmed the importance of cyber resilience for businesses of all sizes and highlighted the key role to be played by (re)insurers in the prevention, mitigation and transfer of cyber risk. This is an area where the (re)insurance industry can play an active and positive role in mitigating the negative effects of the COVID-19 pandemic or potential future, similar events, on the cybersecurity of businesses.

1.2. To whom do you think this document should be addressed within your organisation?

The answer to this question depends on the organisation of each insurance company; for example, for an insurance group: the ISS (Information Systems Security) team is in charge of the risk life cycle. The ISSM (Information Systems Security Manager) defines the multi-year exposure reduction program, which is validated by the Executive Committee. The Group holding company defines a global information security framework and continuous improvement objectives.

Other, smaller undertakings, such as captive (re)insurance companies, outsource all key functions and processes and do not have any dedicated staff. As such, these undertakings rely on the ICT assets, ICT systems and ICT processes of their outsourced service provider. An outsourcing agreement between insurer and service provider ensures that the service provider has adequate contingency plans in place to deal with emergency situations or business disruptions and periodically tests backup facilities where necessary, taking into account the outsourced functions and activities. Therefore, in cases such as these, this document would need to be addressed to the relevant information security officer within the service provider organisation.

1.3. How does your organisation link cyber incident response and recovery with the organisation's business? Does your organisation follow international standards or common frameworks? If so, which international standards or common frameworks?

Managing ICT security risks is a priority for the insurance industry. In the EU, the insurance sector follows several sets of rules impacting on its cyber incident response and recovery capabilities: for instance, guidelines issued by supervisory authorities, whether by the European Insurance and Occupational Pensions Authority (EIOPA) or at national level, or, in some cases, the NIS Directive and its implementing texts, applicable to insurance companies in EU member states where they have been classified as Operators of Essential Services. In addition to these rules, ICT risks as a component of operational risks (see Art. 13 No. 33 Solvency II-Directive) are already part of the integrated risk management system of all Solvency II regulated insurers. As such, ICT risks are taken into account in capital requirements, governance and reporting.

There are also other ongoing EU initiatives in the area of cyber incident response and recovery that may have an impact on Europe's insurance sector, such as the envisaged European Commission proposal on a digital operational resilience framework for financial services, which seeks to legislate on the areas of ICT and security requirements, incident response, stress testing, risk transfer mechanisms and information sharing, or the upcoming review of the NIS directive, scheduled for end-2020.

Aside from EU rules, (re)insurers also follow a variety of different international standards/common frameworks, among them: the ISO 27000 series (information security standards); ITIL incident management processes.

- **1.4. Does your organisation structure its cyber incident response and recovery activities along the seven components set out in the FSB toolkit? Please describe any additional components your organisation considers.**

Prevention is also an important component of any toolkit for cyber incident response and recovery. Preventing cyber incidents is closely linked to awareness of them, given that often inadequate cybersecurity standards are the result of an inadequate understanding of the risks and a lack of appropriate skills among an organisation's staff. As such, training and awareness-raising programmes should figure centrally in an organisation's cyber incident response and recovery activities.

- **1.7. What role, if any, should authorities play in supporting an organisation's cyber incident response and recovery activities?**

Private insurance undertakings expect support from authorities in the form of general guidelines on the practices that should be adopted and implemented in sound cybersecurity plans, while this component is also integrated in the supervision and inspection routines deployed by authorities in compliance with their legal responsibilities. It is important that guidelines are composed of general provisions and are principle and risk-based, leaving full room for individual company-level strategy-planning and decision-making, while also being sufficiently proportional so that they can be applied in a manner appropriate to the nature and scale of ICT operations stemming from an undertaking's business profile. This is to ensure that these cyber incident response and recovery support initiatives can be applicable across a varied industry like insurance without imposing disproportionately burdensome obligations on some organisations.

Insurance Europe would like to stress the importance of alignment between the various initiatives from different authorities so that any multiplication of obligations and requirements on organisations, all of which may be intended at achieving the same goal (of supporting cyber incident response and recovery), can be avoided. There are many existing rules in force and many others in the pipeline (see response to question 1.3), so close coordination between authorities in this area is essential. Otherwise, the regulatory environment to which organisations are subject becomes difficult to navigate, interfering with an organisation's ability to ensure compliance and detracting from the added value of having such requirements in place.

