Response to EIOPA discussion paper on Methodological Principles of Insurance Stress Testing – Cyber Component

Our reference:	EXCO-CS-23-033	Date:	28 February 2023
Referring to:	Discussion Paper on Methodologies of Insurance Stress Testing - Cyber component		
Contact person:	Kenny Piasecki Policy advisor, general insurance	E-mail:	piasecki@insuranceeurope.eu
Pages:	9	Transparency Register ID no.:	33213703459-54

Section 2 - Cyber risk for insurers

Q1. *What is your view on the proposed relevance of loss factors as described in Table 1 and based on expert judgment? Please provide an explanation.*

The industry would like to note that any stress test exercise should have clear objectives, appropriate timescales and be proportionate to its objectives. Specific comments on the proposed relevance of loss factors are as follows:

- In terms of ransomware, direct losses are low when systems are restored quickly enough. However, there tends to be competing factors in practice, such as the extent of encryption and the quality of backups. Therefore, the rating of moderate is plausible.
- The denial of service is a relevant scenario but, in general, not deemed significant. For most insurers and pension providers, an outage would need to be of a long duration to be significant. "Simple" denial-of-service attacks can usually be mitigated rather quickly. In addition, denial of service rarely affects all services (which are usually not in the same place because of the multiplication of SaaS services) and is, in most cases, for a relatively short time. Insurance companies seem less affected by these services.
- For data breach, the impact on "Restoration" should not be "moderate": it should be "low", unless the scenario is for both "data theft and deletion of the copy held by the undertaking". The restoration indeed does not impact the recovery (a company will tend to correct the flaw in question rather than restoring to a version that is likely to have the same flaw or is obsolete).
- There is no link between availability and cryptojacking.
- For the payment infrastructure outage, it would be low, except if the unavailability affects systems supporting tax declarations and if the amounts are evaluated as "moderate".
- The "Data Center / Infrastructure" scenarios are usually not the consequence of a cyber act but rather the consequence of an event (for example, natural disaster) affecting IT infrastructures. It is rather a scenario associated with a technical stress. In the cases where a "Data Center/ Infrastructure" scenario occurs as a result of a cyber-attack, this may be significant if infrastructures are shared across a group and there is an additional cost for policyholders to check data and systems to ensure that they have not been corrupted. Therefore, if the "Data Center/ Infrastructure" scenario should be implemented at all, the nature of the drivers should be taken into account in the design of this scenario.

Insurance Europe aisbl • rue Champ de Mars,23 B-1050 Brussels
Tel: +32 2 894 30 00 • E-mail: info@insuranceeurope.eu
www.insuranceeurope.eu

- As for power outage, it should be low for direct losses to be consistent with other scenarios. However, a point can be made that out of all scenarios proposed, power outage may be argued to not be included since it is primarily caused by external factors and is not dependent on the maturity of a company in their ability to deal with cyber risk. Therefore, the relevance of having this scenario within a cyber stress test is questioned.
- "Unauthorized transaction" is a plausible scenario which could trigger important losses. This scenario should be retained.

Q2. *What is your view on the main sources of cyber risk for insurers as described in sections 2.2 and 2.3? Are there any other relevant sources not covered in these sections? Please provide clarification.*

The main sources of cyber risk for insurers identified are sufficient for the most part, but a few points may be addressed:

- It could have been beneficial to discuss the use of legal protection following a disclosure of information incident (in reference to paragraph 2.3 and the exploration of extreme motor insurance scenarios).
- For the types of cyberattacks listed in section 2.2.3, there is no reference to vulnerabilities exploitation vendor software/hardware compromise as relevant.
- There is no explicit reference to existing controls and their role in risk reduction, such as multifactor authentication or remote access management.

Section 3 – Key assumptions

Q3. What is your view on the proposed approach regarding operational errors (i.e. considering non-malicious events at a later stage)? Please provide clarification.

Overall, the approach is sufficient. However, the potential impact/likelihood ratio seems low.

From the perspective of immediate mitigating measures, the treatment of malicious and non-malicious events in the context of a stress test is comparable. There are significant differences in the further (post-) treatment (for example, in the context of offender investigation and prosecution). However, there are some instances where malicious and non-malicious events must be treated separately, as the nature of the risk may be different for malicious events.

Q4. *Par. 80 proposes a different treatment of the operational errors in case of in- and -outsource of operations. In the light of the potential biases introduced by the different in- out-sourcing operational models, please provide an indication on the materiality of such bias.*

This question is not entirely clear as it refers to the different treatment of in-/outsource operations, while paragraph 80 refers to the (initial) lack of distinction between deliberate and non-deliberate actions. The lack of consistency creates confusion.

The distinction between deliberate and non-deliberate actions would have to be considered within the context of specific examples: for many scenarios, the impact of these distinctions on observed effects could be very minor. However, the consequences will not always be the same for deliberate and non-deliberate actions. There should be further consideration regarding deliberate and non-deliberate actions, as they will have differences in:

- Threat agents (internal or external)
- Control sets reducing the risk
- Frequency and impact
- Duration
- Scenarios (third party involved as attacker or as unaware entry point)

A bias is not expected between in and outsourcing operational models as it is viewed that there is not a significant difference between said models.

Q5. *What is your view on the proposed treatment of regulatory fines and compensation against legal actions? Please provide clarification.*

There is agreement that the proposed treatment of regulatory fines and compensation against legal actions should be excluded, as said measures would have to be massive to be significant. However, consideration for different local impacts means that legal actions could be a major component of the loss deriving from certain types of attacks in some scenarios.

Section 4 – Scope

Q6. *How do you assess the concentration of critical IT systems within group structures, i.e. are critical IT infrastructures such as the data center, the communications network (phone system, mail), management of critical applications, among others, often shared within an insurance group? Please provide clarification.*

This will vary from group to group depending on their IT architecture. Some companies assess the concentration of crucial IT systems as part of the risk analysis for the whole financial sector performed by the authorities. In addition, the assessment of the concentration of crucial IT systems can be done through modelling techniques such as setting a high correlation (eg perfect correlation) in a dependency structure between the different modelled units, in order to account for multiple scenarios hitting simultaneously within the group (ie macro scenarios).

The critical IT infrastructures listed are often shared within a group. However, there are cases where they are only shared with the largest entities in an insurance group and by extension, smaller companies often have their own critical systems as they wish to remain autonomous. If small independent entities have an interconnected IT system within the group, the risk is increased.

Q7. *Should stress testing of cyber resilience risk be carried out at group or solo level? Please provide clarification.*

Both approaches could be used, as the suitability of carrying out a cyber resilience risk on either level is determined by factors such as size, type of insurance products, and structures of process and systems, among other factors.

Q8. *Should stress testing of cyber underwriting risk be carried out at group or solo level? Please provide clarification.*

Both approaches could be used, as the impacts on solo and group level can be very different, as well as it can differ between different solo undertakings.

Q9. *What is your view on the considered hybrid approach to the scope definition, e.g. targeting groups for an assessment of cyber resilience risk and solos for an assessment of cyber underwriting risk? Please provide clarification.*

There is no one-size-fits-all approach and there is not an approach that will make sense in all cases. Therefore, both approaches could be considered as the way that solos and groups would be impacted depends on several factors as described in questions 7 and 8.

Q10. *Which are in your view the Solvency II lines of business expected to be more impacted by affirmative cyber underwriting risk?*

Affirmative cyber underwriting risk is expected to have an impact on various lines of business due to the variety of perils covered by cyber insurance contracts. From a Solvency II perspective, the main lines of business that are impacted are:

- General liability (direct and proportional),
- Legal expenses (direct and proportional) and
- Non-proportional casualty
- Fire and other damage to property insurance
- Miscellaneous Financial Loss
- Assistance (direct and proportional).

Q11. *Which are in your view the Solvency II lines of business expected to be more impacted by non-affirmative cyber underwriting risk (i.e. silent cyber risk)?*

Due to its implicit nature, non-affirmative cyber underwriting risk can have a material indirect impact to the following Solvency II lines of business:

- Fire and other damage to property (direct, proportional, non-proportional),
- Marine, aviation and transportation (direct, proportional, non-proportional),
- General liability (direct and proportional),
- Credit and suretyship (direct and proportional),
- Legal expenses (direct and proportional),
- Non-proportional casualty.