Governance

- **1.1. To what extent does your organisation designate roles and responsibilities as described in Tool 3? Does your organisation identify these roles by business line, technology application or department?**

The administrative, management or supervisory body (AMSB) should ensure that undertakings' system of governance, in particular the risk-management and internal control system, adequately manage undertakings' ICT and security risks. ICT and security risks belong to the general risk management system and internal control system; ICT risk is classified as an 'operational risk' already taken into account by insurance undertakings. Even if the AMSB is ultimately responsible for an undertaking's risk management system, it should not have to review the detail of the undertaking's ICT and security risks.

Preparation

- **2.1. What tools and processes does your organisation have to deploy during the first days of a cyber incident?**

From a cyber insurance perspective, in the immediate aftermath of a cyber incident, an increasing number of insurers offer forensic IT services and legal support to mitigate the adverse consequences of the incident.

- **2.3. How does your organisation monitor, manage and mitigate risks stemming from third-party service providers (supply chain)?**

When using third-party service providers, insurance companies are subject to the rules imposed by the Solvency II Directive and its implementing texts (Delegated Regulations, EIOPA Guidelines, guidelines issued by National Supervisory Authorities). Large service providers do not offer any specific adjustments to their product lines to meet the regulatory requirements specific to the insurance sector and smaller service providers do not always have the means to do so. As such, insurance companies bear the burden of ensuring that any third-party service providers they use comply with the regulatory framework (in terms of contractual requirements, audit, monitoring and oversight). However, the capabilities of individual insurance companies to ensure that ICT third-party service providers meet appropriate ICT and security standards are limited.

In this regard, Insurance Europe welcomes the work of the European Commission to develop standard contractual clauses for cloud outsourcing by financial institutions, as this would allow insurance companies to better reflect their sectoral regulatory constraints (e.g. Solvency II) in their contractual agreements with cloud service providers.

Analysis

- **3.1. Could you share your organisation's cyber incident analysis taxonomy and severity framework?**

(Re)insurance companies refer to the FSB cyber lexicon[1], the CRO Forum taxonomy[2] and the National Institute of Standards and Technology (NIST) cybersecurity framework[3], among others. However, Insurance Europe's members have raised questions over the usefulness of taxonomies over time, given the evolving nature of cyber risk, which entails a risk that certain terms become rapidly out of date or evolve to include a different scope and definition.

- **3.2. What are the inputs that would be required to facilitate the analysis of a cyber incident?**

The analysis of a cyber incident has a different aim depending on the time at which it is carried out in relation to the incident taking place.

When a bug or virus is in circulation, having a mechanism in place to facilitate real-time sharing of indicators of compromise (IOC) would assist organisations in the prevention of immediate cyber threats.

However, the ex-ante analysis of a large number of aggregated past cyber incidents would allow for the threat landscape to be better understood. The establishment of a voluntary two-way reporting

[1] FSB Cyber Lexicon
[2] CRO Forum taxonomy
[3] NIST cybersecurity framework

mechanism for the exchange of cyber incident reports (above a certain materiality threshold) between participating financial institutions and National Competent Authorities (NCAs) would allow NCAs to gather data on incidents and operate a feedback mechanism with financial institutions, who could draw upon incident data from across the financial sector to improve their own ICT security. As an added layer, an incident exchange mechanism between the different NCAs would widen the pool of incident data, strengthening the added value of such a mechanism. To make such a mechanism increasingly efficient, it would be important to avoid the multiplication of authorities to which financial institutions have to report (for instance, one incident should not require reporting to a number of authorities). Lastly, participating insurance companies could also make use of incident data for underwriting purposes, encouraging the growth of the cyber insurance market and contributing to the overall cybersecurity of businesses.

- **3.4. What sector associations does your organisation participate in and what benefit does your organisations accrue from that participation?**

Insurers participate in sector associations at a national and/or regional level.

Most German (re)insurers are connected to the LKRZV (Crisis Reaction Centre for IT Security of the German Insurance Industry), a national platform which facilitates event-related communication for the purpose of early detection, alerting and management of crises, together with the Federal Office for Information Security (BSI - Bundesamt für Sicherheit in der Informationstechnik) and insurance companies on a 24/7 basis. The LKRZV is a two-way reporting and communication process – allowing not only pseudonymous reporting but also distributing information, alert and requests to the insurers in a coordinated, timely manner.

Since 2017, France along with the French Federation of Insurance and other stakeholders have created a public interest group, GIP ACYMA. This public-private partnership brings together private and public players who wish to get involved in the action of the Cybermalveillance.gouv.fr system which consists in active participation in working groups on targeted projects (e.g. prevention), in contributing to certification processes, but also in the setting up of a Digital Risk Observatory, a tool to support decision-making and public action. In addition, some (re)insurers in France are members of a cross-sectoral group, INTERCERT-FR, which is dedicated to strengthening the capacity of its members to detect and manage cyber security failures.

Some (re)insurers in Denmark, Norway, Sweden and Iceland are members of the Nordic Financial CERT, established to strengthen the Nordic financial industry's resilience to cyberattacks, by enabling Nordic financial institutions to respond rapidly and efficiently to cyber security threats and online crime. As a collaborative initiative, it allows members to work together when handling cybercrime, sharing information and responding to threats in a coordinated manner.

In the Netherlands, most insurance companies are connected to the Computer Emergency Response Team (i-CERT) of the Dutch Association of Insurers. This allows for real-time information sharing on cyber threats, incidents and vulnerabilities between Dutch insurance companies.

Mitigation

- **4.1. Besides reducing impact to business and system security, what are other considerations that need to be taken into account during mitigation?**

In a financial sector that is increasingly digitised and confronted with a significant number of cyber incidents, there is a need for financial institutions and their supervisors to better understand the role

that insurance cover for cyber risks can play in an organisation's risk management, acting as a mechanism to transfer risk and providing them with compensation for losses that cannot be fully prevented.

With regard to mitigation in particular, cyber insurance policies can include forensic services so that the impact of a cyberattack can be assessed and minimised in a timely fashion, as well as crisis management and public relations services in order to mitigate any potential reputational damage that may result from a cyber incident.

Improvement

- **6.1. What are the most effective types of exercises, drills and tests? Why are they considered effective?**

Insurance Europe acknowledges the important role that testing of ICT infrastructure can play in identifying and addressing vulnerabilities. In this regard, it is important that organisations carry out pluri-annual testing that is appropriate to the criticality of the ICT systems in question. Such testing can include baseline testing (gap analyses, compliance reviews, vulnerability scans) and more advanced testing, such as threat led penetration testing (TLPT) if an organisation assesses that there is a need for it.

However, conducting testing can be very financially burdensome for organisations (penetration testing can cost in the region of €80,000 – €100,000) and can often involve considerable delays in applying corrections. As such, the frequency of testing should be at the discretion of each individual organisation. It is important to note that many larger insurance companies are moving increasingly towards conducting security testing on an ongoing basis.

- **6.2. What are the major impediments to establishing cross-sectoral and cross-border exercises?**

One of the major impediments to cross-sectoral and cross-border testing exercises is the reputational issues associated with sharing the results of such exercises, since these results could affect an organisation's relationship both with its supervisor and with its peers. The success of any exercise is therefore conditional on it being carried out on an anonymous or pseudonymous basis.

The same reputational issues are associated with information-sharing exercises. Other impediments to establishing these exercises include: the degree of fragmentation of both information collecting and information sharing practises both across different financial sectors and across different jurisdictions; and the lack of a common taxonomy on cyber risk which may complicate the development of streamlined reporting templates.

Coordination and communication

- **7.3. Apart from regulatory/compliance reporting, what other information does your organisation consider useful to share with authorities?**

All aggregated information that helps authorities to establish an adequate picture of the cyber security landscape within a sector would be considered as useful information to share. However, the main point in this field is that concerned with coordination. Beyond regulatory and compliance reporting, there is a risk of the different public powers and institutions related to cybersecurity matters gathering information by themselves, leading to information overlap and, as a consequence, an excessive burden on

organisations. From a private sector point of view, then, it is crucial that any complementary demand of information would be duly coordinated between the different acting public actors. It would be also crucial for private sector financial organisations to benefit from the data collected by public actors, in particular information on significant data breach episodes, thus making it easier to prevent future cybersecurity events. As such, organisations must benefit from sharing information with authorities and any mechanism must be reciprocal, allowing participating organisations to access anonymised and aggregated data in return for their participation.