Q12. *What is your view on the criteria for the selection of the participating entities listed in Table 3? Please provide clarification.*

The scope for the table would be expected to be set in accordance with the effect in the event of a failure, rather than the size of the market or business.

For the cell pertaining to exposure and cyber resilience, risk profile should be included with size of the company.

The use of "critical functions" to determine scope of a cyber stress test is not supported and should be avoided, particularly at the present time given its importance in the ongoing discussions on the EC's Insurance Recovery and Resolution Directive proposal.

Q13. Are there any other relevant criteria not covered in Table 3 or in your answers to the previous questions? Please specify.

N/A

Section 5 – Scenarios

Q.14 *What is your view on the five selected scenarios for both cyber underwriting and cyber resilience risks? Please provide clarification.*

In terms of the design of cyber stress tests, it is important to recognise the fact that the market in question is maturing and remains highly specialised. As such, any European stress tests will come at a critical time and be influential on the development of the market, including by potentially having an effect on both regulatory and industry considerations and approaches. It would, therefore, be desirable for EIOPA to further consult on specific scenarios once these have been designed in full as, although it is also very helpful to provide input to the high-level design principles at this stage, important facets may emerge in detailed scenario designs which would merit industry input, and which would not be apparent at the design stage.

Nevertheless, and until a detailed consultation is carried out by EIOPA, some preliminary points on the scenarios are provided:

- The data centre/infrastructure (cloud outage) damage scenario is a problem specific to a specific insurance company, whereas the power outage scenario is a global risk by territory. Thus, data centre/infrastructure damage would imply a reputational risk that power outage would not.
- The data centre/infrastructure (cloud outage) damage scenario is usually not the consequence of a cyber act, but rather the consequence of an event (such as a natural disaster) affecting IT infrastructures. Nonetheless, it is a relevant scenario as there may be severe consequences, especially if infrastructures are shared across a group and there is an additional cost for policyholders to check data and systems to ensure that they have not been corrupted. The cloud outage underwriting scenario could benefit from having additional dimensions included in the scenario design principles. For example: the outage timeframe (eg hours/days), what is impacted (eg major cloud service provider) and what was the cause (eg misapplied software attacked by malicious code).
- With additional regard to power outage, the scenario itself is seen as very impactful, but not necessarily as part of a cyber stress. Power outages can have many sources, with cyber being only one among many - and a very unlikely one compared to others at that. Furthermore, it can be complicated to define and calibrate, as it is understood to concern an energy-operator failure.
- There could be a connection between ransomware and data breach, as both scenarios have closely related risks and consequences. It is noted that they do not systematically occur together, but there are some instances where the data unavailability caused by a ransomware attack can fall under the case of a data breach.
- Denial of service is, in general, not deemed significant. For most insurers and pension providers, an outage would need to be of a long duration to be significant. "Simple" denial-of-service attacks can usually be mitigated rather quickly. The denial-of-service *underwriting* scenario could benefit from having additional dimensions included in the scenario design principles. For example: who is impacted (eg global IT network of a MNE), whether it includes a ransom demand, length of outage (eg hours/days), location (national/regional/global).

Generally, it is reasonable to estimate financial impacts for the given scenarios as part of a EIOPA stress testing exercise. However, conducting and documenting business interruption exercises - with details of qualitative information such as the availability of backup systems - should not part of such a stress test. Further, this type of information will presumably be available via the tests implemented in the Digital Operational Resilience Act (DORA).

Summarising the above-mentioned arguments, it is advised that EIOPA carries out a detailed consultation on the specificities of each scenario. Until this takes place, it is concluded that the ransomware, cloud outage and data breach scenarios are relevant and necessary; denial of service is deemed to be comparatively small but still a valid scenario; whereas power outage does not seem to fit a cyber stress testing framework in its current wording.

Q.15 *Which scenario do you consider most relevant from the list of scenarios proposed for cyber underwriting? Please provide clarification.*

Ransomware (and other types of destructive cybercrime) is considered the most relevant for cyber underwriting as it is the scenario which costs the most for companies, especially if it comes with a data breach. Furthermore, it is relevant due to the global proliferation of attacks and the uncertainty in the approach taken by insurers on whether to insure such attacks. In addition to ransomware, cloud outage is a significantly relevant scenario. These scenarios are relevant as they could have a large impact, be widespread, and the severity could be high.

Q.16 *Which scenario do you consider most relevant from the list of scenarios proposed for cyber resilience? Please provide clarification.*

Ransomware, cloud outage and data breach (and other types of destructive cybercrime) are considered to be the most relevant for cyber resilience. In addition, they may cause availability and confidentiality issues that organisations might face that are linked to a number of causes.

Q.17 *Are there any additional cyber risk stress scenarios that should be considered? If yes, please provide their narrative and specification.*

N/A

Q.18 *What is your view on the separate treatment of the Ransomware and Data breach scenarios? Please provide clarification*

For cyber underwriting, this separation can be very helpful with regard to the application to different types of coverage. As many policies differentiate between first- and third-party coverages, it seems to be sensitive to mirror that distinction in the scenarios (ransomware being mainly first party driven and data breach being a scenario for third party coverages). In addition, ransomware and data breach do not systematically occur together.

Regarding cyber resilience, the distinction seems necessary, as the motive behind undertaking a ransomware attack or data breach attack would be different.

Section 6 - Cyber Underwriting: Shocks, Specifications and Metrics

Q.19 *What is your view on the proposed metrics and indicators in terms of completeness and viability? Please provide clarification.*

The provisions, claims and loss ratio metrics are relevant.

The output metrics are suitable, as they are the ones present in Solvency II.

The "cyber loss ratio" metric is difficult to compute in an isolated manner, as of today.

Q.20 *What is your view on the feasibility of splitting metrics for affirmative and non-affirmative coverages? Please provide clarification also with respect to add-on cyber coverages.*

Depending on the LoB, it is reasonable to distinguish between affirmative and non-affirmative cyber risk. As mentioned above, the industry sees problems with regard to the differentiation between the two types of add-on coverage. With regard to the differentiation between silent cyber and affirmative cyber risk, in general, the industry sees this as a key difference that should absolutely be reflected in the reporting. There is a profound difference between the metrics for silent and affirmative exposure and the industry finds these numbers

should not be mixed. While metrics for affirmative covers can certainly be based on detailed information, it might be a stretch to expect the same for non-affirmative cyber coverage. This is especially the case, as the peril is constantly subject to change and hence changes in affected lines of business and types of coverage are to be expected.

Q.21 *What is your view on the feasibility of the metric "Expected losses if key exclusions are not applicable under stress"? Please provide clarification.*

As uncertainties exist, the industry agrees that expected losses should be consistent if exclusions are not applicable. Nevertheless, the variety of existing exclusions, even of the most widely used ones, is large. The schematics of the exclusions differ so much that a simultaneous failure of all is not a realistic basis for a shock. So, the extent and the impact of non-applicable exclusions should be concretized.

In addition, expected losses if reinsurance is not responding as expected should be considered. This is especially important to non-affirmative covers, as reinsurance exclusions are oftentimes stricter than insurance exclusions and, therefore, do not offer back-to-back coverage.

Q.22 *What is your view on the approach to silent cyber approximation? Please add suggestions to improve it and provide clarification.*

The approach can be regarded as pragmatic and comprehensible, but could lead to uncertainties and imprecise results. For reinsurance undertakings, the application of the proposed example shocks might lead to roughly estimated results as much of the required information is not available to them. In general, numbers for silent cyber should not be expected to be available in as much detail as for affirmative cover.

Q.23 *What is your view on the data collection? Is there any relevant information missing? Please provide clarification.*

There is agreement on the general scope of the data collection, but consideration should be taken on a few aspects:

- It is becoming more and more common to insert sub-limits or exclude certain parts of typical coverages. Thus, this should be included as it has a huge impact on the risk. These would need to be applied on a more granular level.
- It must be taken into account that data of non-affirmative cyber exposure is only available to a certain extent.
- Table 9.4.3 in the annex is not feasible, as there is not an exhaustive view of all IT service providers used by clients covered by an insurance policy.

Section 7 - Cyber Resilience: Shocks, Specifications and Metrics

Q.24 *What is your view on the assumed increase in operational and other costs due to a cyber risk event? Please provide clarification.*

There is an agreement on the assumed increase in operational and other costs due to a cyber risk event. In particular, recovery costs could be significant.

Q.25 *What is your view on the proposed shocks in terms of completeness? Please provide clarification.*

The list of proposed shocks seems exhaustive. Some additional comments are proposed to limit the scope:

- For the data breach scenario, the concepts of "data breached" and "sensitive data breached" should be merged to consider a worst-case scenario: ie only "sensitive data breached".
- For the "cloud outage" scenario: the "outage time" should be considered only for critical functions as defined in DORA.
- When considering data lock scenarios (eg ransomware), stressing the number of business processes affected may result in an unrealistic scenario. Based on the own process of business continuity management, the relationship between assets and business processes involved is known in theory.

Q.26 *Do you agree that cyber resilience shocks are provided in technical terms, such as the duration of outage following a cyber event, or should they be prescribed also in terms of financial costs (i.e. monetary amount)? Please provide clarification.*

Yes, there is the agreement that the shocks are provided in technical terms, such as the duration of the outage. However, these technical terms must be able to measure the real impact on the ability of the organisation to fulfil its function. Also including monetary measures is a good way of doing this, as the risks are more comparable in this format.

Q.27 *What is your view on the proposed metrics in terms of completeness and viability? Please provide clarification.*

The proposed metrics are deemed to be sufficient for the most part, as they are aligned with DORA. However, the following slight changes should be made:

- Operational Metric: It is stated that "time elapsed until return to business as usual (time to BAU)". This is longer than the duration of the attack itself. Therefore, the industry proposes to use "time of outage or unavailability".
- Financial metrics: The statement "loss of revenue corresponding to lost business during the downtime" can only be speculative. This is not considered to be a reliable input and is generally excluded by the operational risk calculation baseline framework since there may be a high level of arbitrariness (eg estimate of customers simply delaying the purchase).

The metrics mentioned that are determined to be the most appropriate and complete:

- Recovery time
- Operational cost
- Change in assets and liability
- Solvency Capital Requirement
- Solvency II ratio

Q.28 *What is your view on the assessment of the impact of cyber resilience shocks at the level of business processes for all the scenarios? Would a more granular specification depending on the scenario (e.g. at IT systems level) be preferred? Please provide clarification.*

The impacts of cyber resilience shocks at the level of business processes identified for all the scenarios seem to be sufficient. It is noted that these impacts need to be major to constitute a resilience shock, with an assessment of the impact performed to link the events to the asset group, also taking into account which application is critical. It must be stated that this question cannot be answered in detail without knowledge of the specifics of the stress scenarios (which scenario, methodology). In addition, a more granular assessment at IT systems level is not supported.

Q.29 *What is your view on the exclusion of ransom payments in the context of the ransomware scenario? Please provide clarification*

Including ransom payments in the context of the ransomware scenario could be an option as it would give more information on the financial impact. However, it should be excluded in this document as the inclusion could be seen as promoting ransom payments. This can be excluded as the financial impact would not be relevant to factor into "shock metrics" and the legal implications/discussions are not relevant in this scenario. In addition, the payment estimate of ransoms is hardly linkable to the cyber event, since it can be seen as an exogenous variable that does not depend on the magnitude of the cyberattack in any way. For this reason, it could be difficult and off-topic to assess a proper ransom distribution and related statistics.

Q.30 *What is your view on the identified sources for the calibration of the shocks? Do you have any further suggestion on potential sources for the calibration? Please provide clarification.*

The identified sources for the calibration of the shocks should be considered as examples only. They should be maintained on an intranet page of EIOPA rather than be recorded in a document, as the sources may change, or newer examples will become available.

Q.31 *What is your view on the data collection? Is there any relevant information missing? Please provide clarification.*

It is just noted that data collection creates an increase in cybersecurity breach risk. As a lower risk approach, the data collected should only be provided to supervisors and only shared on request via secured channels.

In relation to the communication of results, the industry would like to highlight the fact that the publication of the results of a cyber stress testing exercise should be approached with extreme caution. In that context, the industry would like to reiterate its position that individual publication is neither necessary nor appropriate for any stress testing exercise. Especially in the context of a cyber stress test, the disclosure of the cyber results, even if these are at an aggregate level, could expose participating undertakings to a great extent by uncovering undertakings' vulnerabilities which can be exploited by malicious parties.